УТВЕРЖДЕНО

643.63024504.00003-05 98 01-ЛУ

ПРОГРАММНЫЙ МЕЖСЕТЕВОЙ ЭКРАН «ИНТЕРНЕТ КОНТРОЛЬ СЕРВЕР»

Руководство администратора

643.63024504.00003-05 98 01

Листов 87

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

2021

АННОТАЦИЯ

В данном программном документе приведено руководство администратора программного межсетевого экрана «Интернет Контроль Сервер» (далее МЭ «ИКС»), предназначенного для обеспечения безопасности локальной вычислительной сети и управления сетевым трафиком при организации доступа между несколькими физическими сегментами сети с различными политиками безопасности. В настоящем документе под администратором МЭ «ИКС» подразумеваются лица, пользующиеся МЭ «ИКС» и осуществляющие настройку.

В разделе «Введение» описаны область применения, возможности и уровень подготовки администратора МЭ «ИКС».

В разделе «Назначение и условия применения» описываются виды деятельности и функции для которых предназначено МЭ «ИКС», а при условии их соблюдения применение средств МЭ «ИКС» в соответствии с назначением.

В разделе «Подготовка к работе» описывается состав дистрибутива, запуск программы и проверка работоспособности МЭ «ИКС».

В разделе «Описание операций» приводится описание модулей МЭ «ИКС», их настройка, расположение и функциональные возможности.

В разделе «Аварийные ситуации. Восстановление МЭ «ИКС» приведено описание действий, требуемых для создания резервных копий и выполнения процедуры восстановления МЭ «ИКС» после аппаратных и программных сбоев.

В разделе «Сообщение пользователю» приведено описание сообщений, выдаваемых МЭ «ИКС» системному администратору/пользователю МЭ «ИКС».

Настоящий документ разработан в соответствии с РД 50-34.698-90. Автоматизированные системы.

Данный документ разработан для удовлетворения требований доверия методического документа ФСТЭК России «Профиль защиты межсетевых экранов типа «Б» пятого класса защиты ИТ.МЭ.Б5.ПЗ».

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

5.1. Область применения

МЭ «ИКС» представляет собой программное средство, осуществляющее контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. МЭ «ИКС» предназначен для обеспечения безопасности локальной вычислительной сети и управления сетевым трафиком при организации доступа между несколькими физическими сегментами сети с различными политиками безопасности. В МЭ «ИКС» реализованы следующие функции:

- контроля и фильтрации, проходящего через него трафика;
- идентификации и аутентификации субъектов межсетевой защиты;
- регистрации событий безопасности;
- преобразования сетевых адресов;
- маскирования локальной сети;
- приоритизации информационных потоков;
- взаимодействия с другими средствами защиты информации.

5.2. Краткое описание возможностей

МЭ «ИКС» предоставляет следующие возможности:

- контроль и фильтрация сетевого трафика, проходящего через МЭ «ИКС». Управление и обработка информационных потоков происходят на основе правил и задач информационной безопасности, индивидуально для каждого объекта защиты;
- идентификация и аутентификация субъектов межсетевого взаимодействия при доступе к различным ресурсам;
- регистрация всех событий, в том числе событий безопасности;
- обеспечение бесперебойного функционирования и восстановление после сбоев;
- тестирование и контроль целостности программного обеспечения МЭ «ИКС»;
- графическое отображение и управление всеми функциями;
- взаимодействие с другими средствами защиты информации, такими как антивирусные программные продукты.

5.3. Уровень подготовки пользователей

Администратор должен иметь как минимум среднее техническое образование, обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы, а также должен быть аттестован на II квалификационную группу по электробезопасности

(для работы с конторским оборудованием). В перечень задач, выполняемых системным программистом/пользователем, должны входить:

- задача поддержания работоспособности технических средств;
- задачи установки (инсталляции) и поддержания работоспособности системных программных средств – операционной системы.

5.4. Перечень эксплуатационной документации

Перечень эксплуатационных документов, с которым необходимо ознакомиться, является:

- СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы";
- Подготовительные процедуры (643.63024504.00003-05 94 01).

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

В данном разделе указаны:

1) Виды деятельности, функции для которых предназначено МЭ «ИКС».
2) Условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средств МЭ «ИКС» в соответствии с назначением.

5.1. Виды деятельности, функции

МЭ «ИКС» предназначен для обеспечения безопасности локальной вычислительной сети и управления сетевым трафиком при организации доступа между несколькими физическими сегментами сети с различными политиками безопасности. В качестве основного функционала стоит рассматривать раздел 1.2 настоящего руководства.

Связь между составными частями МЭ «ИКС», обеспечивающими основной функционал, осуществляется, с одной стороны, посредствам выполнения команд графического интерфейса или командной строки, с другой стороны - при помощи модуля общей шины. Данный модуль является связывающим модулем для регистрации событий от других модулей. Под модулем будет пониматься, в данном руководстве, программное обеспечение, предоставляющее основной функционал и являющееся минимальной составной единицей. Каждый модуль может посылать события, получать события, вызывать функции другого модуля (эта технология называется remote procedure call - RPC). С каждым событием могут также передаваться данные. Если модуль хочет получать определенный тип событий, то сообщает об этом модулю общей шины, который запоминает получателя для указанного события. Если модуль хочет оповестить о случившемся событии, он посылает сигнал на модуль общей шины, который в свою очередь смотрит, кто подписан на нужное событие и пересылает им данные. Если модуль хочет вызвать функцию другого модуля, то также посылает сигнал модулю общей шины и ожидает ответа. В это время вызывается соответствующая функция модуля назначения, получает ответ и пересылает ожидающему модулю. Удаленно вызываемые функции должны быть зарегистрированы в модуле общей шины. Все сообщения, обрабатываемые модулем общей шины, представляются в формате JSON.

Доступ к графическому интерфейсу МЭ «ИКС» осуществляется посредством обозревателя сети Интернет (например: Mozilla Firefox версии 3.0 и выше, Internet Explorer версии 8 и выше, Opera версии 9 и выше, Google Chrome любой версии).

МЭ «ИКС» поддерживает функционал сторонних программ через модули-обертки, которые предоставляют API (application programming interface) для данных программ. Например, антивирусные программы такие как Kaspersky, ClamAV осуществляют связь с МЭ «ИКС» при помощи модуля антивирус, а связь с сервисом SkyDNS осуществляется по протоколу HTTP.

5.2. Программные и аппаратные требования к системе

Для корректного функционирования МЭ «ИКС» необходимо использовать аппаратное

техническое средство (сервер), минимальные и рекомендуемые характеристики технического средства указаны в Таблице 1. МЭ «ИКС» устанавливается на 64-битные аппаратные средства. Аппаратное средство должно иметь как минимум две сетевые карты и привод чтения flash-накопителей.

Таблица 1 - Минимальные и рекомендуемые требования к аппаратной платформе

Характеристика	**Минимально**	**Рекомендуемое**
Частота центрального процессора	2 ГГц	2.4 ГГц и выше
Объем оперативной памяти	2048 Мб	3072 Мб и выше
Объем жесткого диска	512 Гб	1 Тб и выше

Следует учесть, что рекомендуемый объем жесткого диска, устанавливаемый на сервер, зависит от планируемого объема хранимых данных.

МЭ «ИКС» включает в себя минимально необходимый комплект программных средств, включая операционную систему, поэтому не требует наличия дополнительного программного обеспечения и может быть установлен на чистый жесткий диск.

5.3. Скорость обработки трафика (производительность)

Производительность программного межсетевого экрана напрямую зависит от аппаратной платформы на котором установлен. При использовании рекомендованных требований:

- Скорость обработки трафика в режиме межсетевого экрана составляет 1 Гбит/с
- Скорость обработки трафика в режиме IPS (анализ трафика детектором сетевых атак Suricata, с включенными правилами всех категорий и с учётом атак типа «отказ обслуживания» SYN-flood, UDP-flood, ICMP-flood при размере пакета передаваемых данных 1500 байт) составляет 130 Мбит/с

5.4. Источники обновления данных (использование облачных сервисов)

МЭ «ИКС» получает обновления данных из следующих источников:

- Обновления МЭ: hub.a-real.ru;
- Детектор атак: etrules.upmirror.a-real.ru, snort.upmirror.a-real.ru;
- Антивирус Касперского: kasmirror.a-real.ru;
- Антиспам Касперского: kasmirror.a-real.ru;
- Веб фильтр Касперкого: kfwmirror.a-real.ru;
- Clamav: clamav.upmirror.a-real.ru;
- Гарнет фильтр: garnet.a-real.ru.

Никакие пользовательские данные не отправляются за пределы МЭ «ИКС» в процессе обновления и работы. Администратор может предоставить удаленный доступ к МЭ «ИКС» для технической поддержки. В данном режиме, использует удаленный адрес dev.a-real.ru.

3. ПОДГОТОВКА К РАБОТЕ

В разделе «Подготовка к работе» указаны:

– состав и содержание дистрибутивного носителя данных;

– порядок загрузки данных и программ;

– порядок проверки работоспособности.

5.1. Комплектность поставки

В состав комплекта при приемке МЭ «ИКС» должны входить следующие изделия и документы:

– ПО (Дистрибутив);

– Формуляр;

– Руководство администратора;

– Программа и методика испытаний.

5.2. Запуск системы

Предварительно необходимо выполнить установку системы. Установка МЭ «ИКС» осуществляется системным администратором. Для установки МЭ «ИКС» необходимо выполнить следующие действия:

– вставить дистрибутивный flash-носитель;

– после окончания процесса загрузки — на экране появится приветствие и окно выбора языка установки;

– далее необходимо выбрать «Установка»;

– будет выведено «Лицензионное соглашение», с которым необходимо ознакомиться и принять;

– затем необходимо выбрать часовой пояс, в котором будет использоваться МЭ «ИКС»;

– выбрать сетевой интерфейс, через который будет производиться настройка и управление МЭ «ИКС»;

– произвести настройку IP-адреса и маски для изолированной сети, из которой будет производиться управление МЭ «ИКС». Поле «Шлюз» необходимо оставить пустым;

– указать сетевое имя сервера;

– согласиться с выбором настройки ZFS и выбрать жесткий диск для установки.

Штатный режим работы Изделия предполагает создание доверенного канала передачи данных, а также доверенного маршрута между МЭ и администраторами МЭ для осуществления функций управления МЭ, путем доступа к веб-интерфейсу. Для этого рекомендуется выполнить следующие действия:

- В процесс установки изделия, при указании IP/mask на сетевом интерфейсе:

1) В указанный сетевой интерфейс должен быть подключен провод из управляющей сети, являющейся безопасной.

2) Указывается свободный IP-адрес из управляющей сети.

3) Указывается маска управляющей сети после «/».

4) В случае отсутствия управляющей сети. Необходимо взять заведомо безопасное устройство, с установленным браузером (Firefox, Chrome итд); подключить его напрямую к МЭ; задать на безопасном устройстве сеть, не пересекающуюся с сетями на предприятии, с 30 маской; выполнить шаги 1.1-1.3

- После выполнения установки, выполнить вход в веб-интерфейс МЭ.

- Перейти в Меню – Сеть – Провайдеры и сети. В открывшейся вкладке нажать кнопку «Добавить» и выбрать из выпадающего списка «Локальная сеть». Будет открыта форма создания локальной сети. В данной форме необходимо выбрать интерфейс, который был указан в шаге 1.1, в поле «IP-адрес/префикс» указать данные заведенные в пунктах 1.2-1.3, установить флаги «Разрешить управление ИКС через веб» и «Разрешить управление ИКС через SSH».

В Меню - Обслуживание - Все службы необходимо выключить службы/сервера: DNS-сервер и Сервер каталогов"

- После выполненных действий произвести дальнейшую настройку МЭ.

- Запрещается устанавливать флаги «Разрешить управление ИКС через веб» и «Разрешить управление ИКС через SSH» в сетях не являющихся управляющими.

По окончании процесса установки МЭ «ИКС», будет открыта консоль восстановления. Дальнейшую настройку МЭ «ИКС» рекомендуется выполнить через веб-интерфейс, который будет доступен на 81 порту по протоколу HTTPS, на указанном IP-адресе в изолированной сети (пример адреса: https://IP_ics:81).

5.3. Проверка работоспособности МЭ «ИКС»

Для проверки работоспособности МЭ «ИКС» системный администратор должен обратиться к сетевому адресу МЭ «ИКС» (заданному в п.п. 3.2) с помощью веб-браузера по протоколу HTTPS на 81 порт. В качестве браузера рекомендуется использовать Mozilla Firefox или Google Chrome. При первом входе в веб-интерфейс, система встроенной защиты браузеров, выдаст предупреждение о вероятной угрозе безопасности. Это связано с тем, что веб-интерфейс МЭ «ИКС» работает по протоколу HTTPS, который требует использование сертификата. Данный сертификат создается при установке, самим МЭ «ИКС», в том числе и подписывается им. Так как МЭ «ИКС» не является доверенным центром сертификации, подписанные им сертификаты будут считаться не доверенными и поэтому так реагирует система защиты в веб-браузерах. Необходимо проигнорировать данное предупреждение и добавить в исключение веб-браузера сертификат.

После этого будет открыта форма авторизации. По умолчанию установлен логин – root и пароль – 00000 (пять нулей) для учетной записи администратор. Кроме того, в окне авторизации находятся ссылки на: документацию; утилиту авторизации (Xauth); страницу авторизации (Captive portal); веб-интерфейс почты (Веб-почта); страницу softphone (Xphone).

Этап проверки работоспособности МЭ «ИКС» считается выполненным, если, введя логин и пароль по умолчанию, будет открыта главная страница.

4. ОПИСАНИЕ ОПЕРАЦИЙ

В данном разделе рассматриваются все функциональные модули, функции и способы их настройки, применяемые в МЭ «ИКС».

5.1. Описание веб-интерфейса и первоначальная настройка

Веб-интерфейс разделен на две части. В левой находится список модулей системы, а в правой - окно текущего модуля. При первом входе ни один модуль еще не открыт, поэтому отображается главная страница системы.

Главная страница веб-интерфейса представляет собой систему виджетов, отображающих актуальную информацию о системе (Таблица 2). Стоит отметить, что первоначально не все виджеты выведены на главную страницу. Для работы с виджетами (изменение размера, положения; добавление/удаление) необходимо нажать справа снизу на иконку карандаша.

Таблица 2 - Главная страница веб-интерфейса

Виджет	Информация	Возможные действия	Переход	Зависимые службы
Пользователи	Общее количество, количество активных, заблокированных, отключенных и подключенных по VPN пользователей	Добавить пользователя, импортировать пользователей	Пользователи, Роли, Монитор соединений	-
Статистика	Размер входящего и исходящего трафика за текущие день, неделю и месяц	Включить/отключить статистику	Отчеты	Статистика, Счетчики, Прокси
Отчеты по категориям	Сводная информация о распознанных категориях трафика за текущий день	-	Отчеты (Категории трафика)	-
Безопасность и ограничение доступа	Число совершенных атак и обнаруженных вирусов	Включить/выключить систему безопасности	Наборы правил, Категории правил, Межсетевой экран (правила), Прокси (настройки)	Прокси, Межсетевой экран, DNS-сервер, Антивирус, Антивирусный прокси-сервер, Контент-фильтр
Провайдеры и сети	Провайдер по умолчанию, пинг, средняя загрузка интерфейса, количество VPN - подключений	Запустить мастер настройки сети	Провайдеры и сети, Доступ к VPN (Пользователи), Управление отчетами (отчет по	-

Виджет	Информация	Возможные действия	Переход	Зависимые службы
			интерфейсам), Сетевые утилиты	
Почта	Количество обработанных писем (отправленных, полученных, отправленных в спам, обнаруженных вирусов)	Включить/выключить почтовые службы, добавить почтовый ящик	Почта: главная страница, домены и ящики, фильтры, адресная книга, почтовая очередь, статистика почты	Почтовый сервер, Хранилище почты, Сборщик почты, Антиспам SpamAssassin, DNS-сервер, Сервер каталогов, Служба DKIM-подписи
Веб и файловый сервер	Количество виртуальных хостов, ресурсов, оставшееся свободное место на диске	Включить/выключить файловый сервер, добавить один из ресурсов, добавить раздел и подключить жесткий диск	Хранилище файлов, Веб (ресурсы), FTP (FTP-ресурсы), Сетевое окружение (идентификация)	FTP-сервер, Сетевое окружение, DNS-сервер
Телефония	Количество внешних каналов, телефонных номеров, факсов	Включить/выключить службу телефонии, добавить телефонный номер, добавить факс	Телефония (телефонные номера, правила, журнал звонков)	Телефония, DNS-сервер
Монито-ринг и обслужива-ние	Загрузка процессора, оперативной памяти, системы, время до конца демо-версии (если система не активирована)	Включить/выключить мониторинг системы, создать резервную копию	Мониторинг, Обновления, Время и дата, Системный журнал	Мониторинг состояния системы, Системные уведомления
Лента сайтов	Последние зарегистрированные посещения сайтов	-	Отчеты (Активность пользователей)	-
Лента поисковиков	Последние зарегистрированные запросы в поисковых системах	-	Отчеты (Лента поисковиков)	-
События	Последние события системы из системного журнала	-	Журнал и уведомления (Системный журнал)	-

Все представленные виджеты обновляются в реальном времени.

В правом верхнем углу интерфейса находятся: имя пользователя, под которым была произведена авторизация, при нажатии по имени откроется выпадающий список (Личный кабинет, Xauth, Captive portal, Веб-почта, Xphone, Выход); иконка загрузки файла; непрочитанные системные сообщения; переход к документации. Непрочитанные системные сообщения – отображают количество не прочитанных системных сообщений с момента последнего входа в систему. При нажатии на нее в отдельном всплывающем окне показывается последнее непрочитанное сообщение.

После первого входа в веб-интерфейс необходимо провести первичную настройку системы. Первичная настройка системы запускается автоматически и происходит при помощи мастера начальной настройки системы. Мастер представляет собой пошаговую настройку системы. Он запросит ввести название организации, имя хоста и новый логин/пароль администратора. После прохождения всех шагов МЭ «ИКС» выведет таблицу всех применяемых изменений. Подтвердите их нажатием кнопки «Готово».

Для настройки основного функционала, сперва необходимо запустить мастер настройки сети. Для этого в списке модулей системы выбрать «Сеть – Мастер настройки сети». Будет открыто новое диалоговое окно. На первом шаге, будет предложено выбрать как будет использоваться тот или иной физический интерфейс. Минимально рекомендованное количество интерфейсов три, при этом для управляющего интерфейса стоит устанавливать тип «Локальная сеть». Всевозможные типы описаны в Таблице 3.

Таблица 3 - Типы сетевых интерфейсов

Тип	Описание
Не использовать	Интерфейс не будет использоваться
Локальная сеть	В этой сети будут находиться объекты, трафиком которых может управлять МЭ «ИКС»
DMZ-сеть	В этой сети могут находиться корпоративные сервера с внешними IP-адресами. Такая настройка сети проводится для повышения их безопасности и ограничения уровня доступа к ним посредством межсетевого экрана
Провайдер	Провайдер предоставляющий доступ в сеть интернет по технологии Dynamic or Static IP over Ethernet
Провайдер PPPoE	Провайдер предоставляющий доступ в сеть интернет по протоколу PPPoE
Провайдер PPTP поверх IP/DHCP	Провайдер предоставляющий доступ в сеть интернет по протоколу PPTP. При этом можно выбрать статически сконфигурированный IP-адрес «серой» сети провайдера либо динамический IP-адрес «серой» сети провайдера, получаемый от DHCP-сервера провайдера
Провайдер L2TP поверх IP/DHCP	Провайдер предоставляющий доступ в сеть интернет по протоколу L2TP. При этом можно выбрать статически сконфигурированный IP-адрес «серой» сети провайдера либо динамический IP-адрес «серой» сети провайдера, получаемый от DHCP-сервера провайдера

Стоит отметить, что такие провайдеры, как 3G и Wi-Fi, требуют отдельной настройки.

На следующих этапах «Мастер настройки сети» предложит ввести параметры для каждого сетевого интерфейса, с выбранным типом не являющимся «Не использовать». На последнем шаге «Мастера настройки сети» будут выведены все введенные параметры. Стоит отметить, что параметр «Управление ИКС» должен быть установлен только у управляющего интерфейса. Если все было введено верно, то необходимо нажать кнопку «Готово» – мастер настройки сети применит новую конфигурацию и откроет модуль «Провайдеры и сети».

5.2. Контроль и фильтрация сетевого трафика

Для контроля и фильтрации трафика в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: Пользователи, Диапазон адресов, Набор правил, Категории трафика, Сетевое окружение, Контент-фильтр, Почтовый сервер, Сертификаты, Телефония, VPN, Маршруты, Межсетевой экран, Прокси, Перенаправление портов.

5.2.1. Пользователи

В данном подразделе под пользователем стоит понимать статистическую единицу МЭ «ИКС». Пользователь – это наименьший объект применения политик МЭ «ИКС» и детализации статистики сетевого трафика. После того как пользователь добавлен, он получает доступ во внешнюю сеть (Интернет) в соответствии со своим способом авторизации, а также индивидуальными и глобальными политиками доступа. Модуль «Пользователи» расположен слева в меню в разделе «Пользователи и статистика».

Для добавления пользователя необходимо нажать кнопку «Добавить». Данным способом пользователю возможно назначить имя, логин, пароль, описание и привилегии администрирования системы, при этом у данного пользователя появится возможность удаленно подключаться к серверу через VPN и выход в сеть Интернет с помощью логина и пароля. Остальные параметры редактируются непосредственно в индивидуальном модуле пользователя.

Кроме описанного способа, пользователей в МЭ «ИКС» можно добавить следующими способами:

– используя «Мастер создания пользователя», в модуле «Пользователи» с пошаговым прохождением этапов добавления параметров пользователя, таких как имя пользователя, роль, имя входа (логин), пароль, один или несколько IP-адресов, наборы правил, а также почтовый ящик. Из всех перечисленных параметров обязательным является только имя пользователя. Для запуска «Мастера создания пользователей» необходимо нажать соответствующую иконку в правом верхнем углу горизонтального меню модуля «Пользователи». В случае если назначаемый почтовый ящик не может быть присвоен ни одному из созданных в системе почтовых доменов, МЭ «ИКС»

предложит создать новый почтовый домен. После прохождения всех шагов мастер выведет сводку создаваемых параметров пользователя. По нажатии кнопки «Готово» пользователь будет создан;

- в модуле «Пользователи» нажмите кнопку «Добавить» и создайте нового пользователя или группу. В этом случае форма позволит указать имя пользователя, описание, роль, логин, пароль, а также дополнительные поля, такие как номер телефона и должность. Остальные параметры нужно будет добавить уже после создания пользователя или группы. По умолчанию доступны следующие привилегии для пользователей: Администратор (пользователь имеет полный доступ ко всем функциям веб-интерфейса МЭ «ИКС»); Пользователь (пользователь имеет доступ только к своей персональной странице просмотра статистики); Администратор группы (пользователь имеет доступ к функциям создания, удаления и редактирования пользователей группы, в которой он находится, а также назначения правил, квот и просмотра статистики). Категории привилегий можно расширить при помощи модуля «Роли». Пользователи могут быть объединены в группы. Группам можно назначать правила доступа и квоты, которые будут применяться для всех ее членов. Пользователя можно переместить из одной группы в другую простым перетаскиванием мыши. Пользователь или группа пользователей могут быть отключены в любой момент выбором пункта «операции\выключить». При этом у данного пользователя пропадает доступ к сети Интернет;
- импортированием пользователей. Чтобы импортировать пользователей, зайдите в модуль «Пользователи» и нажмите в правом верхнем углу на кнопку «Импорт». Откроется диалоговое окно, предлагающее выбрать, каким образом пользователи будут импортированы. Существуют следующие варианты импорта: 1) из файла (источником служит файл формата *.txt, в котором перечислены строки, содержащие параметры: имя, логин, пароль, IP-адрес. Каждый пользователь в отдельной строке, кроме того, в окне формы импорта можно вручную создать необходимое количество пользователей); 2) из сети (МЭ «ИКС» сканирует свою локальную сеть и заносит все IP-адреса, которые в настоящий момент активны. Очень удобный способ для занесения пользователей с авторизацией по IP-адресу. МЭ «ИКС» импортирует пользователей, присваивая им имена и логины в виде pcX-Y, где X – это предпоследняя цифра IP-адреса, а Y - последняя цифра IP-адреса. Отметив нужных для импорта пользователей в списке, необходимо нажать кнопку ОК); 3) из LDAP/AD (данный способ более универсален и подходит для большинства LDAP-каталогов. Пользователи будут сгруппированы по их organization unit'ам. Если синхронизована группа пользователей, то отредактировать или

удалить отдельного пользователя в этой группе через веб-интерфейс МЭ «ИКС» невозможно. Импортированные и синхронизированные пользователи будут отмечены в списке пользователей специальной иконкой).

4.1.1.1. Авторизация пользователей в МЭ «ИКС»

После окончания процесса создания пользователей в МЭ «ИКС» необходимо настроить их авторизацию. В МЭ «ИКС» применяются следующие способы авторизации пользователей:

- авторизация по IP-адресу. Применяется в том случае, когда пользователи локальной сети имеют статические IP-адреса либо динамические IP-адреса, регистрируемые с привязкой к MAC-адресу. Пользователь получает доступ во внешнюю сеть по всем протоколам в соответствии с глобальными и индивидуальными политиками доступа. Для того чтобы выдать пользователю IP-адрес, необходимо кликнуть на имя пользователя в списке в модуле «Пользователи», при этом откроется страница с информацией о выбранном пользователе. Затем нужно открыть вкладку «IP/MAC-адреса», нажать кнопку «Добавить» и задать адрес, выделенный для этого пользователя. После этого назначенный адрес появится в списке адресов пользователя. Одному пользователю можно назначить любое количество IP-адресов. Также, если записать адрес в формате адрес/префикс, можно назначить пользователю диапазон адресов. Для сохранения функций безопасности МЭ «ИКС» в данном случае рекомендуется производить привязку к MAC-адресу.
- авторизация по MAC-адресу. Данный вид авторизации удобен, когда в сети используются динамические адреса. Для того чтобы добавить пользователю MAC-адрес, перейдите во вкладку «IP/MAC-адреса» и нажмите «Добавить - MAC-адрес».
- авторизация по логину и паролю. Чтобы установить данный тип авторизации, поставьте соответствующий флаг в настройках Captive Portal. Тогда в модуле «Captive Portal» будет включен и запущен сервер веб-авторизации. При первом обращении пользователя к какому-либо ресурсу ему будет предложено ввести логин и пароль, закрепленный за его учетной записью в МЭ «ИКС». При необходимости установите флаг «Запретить множественную авторизацию с одним логином». Тогда пользователь, использующий конкретный логин, не сможет одновременно авторизоваться при помощи Captive Portal с различных устройств (IP-адресов). Аналогичная опция присутствует в настройках сервера авторизации (Xauth), однако действие этих опций не перекрывается, и каждая из них влияет только на соответствующую службу.
- SMS-авторизация. Чтобы установить данный тип авторизации, поставьте соответствующий флаг в настройках Captive Portal. Тогда пользователи будут

проходить авторизацию через SMS. В поле «Назначать адреса пользователю» выберите одного из пользователей, заведенных на МЭ «ИКС». Данному пользователю для каждой новой сессии будут выдаваться динамические IP-адреса. В поле «Время действия кода, отправленного в SMS» укажите время действительности кода в секундах (от 60 до 999999). Если время действия кода истекло и код не был введен, то пользователю необходимо вновь запросить код, нажав соответствующую кнопку в форме веб-авторизации. По умолчанию установлено значение 180 секунд. В поле «Интервал между повторными попытками отправки SMS» задайте время блокировки кнопки «Отправить СМС повторно» для пользователя при SMS-авторизации. Значение, задаваемое в данном поле, не должно превышать время действия кода. В поле «Максимальное число попыток повторной отправки SMS для одного номера» укажите число попыток повторной отправки SMS, которое может совершить пользователь для одного абонентского номера. При этом время между попытками будет вычисляться по формуле: номер попытки * «Интервал между повторными попытками отправки SMS». Если пользователь исчерпал указанное число попыток отправки SMS, он сможет изменить абонентский номер для отправки SMS. При смене абонентского номера число попыток обнулится. В поле «Текст SMS» введите текст сообщения, которое будет отправлено пользователю при авторизации. Данное сообщение обязательно должно содержать шаблон {code}. Вместо этого шаблона SMS-сервер вставит четырехзначное число. Для подключения сервера SMPP заполните в блоке «Параметры SMPP» следующие поля: «SMPP-сервер», «Порт», «Логин/system_id» и «Пароль».

- авторизация по звонку. Чтобы установить данный тип авторизации, поставьте соответствующий флаг в настройках Captive Portal. Тогда пользователи будут проходить авторизацию по звонку. В поле «Назначать адреса пользователю» выберите одного из пользователей, заведенных на МЭ «ИКС». Данному пользователю для каждой новой сессии будут выдаваться динамические IP-адреса. В поле «Провайдер телефонии для приема звонков» задайте SIP-провайдера модуля IP-телефонии МЭ «ИКС», который будет ожидать входящий звонок от авторизуемого пользователя. В поле «Номер для звонка» укажите внешний номер провайдера, на который необходимо совершить звонок авторизуемому пользователю. В поле «Время ожидания звонка» задайте время (в секундах), в течение которого авторизуемый пользователь должен совершать звонок на указанный номер.
- авторизация пользователей AD. Такая авторизация возможна в двух вариантах в зависимости от протокола сетевой аутентификации, который используется: NTLM либо Kerberos/LDAP. Данные типы авторизации используются, когда необходимо

авторизовать пользователей AD. Авторизация будет выполнена прозрачно, без запроса логина и пароля. Использование данных типов предполагает прямое указание прокси в браузере или других программах, которые их поддерживают.

- утилита авторизации Xauth. Представляет собой exe-файл, запускаемый на машине пользователя (применимо только для Windows-систем). Применять данную утилиту для авторизации стоит в случае действия стороннего DHCP-сервера, выдающего IP-адреса без привязки к MAC, а также в случае, когда пользователи импортированы из Active Directory (в таком случае после импорта пользователя авторизация происходит автоматически сразу после запуска исполняемого файла Xauth.exe). Чтобы скачать файл Xauth.exe, откройте веб-интерфейс на странице авторизации МЭ «ИКС» и нажмите на ссылку «Xauth». Браузер предложит сохранить файл. Если Xauth не находит IP-адрес МЭ «ИКС» автоматически, запустите утилиту с параметром --server IP-адрес МЭ «ИКС». Чтобы вывести полный список дополнительных параметров, запустите Xauth с ключом --help. Чтобы отключить утилиту, нажмите правой кнопкой мыши на значок Xauth в трее системы и выберите пункт «Выход».

Существует возможность использовать два типа авторизации одновременно. Часть пользователей выходят в сеть Интернет с использованием авторизации по логину/паролю, а часть - с использованием авторизации по IP. Более подробно данный порядок авторизации будет описан в разделе настройки прокси-сервера.

4.1.1.2. Управление доступом пользователей

Для того чтобы назначить пользователю или группе правило доступа, нажмите на имя пользователя или группы в модуле Пользователи. Откроется персональная страница пользователя (группы). В ней необходимо выбрать вкладку «Правила и ограничения» и нажать на кнопку «Добавить» на верхней панели. Будет предложено выбрать необходимый вид правила. Для контроля пользователей в МЭ «ИКС» реализованы и применяются следующие методики:

1) Запрещающие, разрешающие правила и исключения – контролируют доступ пользователя к IP-адресам, протоколам, портам и MIME-типам на уровне межсетевого экрана.
2) Запрещающие, разрешающие правила и исключения прокси-сервера – контролируют доступ пользователя к интернет-ресурсам по URL на уровне прокси-сервера.
3) Ограничение скорости – изменяет скорость доступа к указанным ресурсам или к внешней, или внутренней сети в целом.
4) Выделение полосы пропускания – устанавливает минимальное значение скорости доступа к указанным ресурсам или к внешней, или внутренней сети в целом.
5) Квота – устанавливает максимальное значение полученного пользователем объема данных

от указанного ресурса, по указанному протоколу (порту) или от внешней или внутренней сети в целом.

6) Маршрут – устанавливает для пользователя индивидуальное направление потока передачи данных до указанного ресурса, по указанному протоколу (порту) или до внешней или внутренней сети в целом.
7) Приоритет – присутствует только в глобальных правилах межсетевого экрана, позволяет установить очередность обработки потока передачи данных до указанного ресурса, по указанному протоколу (порту) или до внешней или внутренней сети в целом.
8) Правило контентной фильтрации – добавляет правило прокси-сервера, которое проверяет загружаемый HTML-код на совпадения с базой данных контент-фильтра.
9) Ограничение количества соединений – создает правило межсетевого экрана, не позволяющее пользователю превышать указанное количество одновременных соединений с внешней сетью.

Кроме того, существуют специальные объекты, ускоряющие создание политик доступа:

1) Категории – аналогичны разрешающим (запрещающим) правилам прокси-сервера, но позволяют включать в себя множество URL, а также добавляют фильтрацию по расширению загружаемого файла и ключевым словам. Они подразделяются на две группы – стандартные категории – содержат статический список объектов и обновляются вместе с обновлением МЭ «ИКС». Вторая группа – категории SkyDNS – это ссылки, обращающиеся к серверу сервиса SkyDNS и обновляющиеся динамически.
2) Наборы правил – глобальные объекты, позволяющие сохранить любое количество пользовательских правил под указанным именем и применить без повторной настройки сразу к нескольким пользователям или группам.

Также, каждому объекту может быть применен параметр «Время действия», ограничивающий время работы политики.

При применении различных политик контроля доступа пользователей следует учесть последовательность их применения:

1) Глобальные правила межсетевого экрана.
2) Глобальные профили ролей пользователей.
3) Политики корневой группы.
4) Политики вложенных групп.
5) Политики конкретного пользователя.

Для того чтобы скопировать созданное правило, нажмите на него в списке, а затем — на соответствующую кнопку.

5.2.2. Диапазоны адресов

Данный модуль предназначен для создания диапазона IP-адресов, к которым можно применять различные правила и использовать для оптимизации действий в других модулях. В диапазон адресов можно объединять: списки произвольных IP-адресов, подсетей, доменных имен. Данные диапазоны могут быть внешними или внутренними (не тарифицируемыми). По умолчанию любой создаваемый диапазон является внутренним. В качестве примера можно привести создание диапазона адресов, предоставляемых оператором связи к своим внутренним ресурсам, которые не оплачиваются по тарифу. Для того чтобы диапазон адресов приобрел статус «внешний», необходимо установить соответствующий флажок «Внешний диапазон адресов» при настройке. Настройка данного модуля происходит в меню «Пользователи и статистика».

Если список адресов слишком велик, чтобы вводить их по одному в веб-интерфейсе МЭ «ИКС», возможно загрузить его из текстового файла формата *.txt. В нем должны быть перечислены IP-адреса, подсети в формате IP-адрес/префикс или домены, каждый с новой строки. МЭ «ИКС» предложит указать файл для загрузки при нажатии на кнопку «Импорт».

5.2.3. Набор правил

Наборы правил – глобальные объекты, позволяющие сохранить любое количество пользовательских правил под указанным именем и применить без повторной настройки сразу к нескольким пользователям или группам.

Для создания набора правил необходимо нажать кнопку «Добавить», ввести имя создаваемого правила и описание, а также при необходимости можно указать время действия создаваемого правила (например, Пн-Пт 08:00-17:00). Таким образом создастся общее название для последующих устанавливаемых правил, в качестве сравнения можно привести создание каталога для файлов. Для добавления определенного правила, необходимо кликнуть на заданное имя набора правил, при этом должен открыться список правил в отдельном модуле. В открывшемся модуле если нажать на кнопку «Добавить», то можно добавить правила аналогично как обычному пользователю или группе.

Для применения созданных правил к пользователю существует два похода. Во-первых, в меню «Пользователи» выбрать соответствующего пользователя двойным нажатие, в открывшемся модуле, перейти во вкладку «Правила и ограничения» и данной вкладке нажать «Добавить», в выпавшем списке выбрать «Набор правил», и затем выбрать нужный набор правил из списка. Во-вторых, в модуле «Набор правил» необходимо кликнуть на один из наборов правил, если выбранный набор правил не автоматический, то в открывшемся модуле будет вкладка «Пользователи», перейдя в которую можно отметить флажками определенных пользователей или группы их, для которых данный набор правил будет применен.

В модуле «Наборы правил» по умолчанию создано несколько наборов правил - «Набор правил для администраторов», «Набор правил для пользователей» и «Набор правил для администраторов группы». Правила в этих наборах автоматически применяются ко всем пользователям, имеющих привилегии «Администратор», «Пользователь» и «Администратор группы» соответственно. Также в МЭ «ИКС» добавлен специальные наборы правил для учебных заведений (SkyDNS, Kaspersky, поисковики, SkyDNS, набор правил для школ), которые содержат преднастроенные правила доступа для пользователей согласно закону 436-ФЗ РФ. Он содержит следующие правила: запрет доступа на сайты, причиняющие вред здоровью и развитию детей; выдача ответов на запросы в поисковой системе с применением детского режима поисковика, в частности для российского поисковика (Яндекс); сканирование всего трафика контент-фильтром.

Кроме этого, при импорте пользователей из домена автоматически будут созданы наборы правил для каждой импортированной группы.

5.2.4. Категории трафика

Модуль «Категории трафика» служит для объединения множества URL (Uniform Resource Locator), а также ключевых слов или регулярных выражений в единое правило. Их можно применять для создания запрещающих или разрешающих правил прокси. По умолчанию в МЭ «ИКС» создано несколько категорий, наиболее часто применяемых в блокировке трафика, таких как баннеры, порно, троянские сайты, социальные сети и т.д. данные категории можно применять, но нельзя редактировать.

Для того чтобы создать собственный набор адресов, расширений или ключевых слов, необходимо нажать кнопку «Добавить» и выбрать пункт «Категории трафика». Если необходимо создать несколько категорий трафика, то сперва необходимо создать «Группу категорий трафика». При выборе пункта «Категории трафика» откроется диалоговое окно с вкладками. На первой предлагается ввести название новой категории и при необходимости добавить ее описание. На вкладках: «Адреса», «Расширения», «Ключевые слова» и «MIME-типы» создаются соответствующие правила. Если необходимо сохранить список используемых правил, то в каждой вкладке есть функция экспорта в текстовый файл. Также реализована обратная функция, если есть файл, в формате *.txt, то его можно импортировать, нажав на кнопку «Загрузить».

Для оптимизации процесса составления, изменения и актуализации, разрешенных/запрещенных «Адресов», «Расширений», «Ключевых слов» или «MIME-типов» необходимо выбрать пункт «Автоматические категории трафика» и указать путь URL, где расположены текстовые файлы, а также указать частоту обновления данных файлов.

5.2.5. Сетевое окружение

Для управления сетевым окружением необходимо в меню слева выбрать «Файловый сервер» – «Сетевое окружение». Для обмена данными в локальной сети используется протокол SMB (Server Message Block) — сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. В МЭ «ИКС» за реализацию этого протокола отвечает служба Samba. При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Вкладка «Идентификация» определяет роль МЭ «ИКС» в локальной сети. В поле «Имя компьютера» задается сетевое имя МЭ «ИКС», соответственно описание в поле «Описание». Описание ролей представлено в Таблице 4.

Таблица 4 - Описание роли МЭ «ИКС» в сетевом окружении

Роль	**Значение**
Рабочая группа	В локальной сети не используется контроллер домена (AD), компьютеры находятся в одной рабочей группе, WINS-сервер отсутствует. По умолчанию МЭ «ИКС» находится в рабочей группе WORKGROUP, при необходимости возможно переименование.
Домен	В локальной сети используется контроллер домена (AD). МЭ «ИКС» может быть присоединен к домену. Это позволит импортировать доменных пользователей, синхронизировать их, а также использовать доменную авторизацию на сетевых ресурсах МЭ «ИКС». Для того чтобы МЭ «ИКС» могло импортировать пользователей из домена и синхронизировать их через LDAP, доменный пользователь, заведенный для МЭ «ИКС», должен обладать привилегиями администратора домена. А для обратной связи, чтобы МЭ «ИКС» мог присоединиться к домену и обмениваться данными с контроллером, необходимо, чтобы сервер-контроллер домена был занесен в список пользователей МЭ «ИКС», и его авторизация происходила по IP-адресу.

Флажок «Принудительно подписывать SMB запросы» предназначен для включения дополнительных параметров безопасности сетевых ресурсов, однако, они могут не поддерживаться старыми операционными системами. Если требуется, установите флаг «Разрешить SMBv1», который включает поддержку устаревших протоколов для взаимодействия с WindowsXP, PHP-скриптов и т. д. После нажатия кнопки «Подключиться» МЭ «ИКС» применит выбранную роль в сетевом окружении. Если выбрана роль «Домен», то сервер запросит логин и пароль для

присоединения к домену. Если подключение к домену прошло успешно, справа от поля с именем домена появится зеленый кружок.

Вкладка «Общие ресурсы» позволяет добавить, удалить или отредактировать текущие ресурсы в сетевом окружении. При добавлении сетевого ресурса МЭ «ИКС» предложит ввести: имя ресурса, его описание, источник и установить права доступа к сетевому ресурсу. В пункте «источник» указывается директория, в которой будет располагаться содержимое общего ресурса, при необходимости можно создать новую директорию. В пункте «права доступа» настраиваются права для пользователей или групп на запись или чтение. Если отметить запись и чтение для гостевого входа, то представится возможность изменения файлов и просмотра любому подключившемуся к серверу. В случае если МЭ «ИКС» не подключен к домену, то сетевое окружение работает только с логинами, написанными без использования заглавных букв.

Вкладка «Журнал» отображает сводку всех системных сообщений от SMB-сервера. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) Data Leak Prevention - зеленым, предупреждения – желтым, ошибки – красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.2.6. Контент-фильтр

Контент-фильтр позволяет настроить правила для пользователей на блокировку интернет-страниц, если в HTML-коде интернет-страниц содержатся заданные ключевые слова или регулярные выражения. Для управления контент-фильтрацией необходимо в меню слева выбрать «Защита» – «Контент-фильтр». При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Вкладка «Настройки» позволяет произвести настройку контентной фильтрации. Для запуска модуля необходимо отметить флажок напротив «Использовать контент-фильтр» и указать флажками, что применять для контентной фильтрации: шаблоны и/или ключевые слова. При первоначальной настройке базы контент-фильтра загружены. Для того чтобы обновить списки до последней версии, необходимо установить флажок «Проверять наличие обновлений баз контент-фильтра», МЭ «ИКС» подключится к облачному сервису и загрузит списки. В дальнейшем при установленном флажке МЭ «ИКС» будет обновлять списки в соответствии с выбранным временем.

Вкладка «База Контент-фильтра» по умолчанию база контент-фильтра уже содержит список слов, запрещенных Минюстом и Госнаркоконтролем, а также специальный список ялов для школ. Следует учесть, что контент-фильтр обращается ко всей базе целиком. Каждый список содержит два раздела - шаблоны и ключевые слова. В ключевых словах всегда указывается одно слово, шаблон может содержать набор слов и будет фильтроваться по выражению целиком. При необходимости можно выключить данные списки. Удалить данные списки нельзя. Для добавления новой группы слов для контентной фильтрации необходимо выбрать «Добавить» - «Группа слов контент-фильтра». Откроется новое диалоговое окно, в котором будет предложено задать название группы, данное поле является обязательным, и ввести описание, данное поле является не обязательным. Для добавления группы слов, необходимо перейти на вкладку «Ключевые слова» и нажимая кнопку «Добавить» можно добавлять по одному слову или импортировать из файла. Стоит отметить, что при импорте файла, если ранее были введены ключевые слова, то они все удалятся. Импортируемый файл должен иметь следующую структуру – каждое новое ключевое слово должно начинаться с новой строки. При этом стоит отметить, что если задано словосочетание, в импортируемом файле или, когда идет добавление администратором, то МЭ «ИКС» воспримет данный ввод, как ввод нескольких ключевых слов. Задаваемые ключевые слова чувствительны к используемому регистру, например, слова «Дом» и «дом» являются разными ключевыми словами. Для экспорта ключевых слов необходимо нажать кнопку «Экспорт». Для удаления ключевого слова или группы слов, необходимо выделить их и нажать кнопку «Удалить». Работа с добавлением, удалением, импортом и экспорт для шаблона ключевых слов, аналогична работе с ключевыми словами. Главным отличием шаблона от ключевых слов является регистр независимость, а также возможность задавать словосочетания и различные спецсимволы. Выбрав созданную группу ключевых слов, ее можно включить/выключить, редактировать или удалить.

Вкладка «События» отображает список всех блокировок контент-фильтра за текущую дату. В каждой строке блокировки указан пользователь, для которого была произведена блокировка и причина блокировки.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные

журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.2.7. Почтовый сервер

Почтовый сервер (сервер электронной почты, мейл-сервер) — в системе пересылки электронной почты так обычно называют агент пересылки сообщений (англ. mail transfer agent, MTA). Это компьютерная программа, которая передает сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой — клиентом электронной почты (англ. mail user agent, MUA). Для настройки почтового сервера необходимо перейти в меню «Почта».

Организация собственного почтового сервера позволяет более гибко формировать политику отправки и приема почтовых сообщений. Зачастую возможности хостера почтового домена по настройке и обработке писем ограничены, тогда как фильтры МЭ «ИКС» позволяют моделировать множество различных ситуаций, а также вести учет и статистику передаваемых сообщений и много другое. При входе в модуль отображается состояние всех служб почтового сервера и хранилища почты, кнопки «Выключить» (или «Включить» если служба выключена). Также присутствует виджет с выбором основных действий, график статистики почты и ленты почтовика, а также последние события журнала.

На вкладке «Все службы» отображается состояние всех служб почтового сервера, которые есть в МЭ «ИКС», с возможностью выключить (включить) каждую из них. Заголовок каждой службы является ссылкой на соответствующий модуль:

- Fail2ban — блокирует IP-адреса, с которых предпринимается слишком много попыток авторизации;
- Антиспам Rspamd — проверяет письма на спам, добавляет и проверяет DKIM-подпись;
- Антиспам SpamAssassin — проверяет письма на спам;
- Веб-почта — предоставляет веб-доступ к почтовым ящикам МЭ «ИКС»;
- Почтовый сервер — отправляет и получает почту;
- Сборщик почты — получает почту с удаленного почтового сервера;
- Служба DKIM-подписи — добавляет в сообщение цифровую подпись, связанную с доменом, для определения отправителя;
- Хранилище почты — контролирует почтовые домены и ящики.

В закладке «Журнал» находится сводка всех системных сообщений от почтового сервера. Журнал разделен на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены

белым цветом, ошибки - красным. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать в журнале нужные вам записи. Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, выберите нужную дату, используя календарь в левом верхнем углу модуля. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт».

Для настройки почтового сервера необходимо в меню слева выбрать «Настройки». Порт SMTP/POP3/IMAP - позволяет изменить стандартные порты приема и отправки почтовых сообщений. Интерфейсы для SMTP/POP3/IMAP - позволяет выбрать интерфейсы сервера, по которым осуществляется прием и отправка почтовых сообщений. По умолчанию задействованы все интерфейсы.

В соответствующих полях можно изменить стандартные порты приема и отправки почтовых сообщений (SMTP, POP3, IMAP).

Флаг «Включить SMTP через 587 порт» позволяет почтовым клиентам (по умолчанию Mozilla Thunderbird) подключаться к серверу почты МЭ «ИКС» по 587/TCP порту вместо 25.

При установке флага «Автоматически создавать разрешающее правило» в межсетевом экране будет создано разрешающее правило для доступа извне на порты SMTP, POP3 и IMAP. Перейти к списку существующих правил и их настройке можно нажатием на появившуюся гиперссылку «Доступ к почтовому серверу».

В полях «Интерфейсы для SMTP» и «Интерфейсы для POP3/IMAP» можно указать интерфейсы, заданные на МЭ «ИКС», на которых будут работать протоколы SMTP, POP3 и IMAP. По умолчанию работа идет на всех интерфейсах.

В полях «SMTP» и «POP3/IMAP» можно выбрать режим шифрования:

- Почтовый сервер МЭ «ИКС» по умолчанию работает в режиме «Без шифрования» по протоколам SMTP, POP3/IMAP. Поскольку в данном режиме злоумышленники при помощи прослушивания канала могут получить информацию об имени и пароле пользователя, такой режим рекомендуется использовать только в защищенной сети.
- Режим «Необязательное». Если ПО клиента не поддерживает шифрование, пароль передается по незашифрованному каналу, в открытом виде. Если ПО клиента поддерживает шифрование, то авторизация происходит уже внутри шифрованного соединения.
- Режим «С шифрованием». При авторизации пользоваться по протоколам SMTP, POP3/IMAP, STARTTLS пароль передается только внутри шифрованного соединения.

При выборе режимов «Необязательное» либо «С шифрованием» установите следующие параметры:

- «Сертификат для SMTP» — позволяет выбрать сертификат для протокола SMTP из заведенных на МЭ «ИКС». Включает использование шифрованного соединения по методу

STARTTLS поверх использования обычного TCP-соединения по протоколу SMTP на стандартном порту 25. Данное шифрование является компромиссным. Если удаленная сторона не поддерживает шифрование, то письмо будет отправляться (приниматься) по нешифрованному протоколу SMTP.

- «Сертификат для IMAP/POP3» — позволяет выбрать сертификат для протоколов IMAP и POP3 из заведенных на МЭ «ИКС». Включает использование шифрованного соединения по методу STARTTLS поверх использования обычного TCP-соединения по протоколам IMAP и POP3 на стандартных портах 143 и 110 соответственно.
- Флаги «Включить SMTPS» и «Включить POP3S/IMAPS» — позволяют включить шифрование для протоколов SMTPS, IMAPS, POP3S на неклассических портах в параллель 25, 110 и 143 портам. Главным отличием является обязательное использование шифрования, компромисс невозможен. В почтовом сервере МЭ «ИКС» используются только криптографические протоколы TLSv1, TLSv1.1, TLSv1.2. Использование SSL2 и SSL3 для безопасности отключено.
- «Порт SMTPS», «Порт POP3S», «Порт IMAPS» — позволяют задать номера портов для протоколов SMTPS, IMAPS и POP3S соответственно.
- «Длина ключа DH (Diffie-Hellman)» — позволяет установить длину ключа при шифровании методом STARTTLS и для криптографических протоколов TLS различных версий при использовании протоколов IMAP/POP3 и IMAPS/POP3S. Рекомендуемая длинна ключа 2048 бит. По умолчанию установлена длина 1024 бита, это требуется для оптимизации первого запуска МЭ «ИКС».
- Флаг «Автоматически создавать разрешающее правило» — позволяет автоматически создавать в межсетевом экране разрешающее правило.

Для задания различных ограничений при отправке писем можно использовать следующие настройки:

- «Максимальный размер письма» — задает ограничение на загрузку вложений через веб-почту (встроенный клиент Roundcube). Значение устанавливается в мегабайтах;
- флаг «Ограничить частую отправку писем» — включает ограничения на отправку писем через почтовый сервер МЭ «ИКС»;
- «Максимальное количество писем с одного IP-адреса в минуту» — задает величину максимального количества писем, отправляемых за одну минуту, с одного IP-адреса. Данное ограничение не действует на письма, которые отправлены из веб-интерфейса предустановленного клиента электронной почты;

- флаг «Игнорировать при отправке писем с адресов и сетей из белого списка» — создает исключение в ограничении частой отправки писем для IP-адресов и сетей, указанных в блоке «Белый список».

Почтовые сообщения, которые не были отправлены, помещаются в очередь на повторную отправку. Для задания различных интервалов времени при повторной отправке почтовых сообщений можно указать следующие настройки:

- «Интервал между попытками отправки» — позволяет задать время запуска демона, спустя которое демон будет проверять время нахождения письма в очереди (в минутах). По умолчанию установлено 30 минут.
- «Время ожидания в очереди» — позволяет задать интервал времени для письма в очереди, при котором демон попытается повторно отправить данное письмо из очереди (в минутах). По умолчанию установлено от 180 минут до 300 минут.
- Попытки отправить письмо будут повторятся до тех пор, пока общее время нахождения письма в очереди не достигнет значения, указанного в поле «Максимальное время нахождения письма в очереди».
- «Максимальное время нахождения письма в очереди» — позволяет указать максимальное общее время нахождения письма в очереди, по достижении которого отправителю придет уведомление о том, что его письмо не было отправлено (в минутах). По умолчанию установлено 5760 минут.

В МЭ «ИКС» есть возможность настроить отправку исходящей почты через другой SMTP-сервер для всех писем, кроме писем, адресом назначения которых является локальный домен или получатель.

Чтобы включить отправку исходящей почты через другой SMTP-сервер, введите его адрес (доменное имя или IP) в поле «Релей по умолчанию» и задайте порт для подключения.

Флаг «Использовать SMTPS» используется только для соединения по протоколу SMTPS на порту 465. Таким образом, флаг для отправки писем на порт назначения 465 обязателен. При соединении на порт 25 флаг устанавливать не нужно, так как шифрование соединения через расширение STARTTLS будет выбрано автоматически, в зависимости от поддержки данного способа шифрования соединения удаленной стороной.

Если внешний SMTP-сервер требует аутентификацию пользователя, установите флаг «Использовать SMTP-авторизацию» и укажите логин и пароль пользователя.

При отправке почтовых сообщений через SMTP-серверы mail.ru, yandex.ru, gmail.com и др. установите флаг «Подменять адрес отправителя». Это нужно потому, что для данных почтовых серверов необходимо, чтобы адрес отправителя (заголовок FROM) совпадал с пользователем, под которым была выполнена авторизация. В поле «Адрес отправителя» задайте адрес отправителя.

Блок «Список ограничений» позволяет добавить списки белых и черных адресов, с которых разрешена или запрещена входящая корреспонденция.

Белый список добавляется по кнопке «Белый список». В открывшемся окне добавьте пункты списка. Это могут быть IP-адреса, доменные имена, сети (в том числе заведенные в МЭ «ИКС»), почтовые серверы (например, @mail.ru), почтовые ящики. Нажмите «Сохранить».

С указанных адресов МЭ «ИКС» будет всегда принимать почтовые сообщения без проверки серыми списками и без проверки соответствия прямой и обратной записей в DNS, а также без авторизации.

Черный список добавляется по кнопке «Черный список». В открывшемся окне добавьте пункты списка. Это могут быть IP-адреса, доменные имена, сети, почтовые серверы (например, @mail.ru), почтовые ящики. С указанных адресов МЭ «ИКС» не будет принимать почтовые сообщения.

«Домен по умолчанию для авторизации» — позволяет выбрать заведенный в МЭ «ИКС» почтовый домен при авторизации клиента. Например, на МЭ «ИКС» заведен почтовый домен domain.local, а пользователю из данного домена задано имя ящика usermail. Если в данном блоке выбрано значение «domain.local», пользователь при обращении к почтовому серверу МЭ «ИКС» через почтового клиента или через веб-интерфейс в поле «Имя пользователя» сможет указывать только «usermail», а не «usermail@domain.local».

Устанавливать домен по умолчанию для авторизации следует после всех настроек почты, перед началом использования почтового сервера. Смена домена по умолчанию может привести к некоторым проблемам в работе системы. После изменения (удаления) домена по умолчанию рекомендуется очистить базу Roundcube в настройках веб-почты.

«Жесткий диск для хранения почты» — позволяет переместить хранилище почты на отдельный жесткий диск. По умолчанию почта хранится в основном системном разделе (там, где установлен МЭ «ИКС»). При изменении места хранения почты будет произведено копирование всех писем с текущего жесткого диска на новый. Ход копирования почты с диска на диск можно отслеживать в меню Обслуживание > Система > Задачи. Если новый жесткий диск уже содержит файлы с почтой, копирование производиться не будет.

«Имя сервера в команде SMTP HELO при отправке письма» — позволяет задать имя хоста, которое будет передано удаленной стороне при отправке письма в команде SMTP HELO или EHLO.

«При создании ящика автоматически создавать папки» — позволяет задать список стандартных папок, которые будут создаваться в почтовом ящике. При необходимости можно изменить состав.

Антивирусная проверка вложений. Блок включает проверку входящих и исходящих писем на наличие в них вирусов. При положительном результате вместо письма получателю придет

сообщение о результатах проверки, а само письмо будет во вложении к сообщению. Чтобы активировать проверку антивирусом ClamAV либо антивирусом Касперского, установите соответствующий флаг.

DKIM-подпись. В данном блоке выполняются следующие настройки:

- флаг «Проверять DKIM-подпись» — включает проверку входящих писем на наличие и правильность DKIM-подписи. При использовании сборщика почты и релея по умолчанию флаг «Проверять DKIM-подпись» следует убрать;
- флаг «Добавлять DKIM-подпись» — активирует добавление DKIM-подписи в отправленные с МЭ «ИКС» письма;
- «Селектор» — позволяет для каждого почтового сервера в одном домене создавать свой DKIM-селектор. Это нужно потому, что для одного домена может быть несколько почтовых серверов. По умолчанию в МЭ «ИКС» используется селектор default.

Следующий блок содержит флаги:

- «Перекодировать тему в UTF-8» — если флаг установлен, письма, которые отправляются с почтового сервера МЭ «ИКС», будут иметь кодировку темы письма UTF-8.
- «Поддержка SMTPUTF8» — включает (выключает) поддержку кодировки UTF-8 при приеме и отправке писем.

Вкладка «Защита от спама» предназначена для настройки серверов, содержащих черные списки, а также режима работы серого списка в МЭ «ИКС».

Черные списки DNSBL. Блок позволяет добавить либо удалить хосты, содержащие черные списки DNSBL. Данные списки используются для борьбы со спамом. Сформируйте список при помощи кнопок «Добавить» и «Удалить».

Серые списки (greylisting). Блок предназначен для установки автоматической блокировки спама. При установке флага «Использовать серые списки» МЭ «ИКС» будет отслеживать поведение почтовых серверов, которые отправляют письма на МЭ «ИКС». О методологии блокировки можно прочитать здесь. Настройка серых списков происходит по трем параметрам, которые регулируются в соответствующих полях:

- «Игнорировать повторную отправку» — время, за которое достоверный почтовый сервер не отправит письмо повторно (в секундах);
- «Ожидать повторной отправки» — время, не позже которого должно прийти письмо (в часах). Если указанное время прошло, осуществляется повторная отправка;
- «Хранить в белом списке» — количество дней, когда сервер, уже прошедший проверку, не будет подвержен проверке снова (в днях).

Вкладка «Адресная книга» определяет параметры адресной книги почтового сервера. Здесь можно определить порт передачи данных, а также включить или выключить использование адресной книги в веб-интерфейсе Roundcube.

Прежде чем добавлять пользовательские почтовые ящики, необходимо создать почтовый домен. Перейдите во вкладку «Домены и ящики» и нажмите кнопку «Добавить» → «почтовый домен». Вы можете назвать домен любым несуществующим именем, если обмен письмами будет происходить внутри корпоративной сети, либо настроить пересылку сообщений на реально существующем домене, зарегистрированном за вашей организацией. Если установлен в настройках флажок «Создавать DKIM-подпись», то она добавится автоматически. При повторном двойном клике на созданном аккаунте он откроется уже с созданным DKIM-ключом, который при необходимости можно скопировать. После этого, выделив созданный домен, вы можете добавлять в него пользовательские почтовые ящики. Сервер попросит вас ввести имя ящика, пароль и выбрать пользователя, за которым данный ящик будет закреплен. При необходимости вы можете указать квоту - максимально зарезервированное место на жестком диске МЭ «ИКС» для хранения писем данного пользователя. После превышения этой квоты письма для пользователя приниматься не будут. По умолчанию квота отсутствует. Не обязательно создавать отдельный почтовый ящик для каждого необходимого вам почтового имени. Вместо этого вы можете создать ссылку на указанный ящик. Тогда все письма, приходящие на ящик, например, preved@up4k.loc, будут перенаправляться на реально существующий ящик medved@up4k.loc.

Стоит отметить, что при создании почтовых доменов и ящиков соответствующие домены и аккаунты появляются в разделе Jabber-сервер. Верно и обратное.

Почтовый домен с перенаправлением (почтовый релей). Почтовый сервер МЭ «ИКС» может выступать в качестве почтового шлюза (релея), который будет «через себя» ретранслировать сообщения электронной почты, предназначенные для определенных доменов, другому (внутреннему) почтовому серверу. По сути, это почтовый сервер, который соединяет логически разделенные сети. Почтовый шлюз МЭ «ИКС», работая в качестве почтового релея, так же проверяет проходящие через него сообщения на вирусы и спам. Для того чтобы добавить домен на МЭ «ИКС», конечным получателем для которого является другой почтовый сервер, необходимо добавить «Домен с перенаправлением» на вкладке «домены и ящики». Например, если необходимо доставлять почту для домена @a-real.local на почтовый сервер 192.168.17.251, необходимо настроить домен с перенаправлением следующим образом: имя домена – a-real.local; Имя хоста для перенаправления – 192.168.17.251.

Почтовый ящик. При создании почтового ящика указываются его имя и имя домена, пароль, выбирается пользователь, за которым будет закреплен данный ящик. Также можно указать квоту (максимально зарезервированное место на жестком диске МЭ «ИКС» для хранения писем данного

почтового ящика). Почтовые ящики также можно просматривать на вкладке «Почта и телефония» в индивидуальном модуле пользователя. Для перехода к индивидуальному модулю просто нажмите на имя пользователя.

Также в модуле можно добавить ссылку на почтовый ящик, вручную удалять и пересылать письма, загружать или скачивать письма и управлять синхронизированными ящиками.

Стоит отметить, что, принимая почту для несуществующего адресата на внутреннем почтовом сервере, МЭ «ИКС» принимает на себя ответственность за уведомление отправителя в случае невозможности доставки сообщения. Тем самым «загрязняется» почтовая очередь с сообщениями, если отправитель этих писем недоступен. Для того чтобы почтовый домен был доступен из внешней сети и мог обмениваться данными с другими внешними серверами, необходима настройка DNS-записей. После того, как почтовые ящики для пользователей созданы, они могут подключаться к МЭ «ИКС» с помощью почтовых клиентов (например, Mozilla Thunderbird или Microsoft Outlook) или воспользоваться веб-интерфейсом для почты.

Почтовые фильтры. Для обработки отправляемых и получаемых писем используется вкладка «Фильтры». Они обрабатывают почту по следующим условиям: размер, отправитель, получатель, тема. Условие может быть строгое и нестрогое. Количество условий может быть любым, при этом фильтр может обрабатывать почту как при полном совпадении всех условий, так и при первом совпадении. После совпадения условия фильтр может удалить письмо, переместить его в другой ящик или сделать копию. В приведенном выше примере все письма, приходящие на один адрес, размер которых больше 5000 кБ, и тема письма содержит выражение «не спам» будут копироваться на другой почтовый ящик МЭ «ИКС». Для того чтобы создать новый фильтр, сперва необходимо выбрать условия срабатывания - при совпадении всех условий, любого из условий или применить ко всем сообщениям независимо от условий. Фильтровать входящие и исходящие письма вы можете по теме письма, отправителю, получателю и размеру (в килобайтах). Проверка на совпадение условия может быть строгая («совпадает с») или не строгая («содержит», «начинается с», «заканчивается на»), а также обратная («не содержит»). Вы можете назначить любое количество условий для одного фильтра. Последний шаг - выбор действия, происходящего после срабатывания фильтра. Вы можете переместить письмо, скопировать его на другой адрес либо удалить. Первые два условия позволяют вписать имя почтового ящика либо выбрать его из списка созданных на МЭ «ИКС».

Рассылки - это те же фильтры, но с упрощенным интерфейсом, в котором достаточно указать те ящики, на которые будет распространена рассылка. Ящик, на который приходит письмо-оригинал в системе не должен быть заведен, поскольку он представляет собой ссылку.

Сборщик почты. Для управления почтовыми аккаунтами, расположенными на других серверах, вы можете применить функцию МЭ «ИКС» «сборщик почты». С его помощью МЭ «ИКС»

подключается к указанному почтовому серверу под выбранным логином и паролем и перемещает либо копирует содержащуюся почту на почтовые ящики пользователей МЭ «ИКС». Вы можете указать, что делать с письмами на сервере - собирать все, собирать только новые, оставлять письма на сервере или удалять их. Также настраивается интервал работы сборщика и число загружаемых писем за сессию. Он работает в двух режимах - автоматическое определение получателя и указание почтового ящика для сборки. Автоматическое определение работает в том случае, если организация имеет один внешний ящик, расположенный на сервере провайдера, а остальные ящики служат его псевдонимами. В остальных случаях используется прямое указание ящика сборки. То есть, в большинстве случаев при создании сборщика, необходимо поставить переключатель в положение «Пересылать на». Сборщик почты может также использоваться в тех случаях, когда в организации применяется метод так называемой «мультидропной» почты. Он состоит в том, что вся почта приходит на сервер провайдера или хостера и хранится там без разделения на почтовые ящики пользователей. В таком случае, при настройке сборщика почты, поле «получатель» изменять не нужно (значение по умолчанию в нем - адрес получателя). Таким образом, собранные письма будут автоматически распределяться в зависимости от адресата по ящикам пользователей МЭ «ИКС», а в случае отсутствия таких адресатов - складываться в почтовом ящике, выбранном по умолчанию.

Антиспам SpamAssassin. Предназначен для защиты от спама. Если служба определит, что письмо является спамом, она изменит тему письма. Данный модуль расположен в меню Почта - Антиспам SpamAssassin. На странице модуля отображаются сведения об антиспаме SpamAssassin: состояние службы, кнопки «Включить»/«Выключить», настройки службы. Чтобы активировать работу службы, установите флаг «Проверять почту». В поле «Количество баллов, при котором письмо считается спамом» можно задать порог, при котором служба будет считать письмо спамом. Если установить значение 0, все письма будут являться спамом. Кнопка «Обновить базы сейчас» запускает немедленную проверку актуальности баз антиспама и в случае необходимости обновляет их. Журнал событий данного модуля можно посмотреть в меню Обслуживание - Журнал и уведомления - Системный журнал. Выберите журнал «Антиспам SpamAssassin».

Антиспам Rspamd. Предназначен для защиты от спама. Если служба определит, что письмо является спамом, она изменит тему письма либо отклонит письмо. Данный модуль расположен в меню Почта - Антиспам Rspamd. На странице модуля отображаются сведения об антиспаме SpamAssassin: состояние службы, кнопки «Включить»/«Выключить», настройки службы. Чтобы активировать работу службы, установите флаг «Проверять почту». В поле «Количество баллов, при котором в письмо добавляется заголовок SPAM» можно задать порог, при котором служба будет считать письмо спамом. При этом тема письма будет изменена. Если установить значение 0, все письма будут являться спамом. В поле «Количество баллов, при котором письмо отклоняется» можно задать порог, при котором служба будет считать письмо спамом. При этом письмо будет

отклонено. Если установить значение 0, все письма будут являться спамом. Флаг «Включить проверку SPF» включает дополнительную проверку SPF. Флаг «Включить проверку SURBL» включает дополнительную проверку SURBL. В поле «Пропускать проверку писем из сетей» можно указать сети, письма которых не будут подлежать проверкам антиспама.

Антиспам Касперского. Предназначен для защиты от спама. Антиспам проверяет входящие и исходящие почтовые сообщения и сортирует их в соответствии с установленными параметрами. Открыть модуль можно в меню Почта – Антиспам Касперского либо в меню Защита – Антиспам Касперского. Служба «Антиспам Касперского» отвечает за работоспособность предустановленного Антиспама Касперского, который проверяет почтовые письма. На данной вкладке отображаются следующие сведения о службе: статус службы, кнопки «Включить»/«Выключить», виджет с информацией о службе: текущие версии базы данных и антиспама Касперского, дата истечения лицензии, журнал последних событий. Вкладка «Настройки» предназначена для установки параметров работы службы. Кнопка «Менеджер лицензий» позволяет загружать и просматривать сведения о файле лицензии программы. При установке флага «Перенаправлять спам в папку СПАМ» включится автоматическое перенаправление писем, содержащих спам, в соответствующую папку. Если флаг не установлен, письмам только будет добавляться слово «СПАМ» в тему. В поле «Проверять обновления баз антиспама» можно выбрать период обновления баз антиспама. По умолчанию установлен период каждые 5 минут. При необходимости можно изменить время ожидания ответа (в секундах). По умолчанию установлено значение 6000 секунд. При помощи следующих флагов устанавливаются параметры проверки писем на спам. Также на данной вкладке можно настроить вручную белые и черные списки IP-адресов, почтовых доменов и ключевых фраз, содержащихся в сообщении. Чтобы внести пункт списка, нажмите кнопку «Добавить» и введите нужное значение. В закладке «Журнал» находится сводка всех системных сообщений от служб антивируса. Журнал разделен на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, ошибки - красным. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать в журнале нужные вам записи. Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, выберите нужную дату, используя календарь в левом верхнем углу модуля. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт».

Статистика и очередь. Для контроля входящего и исходящего почтового трафика, а также спама и нежелательных писем вы можете воспользоваться разделом «Статистика». Также, как и в пользовательской статистике, вы можете применять различные фильтры на панели управления к общим сведениям о почтовом трафике МЭ «ИКС» и выводить их в виде таблицы. Столбцы таблицы

варьируются в зависимости от применяемого фильтра. Генератор отчетов выглядит во многом похожим на пользовательскую статистику. Основные фильтры могут выводить информацию о трафике пользователей, группируя по следующим признакам:

- по доменам отправителя;
- по доменам получателя;
- по почтовым ящикам;
- по часам/дням/месяцам;
- детализация писем.

Во вкладке «Почтовая очередь» показаны письма, ожидающие отправки, или которые по каким-то причинам не были отправлены (к примеру, отклонены серым списком вышестоящего почтового сервера). При выборе любого объекта из списка можно увидеть код ошибки, по которой он не был доставлен. Управлять почтовой очередью можно посредством кнопок «Очистить очередь» и «Отправить все». Также, каждое письмо можно попытаться отправить индивидуально или удалить его из очереди.

5.2.8. Сертификаты

SSL (Secure Sockets Layer — уровень защищенных сокетов) — криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером. Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причем для шифрования используется асимметричный алгоритм с открытым ключом. При шифровании с открытым ключом используется два ключа, причем любой из них может использоваться для шифрования сообщения. Тем самым, если используется один ключ для шифрования, то соответственно для расшифровки нужно использовать другой ключ. В такой ситуации можно получать защищенные сообщения, публикуя открытый ключ, и храня в тайне секретный ключ. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат. Цифровой сертификат — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов. Реализация происходит следующим образом:

1) Клиент инициирует соединение;
2) В ответ сервер посылает цифровой идентификатор (сертификат). Если требуется аутентификация клиента, то сервер может запросить ответный сертификат;
3) Клиент сверяет идентификатор сервера, при необходимости отправляя свой;
4) После завершения процесса аутентификации клиент передает серверу ключ сессии, зашифрованный при помощи открытого ключа сервера;

5) На основе сгенерированного ключа устанавливается защищенное соединение и происходит передача данных между клиентом и сервером;

Настройка и хранение всех сертификатов происходит в МЭ «ИКС» в меню «Защита» - «Сертификаты». Как обычно, список сертификатов представлен в виде дерева, а поле модуля поделено на столбцы, в которых показана основная информация о сертификатах: тип ключа родительского сертификата, дата начала действия и окончания, а также имя хоста (или IP-адрес), который представляет данный сертификат. Вы также можете экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт», а также просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата». Для того чтобы в списке были показаны и отозванные сертификаты, установите флаг «Показать отозванные сертификаты».

Чтобы создать новый SSL-сертификат, нажмите «Добавить». Сначала заполняются данные сертификата: наименование, код страны, местоположение, сведения об организации, имя хоста или IP-адрес. Затем во вкладке «Настройки» определяется роль сертификата - CA (корневой) или конечный, устанавливается метод шифрования, срок действия и длина ключа в битах. Стоит обратить внимания на то, что первоначально всегда должен создаваться корневой сертификат, затем - дочерние конечные сертификаты! К службам МЭ «ИКС» (кроме SSL-фильтрации), применяются только конечные сертификаты. Будьте внимательны: неверное применение сертификата к службам может сделать их недоступными для пользователя! После этого перейдите во вкладку «Использование ключа» и выберите в списке необходимый шаблон использования. Выбор шаблона автоматически установит флажки параметров сертификата применительно к выбранной роли. Если вы опытный системный администратор, вы можете установить флажки вручную. Вкладка «Netscape расширение» позволяет установить дополнительные netscape-расширения для сертификата. После нажатия кнопки «Добавить» МЭ «ИКС» предложит зашифровать ключ паролем. Введите пароль или откажитесь от его использования. Для служб МЭ «ИКС» всегда применяются только нешифрованные сертификаты.

При необходимости использовать доверенные сертификаты, подписанные центром сертификации, следует добавлять сертификаты в следующем порядке: сначала все промежуточные сертификаты (Intermediate Certificate), а затем корневой сертификат (Root Certificate). Для добавления каждого сертификата нажмите кнопку «Добавить», выберите файл сертификата (промежуточного или корневого). При необходимости можно удалить поле для выбора сертификата, нажав на соответствующую кнопку.

5.2.9. Телефония

VoIP — система связи, передающая аудио-сигнал по IP-сетям. Сигнал по каналу связи передается в цифровом виде и, как правило, перед передачей преобразовывается с целью удаления избыточности. За обработку VoIP-данных в МЭ «ИКС» отвечает модуль «Телефония», разработанный на базе сервера IP-телефонии Asterisk. Это свободное решение компьютерной телефонии с открытым исходным кодом, оно достаточно надежное и давно зарекомендовавшее себя с положительной стороны. В настоящее время модуль поддерживает передачу данных по протоколам SIP и IAX. Настройка и управление данным модулем находятся в меню слева «Телефония». При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить», если модуль выключен) и последние сообщения в журнале. Стоит отметить, что если модуль находится в состоянии «не настроен», то необходимо настроить DNS-зону в МЭ «ИКС» таким образом, чтобы имя системы в модуле Система резолвилось в IP-адрес МЭ «ИКС».

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

Раздел «Телефонные номера» отображает список телефонных номеров, зарегистрированных на АТС. В ней вы можете создать следующие объекты: телефонный номер, факс, группа номеров, конференция.

Телефонный номер. Имеет следующие параметры: собственно, номер, краткое описание, пароль, задаваемый при необходимости и пользователь, к которому данный номер привязан в общей книге. Дополнительно можно указать время ожидания для данного номера (по умолчанию оно определяется в настройках) и число каналов, которые номер может использовать. Флажок «Разрешать подключаться извне» позволяет определить, будет ли доступен номер для подключения из внешних сетей. Кроме того, вы можете указать почтовый адрес пользователя, на который будут отправляться сообщения его голосовой почты. Стоит отметить, что если вы указали флажок «Разрешить подключаться извне» для телефонного номера, то рекомендуется установить сложный пароль для того, чтобы он не был подобран злоумышленниками. Также при создании телефонного

номера можно указать, как будет осуществляться доступ (SIP-клиент либо Xphone) и какие кодеки использовать для номера.

Факс позволяет принимать факсы на указанный номер и сохранять их в формате TIFF в папке Хранилища файлов.

Группа номеров - предназначена для объединения телефонных номеров в группы, которые можно применять как объекты в правилах.

Конференция - создает телефонный номер, позвонив на который, каждый абонент будет слышать всех абонентов, также позвонивших на этот номер.

Вкладка «Настройки». На вкладке можно изменить настройки портов SIP (через UDP) и IAX, а также диапазон портов для входящих соединений RTP. При установке флага «Автоматически создавать разрешающее правило» в межсетевом экране добавится разрешающее правило для указанных портов. Перейти к правилу можно нажатием на ссылку в его названии. Флаг «TCP для SIP» включает поддержку отправки и получения SIP-пакетов по протоколу TCP на выбранном порту. Включите данную опцию, если у вас используются внешние или внутренние номера, которые настроены для работы через тип подключения «Без Шифрования (TCP)». При установке флага «Автоматически создавать разрешающее правило» в межсетевом экране добавится разрешающее правило для указанного порта. Перейти к правилу можно нажатием на ссылку в его названии. В поле «Сертификат для шифрования (TLS и SRTP)» можно выбрать, изменить или удалить сертификат шифрования для телефонии. По умолчанию выбран автоматически сгенерированный конечный сертификат (самоподписанный). После выбора сертификата активируются обязательные поля «Версия TLS» и «Порт для SIP через TLS». Порт для SIP через TLS по умолчанию установлен 5061, но его можно изменить. Поле «Версия TLS» предназначено для выбора версии шифрования (TLS 1.0, 1.1, 1.2) и доступно только при использовании драйвера канала chan_pjsip. Для драйвера chan_sip может быть использована только версия TLS 1.0. При установке флага «Автоматически создавать разрешающее правило» в межсетевом экране добавится разрешающее правило для указанного порта. Перейти к правилу можно нажатием на ссылку в его названии. В блоке «Драйвер канала SIP» можно выбрать модуль реализации протокола SIP, который будет использоваться сервером телефонии МЭ «ИКС». Доступно два канальных драйвера: chan_sip и chan_pjsip. Chan_pjsip — это более новый канальный драйвер канала SIP в Asterisk. При переключении на данный драйвер часть настроек IP-телефонии поменяется. Отличия в настройке внешних каналов: а) опции insecure, canreinvite и строка регистрации доступны только для модуля chan_sip; б) опция direct_media доступна только для модуля chan_pjsip. Эта опция определяет, могут ли медиаданные передаваться напрямую между конечными точками. Если нет (no), то все RTP-потоки проходят через Asterisk. Отличия в общих настройках телефонии: опция SRV lookup доступна только для модуля chan_sip. Конференции с режимом распределения видео SFU и Xphone работают только на

канальном драйвере pjsip. Поле «Время ожидания ответа» позволяет задать период времени, по истечении которого сервер телефонии посчитает абонента не ответившим на звонок и переведет звонящего абонента в следующий набор правил (в секундах). По умолчанию установлен период 30 секунд. Некоторые правила телефонии позволяют переопределить это время для конкретного правила. Данная настройка общая. Если требуется, чтобы время ожидания ответа отличалось от стандартного для конкретных внутренних номеров, то у каждого внутреннего добавочного номера можно переопределить эту опцию. При установке флага «Использовать BLF» включится поддержка функции Busy Lamp Field, позволяющая в реальном времени отслеживать состояния абонентов АТС (занят/свободен). Важно: конечное устройство должно поддерживать данную функцию. Флаг «SRV lookup» активирует DNS-поиск SRV-записей. Данный флаг недоступен при выборе chan_pjsip в качестве драйвера канала SIP. Чтобы включить голосовую почту, установите флаг «Использовать голосовую почту». При помощи соответствующих флагов можно установить перенаправление на голосовую почту при неответе и (или) отправление сообщения голосовой почты на e-mail. Данный e-mail указывается в настройках внутренних номеров. Если требуется, измените номер для голосовой почты. По умолчанию установлен номер *100. Чтобы прослушать оставленное на внутреннем номере голосовое сообщение, позвоните с него на номер голосовой почты. В настройках также можно установить номера для: а) безусловной переадресации — позволяет перевести входящий звонок без подтверждения; б) обычной переадресации — позволяет перевести входящий звонок, предназначенный одному абоненту, на другого абонента, пока происходит звонок. Для этого необходимо набрать номер для переадресации, а затем номер другого абонента, дождаться ответа второго абонента и затем положить трубку у себя. Перехват в рамках группы предназначен для ответа на входящий звонок, предназначенный одному абоненту, другим абонентом, пока происходит звонок и трубка не снята. Это удобно в том случае, если второй абонент видит, что первого нет на месте. Чтобы перехватить вызов, предназначенный другому абоненту, необходимо ввести во время звонка специальную комбинацию клавиш (по умолчанию это *8). Комбинацию можно изменить в поле «Номер для перехвата». Направленный перехват звонков предназначен для перехвата входящего звонка на конкретный внутренний номер вне зависимости от группы внутренних номеров. Чтобы перехватить вызов, предназначенный другому абоненту, на своем телефоне необходимо ввести во время звонка специальную комбинацию (по умолчанию **) и внутренний номер вызываемого абонента. Комбинацию клавиш для направленного перехвата вызова можно изменить в поле «Номер для направленного перехвата». В блоке «Факсы» задаются настройки работы с факсимильными сообщениями. При установке флага «Поддержка T38» включится поддержка стандарта T.38 для передачи факсимильных сообщений. В поле «Обнаружение ошибок» можно выбрать тип корректировки входящих сообщений: а) «Redundancy» (Redundancy error correction) — исправление ошибок избыточности; б) «FEC» (Forward error

correction) — прямое исправление ошибок; в) «Не задано» — не проверять сообщения на наличие ошибок. Поле «Максимальный размер пакета» позволяет определить максимальный размер сообщения. Флаг «Конвертировать принятые факсы в PDF» предназначен для определения формата файлов (возможность конвертировать файлы в PDF-формат). По умолчанию все факсимильные сообщения будут иметь формат .tiff. Блок «NAT» отвечает за настройку поведения модуля телефонии, если он находится за NAT. Флаг «Использовать NAT (ICS за NAT)» включает преобразование IP-адресов внутри пакетов телефонии. Для корректной работы данного блока необходимо указать внутренние локальные сети и внешний IP-адрес. В поле «Внешний общий IP-адрес» укажите внешний IP-адрес, который используется для преобразования IP-адресов в обработке SIP (если пункт назначения SIP-сообщений находится за пределами IP-сети, определенной в поле «Локальные сети»). Таким образом все указанные в данном поле сети сервер телефонии будет считать локальными, для них не будут применяться правила преобразования IP-адресов внутри пакетов IP-телефонии. Блок «Почтовый сервер» отвечает за настройку пересылки факсов, уведомлений и сообщений голосовой почты. Выберите, какой сервер будет использоваться для отправки писем: а) почтовый сервер МЭ «ИКС» — в поле «Адрес отправителя» укажите один из почтовых адресов, созданных в МЭ «ИКС»; б) внешний SMTP-сервер — заполните поля «SMTP-сервер», «Порт», «Логин», «Пароль» и «Адрес отправителя», а также при необходимости установите флаг «SSL». В блоке «Кодеки» можно выбрать заданные по умолчанию кодеки, которые будут использоваться модулем телефонии для всех номеров. В столбце «Использовать» расположены кодеки, которые используются всеми номерами, если не задано иное в настройках отдельных номеров. Порядок следования кодеков в данном столбце имеет следующее значение: чем выше расположен кодек, тем выше его приоритет. Список кодеков будет представлен удаленной стороне во время установления сеанса связи в порядке их следования в данном списке. В столбце «Доступные кодеки» расположены доступные, но не используемые модулем телефонии кодеки. В блоке «Мелодия при удержании вызова» можно задать мелодию, которая будет воспроизводиться звонящему при удержании вызова. Для загрузки мелодии нажмите кнопку «Загрузить новую мелодию» и выберите аудиофайл. После загрузки мелодию можно прослушать или удалить с помощью соответствующих кнопок.

Внешние каналы. Система позволяет обмениваться звонками между сотрудниками организации внутри сети без каких-либо дополнительных настроек. Для того чтобы настроить входящие и исходящие звонки во внешнюю сеть, необходимо добавить хотя бы один внешний канал связи. В текущей версии поддерживаются два вида каналов - SIP и IAX и аналогично два вида туннелей. Туннели — это те же провайдеры, но служат обычно для упрощенного соединения между двумя МЭ «ИКС». Чтобы настроить новый канал, нажмите кнопку «Добавить». Провайдер SIP позволяет настроить сервер подключения, телефонный номер, при необходимости указать логин и

пароль. Флажок «Автоматически создавать правило», используя префикс, служит для указания префикса внешнего звонка по умолчанию. Данный префикс представляет собой цифру, по которой модуль ориентируется, направлять ли звонок во внешнюю сеть. Например, звонок на номер 555-3333 при указанном префиксе 9 будет набираться клиентом как 9-555-3333. Опции режим DTMF, insecure, canreinvite позволяют настроить режимы тонального набора. Если провайдер имеет специфические настройки, то вы можете полностью прописать строку регистрации, установив соответствующий флажок.

Важно: в некоторых случаях провайдер SIP-телефонии не может распознать абонента, набирающего внешний вызов. Если при регистрации провайдера у вас работают входящие звонки, но не проходят исходящие, то в поле fromUser необходимо указать номер телефона либо логин подключения (в зависимости от особенностей провайдера).

Параметр «Поддерживать подключение» указывает, доступно ли удаленное устройство для совершения вызовов. Asterisk периодически будет отправлять SIP сообщение типа OPTIONS, для проверки доступности. Если данное устройство, не ответит в течении заданного периода (или периода по умолчанию в 2000 мс) в миллисекундах, тогда Asterisk рассматривает это устройство как выключенное и недоступное для совершения вызовов. Данная опция используется только если телефония стоит за NAT.

IAX2 (Inter-Asterisk eXchange protocol) — протокол обмена VoIP данными между IP-PBX Asterisk. Наиболее приспособлен к трансляции сетевых адресов NAT, в отличие от SIP и H.323 использует только один порт 4569 протокола UDP для сигнализации и медиапотока. Аналогично провайдеру SIP, провайдер IAX в качестве параметров запрашивает сервер подключения, телефонный номер, при необходимости логин и пароль и внешний префикс. Опция, отличная от настроек провайдера SIP - режим работы. Если вы используете канал связи для подключения к внешнему серверу провайдера, то необходимо использовать опцию «клиент». В случае, когда к МЭ «ИКС» подключаются другие клиенты по внешнему каналу, используйте опцию «сервер».

Туннели в целом аналогичны соответствующим провайдерам, в них спрятаны лишние опции, которые не требуются для настройки. Один из МЭ «ИКС» выбирается сервером, а второй клиентом. Остальная настройка их аналогична настройке провайдера SIP или IAX.

Правила. Для управления входящими и исходящими звонками предназначена вкладка меню «Правила». Все звонки по умолчанию разделены на внешние и внутренние. При необходимости вы можете добавить новый набор правил и добавить к нему необходимые правила. Правила подразделяются на следующие элементы:

- принять вызов - автоматически принимает звонки на все известные номера;
- повесить трубку - отключает звонящего абонента, если он совпадает с указанными условиями;

- ждать набора номера - включает ожидание в течение указанного промежутка времени, пока абонент не наберет номер полностью. Это делается для предотвращения быстрого звонка на внутренний номер, который совпадает с началом внешнего номера;
- перенаправить вызов. Если входящий или исходящий абонент совпадает с указанными условиями, то он перенаправляется на номер или набор правил, в соответствии с которым обрабатывается звонок;
- преобразовать номер - изменяет номер звонящего или набранный номер при совпадении с условиями набора;
- звонок через внешний канал - отправляет звонок, подходящий под заданные условия, через выбранного внешнего провайдера связи.

Перенаправления. Перенаправления служат для организации вызова на указанный внешний номер, если абонент не отвечает или занят.

Очереди. Вы можете использовать очереди для равномерной нагрузки на абонентов и удержания звонка до первого освободившегося номера. Очередь подразумевает выбор одной из трех стратегий - звонить всем, звонить по очереди, звонить с наименьшей нагрузкой.

На вкладке меню «Журнал звонков» перечислены все входящие и исходящие звонки в систему, в том числе перенаправленные и неотвеченные. Также вы можете прослушать и скачать в виде аудиофайла записанный звонок, если включена опция записи в настройках модуля.

5.2.10. VPN

VPN - виртуальная частная сеть, позволяющая объединить в единую сеть пользователей, физически находящихся в различных местах. Кроме того, с помощью VPN можно организовать выход компьютеров локальной сети к сети Интернет по логину/паролю. Для настройки VPN необходимо перейти в меню слева «Сеть» - «VPN».

Обычно VPN используется для организации удаленного доступа к локальной сети: например, в тех случаях, когда пользователю требуется получить доступ к внутренним ресурсам сети предприятия пока он находится в командировке или отпуске.

Создание VPN-сети. Для того чтобы начать работу с VPN, необходимо создать виртуальную подсеть, в которой будут появляться VPN-пользователи после подключения. Для этого необходимо перейти в раздел «Провайдеры и сети» и выбрать пункт «Добавить» - «VPN-сеть».

Необходимо указать диапазон адресов для VPN-сети в формате IP-адрес VPN-интерфейса/маска. Адреса из этого диапазона будут выдаваться пользователям, подключающимся через VPN. Затем выбрать доступные для подключения протоколы - PPTP, L2TP или L2TP+IPsec. Для предоставления пользователям доступа в сеть Интернет посредством PPPoE необходимо выбрать опцию «PPPoE» и указать сетевой интерфейс, который подключен к сети с

пользовательскими компьютерами. В том случае, если в вашей сети находится несколько PPPoE-серверов, вы можете идентифицировать сервер МЭ «ИКС» при помощи поля «Имя сервиса», задав в нем произвольное имя. По кнопке «Скачать файл автоматической настройки» можно скачать файл с расширением .ps1, который предназначен для запуска в PowerShell.

Чтобы сразу перейти к списку пользователей, разрешенных для подключения, нажмите кнопку «Настройки авторизации» на панели созданной VPN-сети.

Настройка пользователя. Для того чтобы пользователь мог подключиться к серверу по VPN, необходимо отметить его флажком в списке пользователей в меню VPN - Пользователи. Также нужно указать ему логин и пароль для подключения. Если пользователь всегда должен получать один и тот же IP-адрес, можно присвоить ему адрес из диапазона VPN-сети во вкладке пользователя «IP-адреса». Этот адрес будет назначаться пользователю при подключении, в противном случае пользователю будет выдаваться первый свободный адрес из VPN-диапазона. Назначение адреса вручную удобно в том случае, если пользователь при подключении не использует МЭ «ИКС» как удаленный шлюз. В таком случае клиенту можно прописать статический маршрут до сетей МЭ «ИКС».

Вкладка «Настройки» предназначена для настройки VPN-сервера. Здесь доступны следующие флаги:

- «Разрешать одновременные подключения под одним пользователем» — позволяет подключаться по VPN разным устройствам под логином и паролем одного пользователя;
- «Авторизовать доменных пользователей через Kerberos» — при установке флага авторизация доменных пользователей происходит только через Kerberos, для пользователей МЭ «ИКС» все остается без изменений. Если флаг установлен, необходимо: 1) настроить Kerberos; 2) доменный пользователь должен подключаться по L2TP с IPSec, в настройках подключения у пользователя должна быть выбрана проверка подлинности PAP (протоколы CHAP и MS-CHAPv2 рекомендуется отключить);
- «Автоматически создавать разрешающее правило» — предоставляет доступ к VPN-серверу из внешней сети. По ссылке на экране можно перейти к правилам межсетевого экрана;
- «Автоматически создавать разрешающее правило OpenVPN» — предоставляет доступ к OpenVPN-сетям. По ссылке на экране можно перейти к правилам межсетевого экрана.

При необходимости можно изменить время ожидания сессии. Это время разрыва сессии в случае неактивности пользователя (в секундах). По умолчанию установлено значение 60 секунд. Если требуется, измените время ожидания ответа от RADIUS (в секундах). По умолчанию установлено значение 3 секунды.

Настройка пользователя. Для того чтобы пользователь мог подключиться к серверу по VPN, необходимо отметить его флажком в списке пользователей в меню VPN - Пользователи. Также

нужно указать ему логин и пароль для подключения. Если пользователь всегда должен получать один и тот же IP-адрес, можно присвоить ему адрес из диапазона VPN-сети во вкладке пользователя «IP-адреса». Этот адрес будет назначаться пользователю при подключении, в противном случае пользователю будет выдаваться первый свободный адрес из VPN-диапазона. Назначение адреса вручную удобно в том случае, если пользователь при подключении не использует МЭ «ИКС» как удаленный шлюз. В таком случае клиенту можно прописать статический маршрут до сетей МЭ «ИКС».

На вкладке «Текущие сеансы» можно посмотреть, какие пользователи подключены в настоящее время, время подключения, а также при необходимости отключить пользователя. В списке отображаются IP-адреса VPN-соединений, тип VPN-соединения и имя пользователя, для которого это соединение создано. При выборе пользователя отображаются: время подключения — время установления данного соединения; длительность подключения; IP-адрес и способ его выдачи; IP-адрес и порт, с которого осуществляется соединение; кнопка «Прервать соединение» для отключения пользователя.

На вкладке «События» можно посмотреть информацию о пользователях. Например, какой пользователь был подключен, с какого адреса и какой адрес получил, а также информацию об отключении пользователя. Вкладка разделена на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать нужные вам записи. Вкладка всегда отображает события за текущую дату. Чтобы посмотреть события за другой день или иной промежуток времени, выберите нужные даты, используя календарь в левом верхнем углу модуля. В правой части верхней панели выпадающее меню «Сообщения» позволяет отфильтровать список событий по выбранному критерию: системные сообщения, сервисные сообщения, ошибки, остальные сообщения.

На вкладке «Журнал» отображается сводка всех системных сообщений служб VPN-сервера с указанием даты и времени. По умолчанию в журнале отображаются сообщения службы PPP-соединений. Чтобы переключить сводку на OpenVPN, нажмите на соответствующую кнопку и выберите нужную службу. Журнал разделен на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя и т.д.) - зеленым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать в журнале нужные вам записи. Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, выберите

нужную дату, используя календарь в левом верхнем углу модуля. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт».

Настройка межсетевого экрана. Для того чтобы удаленные пользователи могли подключаться к МЭ «ИКС» через PPTP VPN, необходимо чтобы в межсетевом экране были разрешены правила «Доступ к VPN-серверу» (разрешены входящие соединения на порт 1723) и «Доступ к серверу через GRE-туннели» (разрешен GRE-трафик).

5.2.11. Маршруты

Маршруты используются для настройки маршрутизации между сегментами сети и для перенаправления трафика на различных провайдеров. Для настройки маршрутов необходимо перейти в меню слева «Сеть» - «Маршруты».

Маршрут может направлять трафик через заданный шлюз, через сетевой интерфейс или через провайдера. Маршрут через интерфейс обычно используется для различных туннельных соединений. Маршрут через шлюз используется для маршрутизации в обычных ethernet-сетях.

Ассиметричная маршрутизация. В случае, когда источник (пользователь) и шлюз находятся в одной подсети, при создании маршрута необходимо установить флажок «Не обрабатывать трафик межсетевым экраном». В приведенном выше примере Пользователь 1 находится в сети 192.168.1.0/24, Пользователь 2 находится в сети 10.10.10.0/24. МЭ «ИКС» является шлюзом по умолчанию для Пользователя 1. На МЭ «ИКС» создан маршрут, позволяющий Пользователю 1 отправлять запросы Пользователю 2. Когда Пользователь 1 отправляет запрос Пользователю 2, пакет данных проходит через шлюз по умолчанию (МЭ «ИКС»), затем через маршрутизатор и доставляется по назначению Пользователю 2. Ответные данные от Пользователя 2 пойдут иначе: пакет данных отправляется на маршрутизатор, а затем непосредственно через коммутатор локальной сети - Пользователю 1. В случае простого обмена данными без установки сессии (обмен UDP-сегментами) такая схема будет работать при настройках межсетевого экрана МЭ «ИКС» по умолчанию. Однако, когда соединение устанавливает сессию с гарантией доставки пакетов (TCP-соединение), МЭ «ИКС» контролирует состояние сессии и, в случае отсутствия ответных данных в течение 30 секунд, обрывает соединение. Для предотвращения этого используется исключение из межсетевого экрана. Стоит отметить, что маршрут, исключенный из межсетевого экрана, не будет обрабатываться никакими другими правилами межсетевого экрана.

Предпочтительность маршрута можно установить при помощи метрики. Чем ниже данное значение, тем более предпочтителен маршрут.

5.2.12. Межсетевой экран

Межсетевой экран — комплекс программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей межсетевого экрана является защита компьютерных сетей или отдельных узлов

от несанкционированного доступа. Также МЭ «ИКС» отвечает за трансляцию сетевых адресов во внешнюю сеть (NAT) и перенаправление портов. Для настройки МЭ «ИКС» необходимо перейти в меню «Сеть» - «Межсетевой экран».

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние события системы. Выключать межсетевой экран не рекомендуется. Выключая межсетевой экран, вы оставляете сервер без защиты от подключений извне. Кроме того, при включении МЭ «ИКС» именно межсетевой экран генерирует NAT для всех сетей, поэтому, если перезагрузить МЭ «ИКС» с выключенным межсетевым экраном, у всех пользователей пропадет доступ в сеть Интернет.

Вкладка «Настройки» позволяет определить уровень доступа к управлению МЭ «ИКС» без создания дополнительных правил межсетевого экрана. Вы можете прописать IP-адреса или подсети, с которых будет осуществляться доступ к веб-интерфейсу МЭ «ИКС» или к консоли восстановления по протоколу SSH. Если вы хотите получать доступ к МЭ «ИКС» из любого места, вы можете полностью открыть доступ, прописав подсеть 0.0.0.0/0. Внимание! Данная настройка не является безопасной, поскольку в таком случае любой может получить доступ к системе. Перед тем как открывать доступ, настоятельно рекомендуется изменить пароль открываемого сервиса на более безопасный (не менее восьми символов, включающих цифры и буквы различного регистра). Параметр «Максимальное количество активных соединений» позволяет установить лимит всех сетевых подключений к системе. Параметр «Режим работы межсетевого экрана» устанавливает очередность запуска модулей pf и IPfw. В некоторых случаях работа VPN-подключений через МЭ «ИКС» может быть затруднена прохождением через NAT модуля pf. В таком случае измените очередность запуска на pf→IPfw.

Вкладка «Правила» является главным рабочим полем администратора по настройке межсетевого экрана. Она разделена на две части: список всех интерфейсов МЭ «ИКС» (в виде дерева) и собственно списка правил. При клике на выбранном интерфейсе будут показаны только те правила, которые относятся к данному интерфейсу. При необходимости вы можете отключить список интерфейсов, нажав на значок в виде стрелки в центре разделительной полосы. Правила межсетевого экрана группируются по типу:

- разрешающие правила;
- запрещающие правила;
- приоритеты;
- маршруты;
- ограничения скорости.

По умолчанию в межсетевом экране все соединения, инициированные снаружи, запрещены. При установке создаются несколько стандартных разрешающих правил для корректной

работы основных сервисов: почтовый сервер (порты 25, 110, 143), FTP-сервер (порты 21, 10000-10030), DNS-сервер (порт 53 UDP), VPN-сервер (порт 1723, протокол GRE). Также создаются два отключенных разрешающих правила: доступ к samba-ресурсам (порты 139, 445) и доступ к трансферу зон DNS (порт 53 TCP) и правило, разрешающее отвечать на ICMP-запросы (пинги). Эти правила не являются жестко заданными, при необходимости вы можете их выключить, отредактировать или удалить.

Вкладка «События» отображает все изменения, происходящие с межсетевым экраном. Она разделена на страницы, кнопками «вперед» и «назад» вы можете переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее. В правом верхнем углу модуля находится строка поиска. С ее помощью вы можете искать нужные вам записи. Вкладка всегда отображает события за текущую дату. Чтобы посмотреть события за другой день или иной промежуток времени, выберите нужные даты, используя календарь в левом верхнем углу модуля. В правой части верхней панели выпадающее меню «Сообщения» позволяет отфильтровать список событий по выбранному критерию: системные сообщения, сервисные сообщения, ошибки, остальные сообщения.

5.2.13. Прокси

Прокси-сервер — служба, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо веб-ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (если кто-то из клиентов уже обращался к этому ресурсу). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях. Для настройки прокси-сервера необходимо перейти в меню слева «Сеть» - «Прокси».

Также прокси-сервер позволяет анализировать проходящие через сервер HTTP-запросы клиентов, выполнять фильтрацию и учет трафика по URL и MIME-типам. Кроме этого, прокси-сервер реализует механизм доступа в сеть Интернет по логину/паролю. Прокси-сервер выполняет кеширование объектов, полученных пользователями из сети Интернет и за счет этого сокращает потребление трафика и увеличивает скорость загрузки страниц. При входе в модуль отображается состояние служб, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки. Обычно для работы через прокси-сервер необходимо указать его адрес и порт в настройках браузера. Однако, в случае если не используется авторизация пользователей по логину/паролю, можно использовать функцию прозрачного прокси. При этом все запросы по протоколу HTTP из локальной сети автоматически направляются через прокси-сервер. Таким

образом появляется возможность фильтрации и учета трафика по URL независимо от настроек клиентских компьютеров. Порт работы прокси-сервера по умолчанию 3128, в настройке модуля вы можете изменить его на любой свободный порт.

Кеширование страниц. Прокси-сервер выполняет кеширование веб-страниц и объектов, которые пользователи скачивают из Интернета. Таким образом экономится интернет-трафик и увеличивается скорость доступа к веб-страницам. Эффективность работы кеша зависит от его размера. Для организации с большим количеством пользователей рекомендуется установить размер кеша в соответствующем поле в несколько гигабайт. Также вы можете ограничить размер загружаемого файла в поле «Ограничивать размер ответа» (В мегабайтах). Опция «Скрывать IP-адрес пользователя» позволяет отключить указание в отправляемом заголовке внутреннего IP-адреса пользователя (параметр forwarded_for). Содержимое кеша прокси-сервера можно посмотреть на вкладке «Кеш». Следует отметить, что веб-интерфейс отображает не все содержимое кеша, а только некоторые элементы, такие как изображения.

Прозрачный прокси. В этом режиме МЭ «ИКС» вместо того, чтобы сразу принимать HTTP-запросы пользователя на порту прокси-сервера, сам перенаправляет их прокси-серверу. Прокси-сервер обрабатывает запрос (с возможной отдачей содержимого из кеша), это содержимое направляется к запросившему пользователю, для которого оно выглядит как «ответ» сервера, к которому адресовался запрос. Таким образом, пользователь может даже не знать, что все запросы и ответы прошли через прокси-сервер. По умолчанию прозрачный прокси перехватывает запросы по 80 порту (HTTP). Вы можете включить или отключить прозрачное проксирование DMZ и локальных сетей, отметив соответствующие флажки в настройках. По умолчанию DMZ сети не проксируются, а локальные проксируются. Некоторые программы могут негативно реагировать на изменения в пакетах, которые проходят через прокси-сервер. Вы можете прописать IP-адреса или имена сайтов, пакеты до которых не будут обрабатываться прокси-сервером в поле «Исключения для прозрачного прокси».

SOCKS — сетевой протокол, который позволяет клиент-серверным приложениям прозрачно использовать сервисы за межсетевыми экранами. Клиенты за межсетевым экраном, нуждающиеся в доступе к внешним серверам, вместо этого могут соединяться с SOCKS прокси сервером. Такой прокси сервер контролирует права клиента для доступа к внешним ресурсам и передает запрос к серверу. SOCKS может использоваться и противоположным способом, разрешая внешним клиентам соединяться с серверами за межсетевым экраном (брандмауэром). В отличие от HTTP прокси серверов, SOCKS передает все данные от клиента, ничего не добавляя от себя, то есть с точки зрения конечного сервера, SOCKS прокси является обычным клиентом. SOCKS более универсален — не зависит от конкретных протоколов уровня приложений (7-го уровня модели OSI) и базируется на стандарте TCP/IP — протоколе 4-го уровня. Зато HTTP прокси кэширует данные и

может более тщательно фильтровать содержимое передаваемых данных. Вы можете использовать SOCKS5-сервер, работающий в составе прокси-сервера для авторизации протоколов, отличных от HTTP. По умолчанию порт доступа 1080, вы также можете его изменить. Авторизация на сервере происходит по IP-адресу пользователя, установив соответствующий флажок, вы можете настроить авторизацию по логину/паролю.

Антивирус. МЭ «ИКС» поддерживает сканирование трафика, проходящего через прокси-сервер антивирусом. Поддерживается 3 антивирусных модуля: бесплатный Антивирус ClamAV и платный модуль Антивирус Касперского. Для работы антивируса необходимо приобрести лицензию и установить ее в соответствующем модуле. Для того чтобы включить антивирусное сканирование веб-трафика каким-либо антивирусным модулем, необходимо включить соответствующую опцию в настройках прокси.

Разрешенные порты. Вы можете указать, к каким портам на внешних серверах можно подключаться через прокси-сервер. Список разрешенных портов для SSL определяет, к каким портам разрешен доступ с использованием метода CONNECT.

ICAP (Internet Content Adaptation Protocol) - протокол расширения для прокси-сервера. В большинстве случаев он используется для сканирования на вирусы проходящего трафика и применения к нему различных контент-фильтров. Вы можете подключить к прокси-серверу МЭ «ИКС» сторонний ICAP-сервер, отметив соответствующий флажок в настройках и указав его адрес. Четыре последних флажка подключают к работе прокси-сервера соответственно модули контент-фильтр, SkyDNS, Garnet и веб-фильтр Касперского. Также вы можете установить флаг «Распределять запросы между основными провайдерами».

Автоконфигурирование прокси. Для того чтобы не прописывать вручную прокси-сервер на каждой клиентской машине, вы можете воспользоваться автоконфигуратором. В браузере клиента должна быть выставлена опция «Автоматическая конфигурация прокси», все остальные настройки определит МЭ «ИКС». Он включается установкой флажка в соответствующей вкладке. Вы можете отметить один или несколько протоколов из доступных (HTTP, HTTPS, FTP, WSS). Опция публикации скрипта автонастройки определяет, будет ли он доступен по IP-адресу сервера либо по созданному виртуальному хосту с доменным именем. При выборе виртуального хоста, он автоматически создастся в системе. Флажок «Создать запись на DNS-сервере» автоматически добавит зону с нужными записями для этого виртуального хоста. «Публиковать скрипт автоконфигурации по DHCP» - данный параметр передает настройки прокси всем DHCP-клиентам сервера.

Родительский прокси. Если в вашей организации несколько проксирующих серверов, расположенных иерархично, то вышестоящий для МЭ «ИКС» прокси-сервер будет являться его родительским прокси. Кроме того, в качестве родительского прокси может выступать любой узел

сети. Чтобы МЭ «ИКС» перенаправлял запросы, приходящие на его прокси-сервер, на родительский прокси, укажите его IP-адрес и порт назначения во вкладке «Родительский прокси». Прокси-сервера могут обмениваться данными своих кешей по протоколу ICP. В случае работы сети через несколько прокси — это может значительно ускорить работу. Если родительский прокси поддерживает работу протокола, отметьте соответствующий флажок и укажите порт работы службы (по умолчанию 3130). Если родительский прокси работает с авторизацией, то в нижеследующих полях укажите логин и пароль для подключения. Также вы можете настроить работу без DNS-сервера при помощи соответствующего флага.

Исключения для авторизации. Данная вкладка служит для настройки прокси-сервера таким образом, чтобы он не требовал авторизации при обработке запросов с определенного хоста в сети и (или) при обращении на определенный хост.

Кеш. Здесь вы можете просмотреть некоторые элементы веб-страниц (в основном изображения), которые сохранились в кэше, а также очистить его содержимое.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.2.14. Перенаправление портов

Иногда возникает необходимость снаружи организовать доступ к компьютеру, находящемуся в локальной сети: для подключения к windows-серверу по RDP и т.д. В этом случае обычно используется функция перенаправления портов. Для настройки перенаправления портов необходимо перейти в меню слева «Сеть» - «Перенаправления портов».

При создании перенаправления необходимо ввести протокол, порт перенаправления (порт который будет открыт на сервере и на который будут подключаться компьютеры из внешней сети), а также порт и хост назначения (порт и адрес компьютера, к которому необходимо организовать доступ). При необходимости вы можете указать интерфейс или группу интерфейсов, на котором будет реализовано перенаправление портов. Стоит отметить, что IP-адрес хоста, на который организовывается проброс порта, должен быть назначен какому-либо пользователю МЭ «ИКС».

Также можно перенаправлять диапазоны портов, введя номера портов через дефис: например, «10000-10100». Также, если необходимо, чтобы машины локальной сети при обращении на перенаправленный порт попадали на хост назначения, можно включить опцию «разрешить подключаться из локальной сети». При этом локальные соединения будут проходить через NAT и хост назначения увидит эти подключения как инициированные МЭ «ИКС». Если для хоста, на который перенаправляется запрос, МЭ «ИКС» не является шлюзом по умолчанию, полезно включить для такого перенаправления флажок «Использовать NAT». Установите флаг «Разрешить подключаться из локальной сети», если требуется, чтобы устройства локальной сети при обращении на перенаправленный порт попадали на хост назначения. Для того чтобы в межсетевом экране автоматически создалось правило, разрешающее подключение на данное перенаправление, отметьте соответствующий флажок. Если вам необходимо настроить доступ индивидуальным образом, вы можете вручную добавить разрешающее правило, в котором нужно указать порт назначения и порт перенаправления через запятую в поле «Порт назначения». Остальные поля заполняются в зависимости от уровня доступа, который вы хотите настроить.

5.2.15. Веб-фильтр Garnet

Сервис Garnet расширяет список возможных категорий трафика, которые могут быть использованы в запрещающих, разрешающих правилах прокси или исключениях прокси для пользователей и групп пользователей. Модуль расположен в меню Защита – Веб-фильтр Garnet. Для возможности использования сервиса Garnet на МЭ «ИКС» должна действовать активная лицензия.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий. Служба «Веб-фильтр Garnet» отвечает за работоспособность предустановленного веб-фильтра Garnet, который определяет, к какой категории принадлежит открываемый веб-сайт (если установлен соответствующий флаг в настройках прокси-сервера). Внимание! По умолчанию служба находится в состоянии «не настроен». Чтобы активировать ее, установите в настройках прокси-сервера флаг «Использовать Garnet».

Вкладка «Настройки». Флаг «Использовать в прокси» соответствует аналогичному флагу в настройках прокси. Данный флаг включает Веб-фильтр Garnet для фильтрации трафика, проходящего через прокси-сервер. Если флаг установлен, то можно определить размер кеша прокси, который будет использоваться для обработки данных, а также время ожидания ответа от облачного сервиса. На вкладке настроек также доступен функционал проверки конкретных URL-адресов. После ввода необходимого URL и нажатия кнопки «Проверить» будет выведен список категорий сервиса Garnet, к которым относится введенный URL, либо категория не будет определена, если проверяемый сайт или сам сервис не доступны. Так как работа сервиса основана на алгоритмах машинного обучения, то результаты проверки адресов могут быть неполными либо полностью

(частично) неверными. Применяемые алгоритмы постоянно улучшаются, и вы можете помочь сделать их еще более точными. Для этого можно воспользоваться формой обратной связи, которая появится, как только введенный URL будет категоризирован.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.2.16. Jabber

В Интернет Контроль Сервере поддерживается Jabber — служба для обмена сообщениями и файлами. Функции Jabber-сервера обеспечиваются следующими инструментами:

Служба. Отвечает за работу Jabber-сервера. Здесь можно посмотреть состояние сервера и журнал событий.

Настройки. Предназначен для настройки параметров работы Jabber-сервера, таких как: администраторы, Jabber-конференции, общий ростер и др.

Домены и аккаунты. В модуле можно присваивать Jabber-домены и аккаунты пользователям, а также работать с ними.

Ростер. Отвечает за управление списком контактов всех созданных на МЭ «ИКС» Jabber-доменов. Здесь можно добавлять группы контактов и распределять контакты по группам.

5.3. Идентификация и аутентификация субъектов межсетевого взаимодействия при доступе к различным ресурсам

Для идентификации и аутентификации субъектов межсетевого взаимодействия при доступе к различным ресурсам в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: Пользователи (см. раздел 4.1.1) и Роли.

5.3.1. Роли

Модуль «Роли» расположен в меню слева «Пользователи и статистика» - «Роли». Этот модуль определяет возможности пользователей по управлению МЭ «ИКС». По умолчанию

доступны следующие роли пользователей: Администратор, Пользователь, Администратор группы (представлены в Таблице 5).

Таблица 5 – Роли пользователей

Роль	Возможности
Администратор	Пользователь имеет полный доступ ко всем функциям веб-интерфейса МЭ «ИКС»
Пользователь	Пользователь имеет доступ только к своей персональной странице просмотра статистики
Администратор группы	Пользователь имеет доступ к функциям создания, удаления и редактирования пользователей группы, в которой он находится, а также назначения правил, квот и просмотра статистики

Чтобы создать собственную роль, нажмите кнопку «Добавить» → «Роль», создайте для нее имя, описание, вид иконки и выберите в списке привилегии, которые получит пользователь в этой роли.

После создания роли в модуле «Наборы правил» создается набор правил, жестко закрепленный за созданной ролью, аналогично наборам правил для пользователей и администраторов.

5.4. Регистрация всех событий, в том числе событий безопасности

Для регистрации всех событий, в том числе событий безопасности, в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: Отчеты, Монитор соединений, Журнал и уведомления.

5.4.1. Отчеты

Модуль «Отчеты» находится в основном меню слева в «Пользователи и статистика». Система статистики пользователей в МЭ «ИКС» может быть как настроена вручную, так и выведена с помощью нескольких стандартизованных отчетов. Все они представлены в модуле «Отчеты». Каждый отчет — это система графиков и цифровых значений, которые могут быть выведены за любой период времени. В правой верхней части отчета находится меню выбора временного периода. Все отчеты генерируются за выбранный временной период - день, неделю, месяц или произвольный указанный. По умолчанию выводятся цифры за текущий день.

Сводный отчет представляет собой наглядное представление о расходе трафика в системе. По умолчанию он состоит из нескольких популярных графических отчетов: по пользователям, по

протоколам, по посещенным сайтам и т.д. Эту страницу можно редактировать, изменяя положение отчетов, вид диаграммы и ее настройки. Также вы можете добавлять собственные отчеты.

Содержит следующие показатели для выбранного пользователя: статистика по часам, по адресам и доменам (посещенным сайтам), статистика по MIME-типам, статистика по протоколам. В случае, если выбрана группа пользователей, то последний отчет заменяется на отчет по объему трафика пользователей в этой группе.

Категории трафика. На данной вкладке отображается сводка трафика, сгруппированная по категориям трафика. Под диаграммой с пятью самыми распространенными категориями можно посмотреть развернутый отчет по всем запрошенным категориям.

Активность пользователей. На данной вкладке отображаются страницы, загруженные пользователями. В отчете можно указать группу пользователей, по которым будет построен отчет.

Лента поисковиков. На данной вкладке отображаются поисковые запросы пользователей. В отчете можно указать группу пользователей, по которым будет построен отчет.

По объему трафика. Выводит список пользователей, упорядоченный по объему потребленного трафика за данный период времени.

Топ 5 IP-адресов и доменов. Выводит список пяти наиболее посещаемых хостов и доменов, а также список пяти самых активных посетителей для каждого из этих доменов.

Топ 5 пользователей. Аналогичен предыдущему отчету, но выводится список наиболее активных пользователей и список пяти самых посещаемых доменов для каждого.

Модуль «Управление отчетами» расположен в меню слева «Пользователи и статистика». Он отображает список всех отчетов - стандартных и сохраненных пользователем. Вы можете создать несколько типовых отчетов, наиболее подходящих для контроля трафика вашей организации, и просматривать их в любое время.

Вкладка «Конструктор отчетов» позволяет создавать отчеты по заданным параметрам фильтров в том случае, если для получения данных недостаточно стандартных.

На вкладке «Службы» отображаются состояния служб «Статистика» и «Счетчики» с возможностью выключить либо включить последние сообщения в журнале.

На вкладке «Службы» можно определить параметры отображения и хранения журналов вышеописанных служб и записей статистики.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка

поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.4.2. Монитор соединений

Модуль «Монитор соединений» расположен в меню слева «Пользователи и статистика». Монитор соединений предназначен для контроля потоков трафика в реальном времени. Если установить флаг «Отображать только активные соединения», будут видны только те пользователи, которые имеют соединения в реальном времени. В таблице соединений могут отображаться следующие столбцы: имя пользователя, количество соединений, время соединений, протокол, состояние, оставшееся время соединения, число прошедших пакетов, объем скачанной информации по соединению в байтах, скорость соединения в пакетах в секунду и в байтах в секунду. Так же, как и в других модулях, таблица соединений состоит из столбцов, видимость которых регулируется выпадающим меню.

5.4.3. Журнал и уведомления

Модуль «Журнал и уведомления» расположен в меню слева «Обслуживание». На вкладке «Системный журнал» отображаются сообщения о действиях пользователей, изменениях в статусах сервисов и ошибках системы. Сообщения можно фильтровать по категориям и дате. Кроме того, можно фильтровать сообщения по содержимому. Для этого введите в строке поиска (верхний правый угол) сочетание символов, которое должно содержаться в событии, например, написав «Администратор» вы увидите все сообщения, связанные с этим пользователем. Фильтр чувствителен к регистру.

Настройки уведомлений. Вы всегда можете быть в курсе того, что происходит в системе, настроив параметры уведомлений. Вы можете указать период доставки сообщения, а также выбрать тип событий, о которых необходимо уведомлять. При записи о любом событии в системном журнале аналогичное сообщение может быть доставлено вам по e-mail, а также в Jabber-контакт.

Уведомления на почту. Если вы хотите получать уведомления МЭ «ИКС» на свой почтовый ящик, вам нужно указать его в поле «Почтовые ящики для уведомлений» вкладки «Уведомления на почту». Вы можете прописать любой внешний почтовый ящик либо выбрать его из заведенных в почтовом сервере МЭ «ИКС». Если МЭ «ИКС» настроен как почтовый сервер, то он может использовать собственный SMTP-сервер. Также для этого необходимо указать с какого почтового ящика из созданных на МЭ «ИКС» будут приходить сообщения. В противном случае вы можете

указать логин и пароль существующей учетной записи на любом другом почтовом сервере. От имени этого почтового ящика и будут приходить уведомления.

Уведомления на Jabber. Также вы можете настроить передачу сообщений посредством протокола XMPP (Jabber). Аналогично почтовой рассылке, вы указываете список Jabber-аккаунтов, на которые будут рассылаться уведомления. Их также можно выбрать из уже созданных на МЭ «ИКС». Затем выбираете, отправлять эти сообщение посредством Jabber-сервера МЭ «ИКС» с указанием учетной записи отправителя, либо же использовать сторонний Jabber-сервер.

Уведомления в Telegram. Вкладка позволяет настроить отправку уведомлений при помощи предварительно созданного бота в мессенджере Telegram. Чтобы создать нового бота, найдите в мессенджере пользователя @BotFather, нажмите «Start» и действуйте далее согласно инструкции. Вкладка содержит несколько параметров. Поле «Telegram-аккаунты для уведомлений» позволяет прописать один или несколько пользовательских телеграм-аккаунтов, а также ID либо ID-группы. Аккаунты указываются без начального символа @. В поле «Токен» указывается токен, полученный в результате создания бота. Флаг «Использовать прокси» позволяет указать внешний прокси-сервер для отправки сообщений. После установки флага необходимо заполнить поля «Сервер», «Порт», «Логин» и «Пароль». Чтобы внесенные изменения вступили в силу, нажмите кнопку «Сохранить» или «Обновить». Если настройки верны, то после сохранения статус подключения изменится на «Соединение установлено». Для того чтобы бот мог отправлять сообщения, необходимо первоначально отправить ему любое сообщение от указанных телеграм-аккаунтов. Также сообщение необходимо отправить при обновлении МЭ «ИКС» или разворачивании резервной копии с настройками службы.

Служба уведомлений. Данная вкладка содержит текущий статус службы. Если не создано ни одного агента отправки, служба находится в состоянии «не настроен». На данной вкладке отображаются следующие сведения о службе: статус службы, кнопки «Включить»/«Выключить» службу, журнал последних событий.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.4.4. Fail2ban

Модуль «Fail2ban» сканирует лог-файлы и блокирует IP-адреса, которые ведут себя подозрительно (например, делают слишком много попыток входа с неверным паролем, чтобы найти уязвимость). Модуль расположен в меню Защита - Fail2ban.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий.

Вкладка «Настройки» предназначена для настройки работы Fail2ban. Флаги «Защитить почтовый сервер», «Защитить веб-почту», «Защитить сервер телефонии», «Защитить VPN-сервер», «SSH», «FTP», «GUI» позволяют Fail2ban анализировать логи авторизации в соответствующих модулях. В поле «Количество неудачных попыток авторизаций» можно задать количество неудачных попыток авторизации в одном из модулей, отмеченных флагом. После этого IP-адресу будет полностью заблокирован доступ к МЭ «ИКС». По умолчанию установлено 3 попытки. В поле «Интервал неудачных попыток авторизаций» задается время, в течение которого в каждом модуле подсчитывается количество неудачных попыток авторизации (в минутах). По умолчанию установлен интервал 10 минут. Поле «Блокировать на» предназначено для установки времени, в течение которого будет действовать блокировка IP-адреса (в минутах). По умолчанию установлено значение 10 минут. Флаг «Увеличивать время бана» позволяет включить дополнительные настройки Fail2ban для увеличения времени бана: а) «Прибавить к времени бана случайное время из диапазона от 0 до» — параметр выберет случайное значение и прибавит к стандартному времени бана (в минутах); б) «Фактор роста» — дополнительный глобальный коэффициент, на который будут умножаться все множители из списка. Увеличение фактора роста удобно использовать, когда вы хотите значительно увеличить время бана. В таком случае не потребуется переписывать список множителей; в) «Список множителей» — список, по которому будет происходить рост времени бана. Порядковый номер множителя будет соответствовать количеству раз, когда IP-адрес попал в дополнительный бан; г) флаг «Не разделять попытки авторизации по службам». На данной вкладке также можно сформировать белый список для Fail2ban. Нажмите кнопку «Белый список» и в открывшемся окне задайте соответствие IP-адреса/подсети/диапазона (192.168.1.1, либо 192.168.1.1/28, либо 192.168.1.1-192.168.1.3) и сервиса (всех сервисов), для которых Fail2ban не будет срабатывать.

На вкладке «Заблокированные соединения» отображается список текущих блокировок IP-адресов. Они распределены по блокам (модулям), в которых произошла блокировка. На вкладке также можно посмотреть время, когда конкретный IP-адрес попал в бан и когда из него выйдет (кроме тех адресов, которые забанены перманентно). При необходимости с помощью соответствующих кнопок пользователь с ролью Администратор может: а) добавить IP-адрес в перманентный бан — действует всегда и по всем сервисам; б) добавить IP-адрес в белый список —

произойдет разблокировка IP-адреса, и он не будет проверяться Fail2ban по сервису, добавленному в белый список; в) разблокировать IP-адрес до истечения бана.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.4.5. Сетевые утилиты

Модуль «Сетевые утилиты» расположен в меню Сеть – Сетевые утилиты.

В состав МЭ «ИКС» входят несколько сетевых утилит, которые помогают выполнять диагностику сети:

– Пинг - Утилита пинг (ping) отправляет ICMP-запросы указанному узлу сети и фиксирует поступающие ответы. Время между отправкой запроса и получением ответа позволяет определять двусторонние задержки по маршруту и средний уровень потери пакетов, то есть определять стабильность и качество связи, а также косвенно определять загруженность на каналах передачи данных и промежуточных устройствах. Кроме того, пингом называют время, затраченное на передачу пакета информации в компьютерных сетях от одного хоста до другого и обратно. Это время также называется лагом или задержкой и измеряется в миллисекундах. Задержка зависит от загруженности и количества узлов в пути между хостами. Для запуска утилиты введите доменное имя или IP-адрес и укажите количество пакетов.

– Трейс - Утилита трейс (traceroute) предназначена для вывода маршрута прохождения запроса до выбранного хоста. Она выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к нему. Данная утилита позволяет определить проблемы с маршрутизацией трафика, а также в случае проблем при доставке данных до какого-либо узла — определить, на каком именно участке сети возникли неполадки. Внимание! Программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети. Из-за особенностей работы протоколов маршрутизации в сети Интернет обратные маршруты часто не совпадают с прямыми, причем это справедливо для всех промежуточных узлов в пути. Поэтому ICMP-ответ от каждого промежуточного узла может идти своим собственным маршрутом,

затеряться или прийти с большой задержкой, хотя в реальности с пакетами, которые адресованы конечному узлу, этого не происходит. Кроме того, на промежуточных маршрутизаторах часто стоит ограничение числа ответов ICMP в единицу времени, что приводит к появлению ложных потерь. Для запуска утилиты введите адрес нужного хоста.

– Опрос DNS - Утилита «Опрос DNS» (dig) позволяет посылать различные запросы к DNS-серверам и определять ошибки в их конфигурации. Для запуска утилиты введите домен и выберите тип записи. Также можно указать конкретный DNS-сервер для опроса.

– Информация о домене - Утилита «Информация о домене» (whois) позволяет получить информацию о владельце домена или диапазона IP-адресов, а также сопутствующую информацию (дата регистрации, контактные данные, тип домена, регистратор и т. д.) из базы данных WHOIS. Для запуска утилиты введите домен или диапазон IP-адресов.

– Дамп - Утилита дамп (tcpdump) отображает заголовки пакетов, проходящих через выбранный сетевой интерфейс. Позволяет диагностировать проблемы, связанные с настройкой межсетевого экрана, маршрутизацией и работой сетевых сервисов. Для запуска утилиты выберите сетевой интерфейс, на котором будет выполняться сбор данных. Для фильтрации сообщений можно указать следующие данные: протокол, порт, направление сетевого трафика для указываемого IP-адреса (хост либо источники и назначение). Также при использовании утилиты можно установить флаг «Сохранить результат в файл» и просмотреть сохраненные файлы dump. Для этого нажмите на кнопку «Показать файлы». Откроется диалоговое окно, в котором есть возможность скачать либо удалить файлы dump с расширением *.pcap. Для открытия данных файлов используйте специальную программу (например, Wireshark). Удаление dump-файлов можно организовать по времени или по объему в модуле «Система». Внимание! Если запустить сбор дампа в файл и оставить вкладку открытой на долгое время, то файл с дампом может занять все свободное место на жестком диске.

– Сетевые интерфейсы - Утилита «Сетевые интерфейсы» позволяет получить сведения о состоянии всех интерфейсов МЭ «ИКС». Она выводит результат команды ifconfig и таким образом позволяет узнать, какие IP-адреса назначены каждому интерфейсу, какие виртуальные интерфейсы созданы, а также проверить наличие сигнала в подключенном кабеле. Для запуска утилиты не требуется вводить никакие параметры.

– Таблица маршрутизации - Данная утилита выводит текущую таблицу маршрутизации МЭ «ИКС». С ее помощью можно увидеть все маршруты, созданные в системе. Для запуска утилиты не требуется вводить никакие параметры.

– Тест скорости канала - Данная утилита позволяет измерить пропускную способность канала. Для измерения выберите сервер и запустите тест. Внимание! Не все сервера могут быть

доступны. Также не все сервера могут показать подлинную скорость вашего канала из-за удаленности, количества промежуточных узлов и их нагруженности.

– Сканирование сети - С помощью сканирования сети можно тестировать безопасность локальной сети предприятия. Она позволяет проверить доступность локальных компьютеров, а также определить открытые в сети порты. Кроме того, при указании в качестве исследуемого хоста сам МЭ «ИКС» есть возможность дополнительно проверить безопасность системы на предмет доступных портов. Для запуска утилиты выберите ее режим работы (поле «Действие»): а) доступность адресов — МЭ «ИКС» проверяет, находятся ли в сети выбранные компьютеры. В качестве аргумента может быть указан как отдельный хост, так и подсеть. В последнем случае МЭ «ИКС» проверит доступность всего указанного диапазона перебором; б) сканирование портов — МЭ «ИКС» проверяет, какие порты открыты для доступа на указанном хосте либо на всех компьютерах указанной подсети; в) информация о версии — МЭ «ИКС» проверяет версию службы каждого открытого порта на указанном хосте либо на всех компьютерах указанной подсети.

– Прокси access.log - Данная утилита позволяет посмотреть в реальном времени логи запросов пользователей на прокси-сервере. Запросы можно отфильтровать с помощью одноименного поля (например, по логину пользователя или его IP-адресу). Также удобно выводить запросы только с определенным кодом http. (например, 403).

Запуск работы утилиты производится кнопкой «Запустить», остановка — соответствующей кнопкой.

5.5. Обеспечение бесперебойного функционирования и восстановления после сбоев за счет возможности кластеризации

Для обеспечения бесперебойного функционирования и восстановления после сбоев за счет возможности кластеризации в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: Мониторинг, Время и дата, Резервные копии, Система, Управление питанием, Жесткие диски.

5.5.1. Мониторинг

Модуль «Мониторинг» расположен в меню слева «Обслуживание». В модуле «Мониторинг» вы можете посмотреть статистику использования сетевых и системных ресурсов, а также различных показателей системы, таких как виртуальная память, загрузка процессора, загрузка системы, пинг до ya.ru, трафик на сетевых интерфейсах и др. На каждый из пунктов

строится несколько графиков, различных по временному интервалу: за последний час, 6 часов, день, неделю, и т.д.

«Графики». В левой части данной вкладки отображается список доступных показателей. На каждый из выбранных пунктов в правой части вкладки строится несколько графиков, различных по временному интервалу: за последний час, 6 часов, день, неделю и т. д. При необходимости можно добавить собственные графики для проверки доступности указанных хостов. Для этого нажмите кнопку «Добавить» и укажите название и адрес. При нажатии на кнопку «Очистить» все графики системы будут удалены и сформированы заново.

Вкладка «Мониторинг состояния системы» содержит статус службы мониторинга, кнопку выключения/включения и последние сообщения в журнале.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.5.2. Время и дата

Модуль «Время и дата» расположен в меню слева «Обслуживание». Модуль «Время и дата» позволяет установить системное время, выбрать временную зону, а также синхронизировать системное время с серверами точного времени в Интернете. Если сервер времени выключен, то можно задать необходимые значения времени и даты вручную. Поле «Временная зона» предназначено для указания текущей временной зоны. Поле «Сервера для синхронизации NTP-сервера» содержит предустановленные URL пулов NTP-серверов. В данном поле можно указывать IP-адреса NTP-серверов или иных пулов. Встроенный NTP-сервер в МЭ «ИКС» использует данные URL для синхронизации времени и даты. При установке флага в поле «Автоматически создавать разрешающее правило для доступа к серверу времени» будет выполнена установка разрешающего правила межсетевого экрана на доступ от локальных и DMZ-сетей на порт NTP (123). После изменения временной зоны МЭ «ИКС» выдаст сообщение: «Временная зона была изменена. Чтобы изменения вступили в силу для всех служб, необходимо перезагрузить МЭ «ИКС»». Пользователь

с ролью Администратор может нажать отмену, тогда система будет работать по новой временной зоне, но некоторые службы продолжат работу по старой.

Вкладка «Сервер времени» отображает текущее состояние модуля, общую информацию о сервере времени МЭ «ИКС», а также кнопку «Выключить» (или «Включить если модуль выключен) для управления модулем.

Вкладка «Временные промежутки» позволяет задать временные промежутки по дням недели и времени «с… по…». На вкладке отображаются все созданные временные промежутки. Их можно добавлять, удалять и редактировать при помощи соответствующих кнопок. Созданные временные промежутки можно применять в различных модулях МЭ «ИКС», где требуется задавать время действия.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.5.3. Резервные копии

Модуль «Резервные копии» расположен в меню слева «Обслуживание». При работе с сервером часто возникает необходимость создания резервных копий. Для ее создания, зайдите в модуль «резервные копии» и нажмите на кнопку «добавить». В появившемся окне отметьте те данные МЭ «ИКС», которые вы хотите сохранить. Для активации резервной копии, выберите ее из списка и нажмите кнопку «Восстановить». Вы можете скачать резервную копию на свой компьютер, для этого воспользовавшись кнопкой «Скачать». Закачать резервную копию на МЭ «ИКС» можно, используя кнопку «Загрузить» и выбрав файл копии в открывшемся окне. Для загрузки копии из файлового хранилища МЭ «ИКС» нажмите кнопку «Загрузить из хранилища файлов» и выберите папку, из которой требуется загрузить резервную копию.

Шаблоны служат для сохранения нескольких выбранных данных в одной резервной копии. Например, вы можете задать в одной резервной копии сохранять настройки системы, почту и указанную папку с пользовательскими данными из хранилища файлов. Шаблон может создаваться по расписанию, а также удалять старые копии, созданные по этому шаблону. Также, каждый шаблон

может быть настроен на копирование на свой FTP-сервер. В МЭ «ИКС» есть два предустановленных шаблона: «Резервная копия настроек» (сохраняет только настройки МЭ «ИКС») и «Полная резервная копия» (сохраняет полную резервную копию МЭ «ИКС»). Для активации одного из шаблонов укажите время его срабатывания в окне редактирования.

Вкладка «Настройки» предназначена для того, чтобы постоянно иметь актуальную копию настроек системы, во вкладке «Настройки» можно указать параметры автоматического сохранения бекапов. Помимо сохранения копии на жесткий диск МЭ «ИКС», вы можете выбрать опцию сохранения на съемный носитель или удаленный FTP-сервер, это позволит обезопасить себя на случай разрушения жесткого диска. Во избежание накопления ненужной информации (резервные копии статистики могут достигать довольно больших объемов) также можно настроить параметры автоматического удаления старых резервных копий. Также вы можете выбрать дополнительный жесткий диск для сохранения резервных копий. Перед тем как скопировать резервную копию на съемный носитель, необходимо его отформатировать формате FAT 32.

5.5.4. Система

Модуль «Система» расположен в меню слева «Обслуживание». Модуль предназначен для ввода следующих данных: название организации, которое будет отображаться в веб-интерфейсе, имейл-адрес, доменное имя системы. Также здесь можно произвести удаление данных и просмотреть текущие задачи в МЭ «ИКС» (создание резервной копии, импорт пользователей и т. д.).

На вкладке «Система» вы можете указать название вашей организации, которое будет отображаться в веб-интерфейсе, а также ввести e-mail организации и доменное имя системы. Доменное имя системы влияет на работу различных сетевых служб, в частности при его неправильном заполнении могут некорректно работать Jabber-сервер, DNS и почта.

Вкладка «Удаление данных» позволяет настроить период и размер (в Мб) хранения каждого типа данных МЭ «ИКС». Удалены могут быть логи статистики, логи детализированной статистики, записи звонков, общие логи системы (записываемые в разделах «События» и «Журнал» всех служб) и результаты сетевых утилит. Иногда бывает необходимо вручную очистить системные логи за какой-либо период. Для этого можно воспользоваться кнопкой «Ручное удаление данных». В появившемся окне необходимо выбрать период, за который нужно выполнить очистку информации и отметить, что именно вы хотите удалить. После нажатия на кнопку «Очистить» выбранные данные будут безвозвратно удалены.

При установке системы автоматически прописываются следующие значения:

– автоматически удалять логи статистики старше 6 месяцев;
– автоматически удалять логи детализированной статистики старше 3 месяцев.

При необходимости можно указать другой период либо отключить автоматическое удаление по временным рамкам.

Если заданы временные рамки и квота, то удаление данных будет происходить в зависимости от параметра, который будет достигнут раньше. В качестве временных рамок предлагается выбрать один из возможных вариантов: никогда, старше недели, старше месяца, старше 2 месяцев, старше 3 месяцев, старше 6 месяцев, старше года.

Чтобы изменения вступили в силу, нажмите кнопку «Сохранить».

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

На вкладке «Задачи» показаны выполняющиеся асинхронные процессы в МЭ «ИКС», а также процент выполнения для каждого процесса. Прервать выполнение процесса можно по кнопке «Cancel». При выполнении асинхронного процесса пользователь МЭ «ИКС» может производить различные настройки в веб-интерфейсе МЭ «ИКС». Асинхронными процессами являются: перенос почты, импорт пользователей, создание резервной копии и т. д.

5.5.5. Управление питанием

Модуль «Управление питанием» расположен в меню слева «Обслуживание». Модуль предназначен для настройки и управления источниками питания.

Сервер можно выключить или перезагрузить несколькими способами:

- кнопкой питания на системном блоке;
- из консоли восстановления (Управление сервером – Перезагрузка/Выключение);
- из веб-интерфейса, используя модуль «Управление питанием».

После нажатия кнопки «выключить» или «перезагрузить», сервер выполнит остановку служб, после чего завершит выключится\перезагрузится.

На вкладке «Управление питанием» показаны виджеты двух разделов: «Управление питанием» и «Контроллер ИБП».

В виджете «Управление питанием» отображаются следующие данные:

- время работы МЭ «ИКС» от сети питания;
- кнопки «Выключить МЭ «ИКС»» и «Перезагрузить МЭ «ИКС»».

В виджете «Контроллер ИБП» отображаются следующие сведения:

- информация о подключенном ИБП (запущен, остановлен, выключен, не настроен);
- кнопка «Включить» («Выключить») — позволяет запустить или остановить контроллер, который взаимодействует с ИБП (источником бесперебойного питания).

Вкладка «Настройки» позволяет задать настройки контроллера для взаимодействия с ИБП. Выберите тип ИБП. Контроллер МЭ «ИКС» может работать с ИБП фирм IPPON и APC по COM-порту или по USB-порту. На вкладке можно задать порог времени работы от ИБП (в секундах) и порог остаточного заряда батареи (в процентах). При достижении одного из параметров МЭ «ИКС» перейдет в режим завершения работы и выключится.

Вкладка «Расписание» позволяет назначить дату и время следующей запланированной перезагрузки МЭ «ИКС» или его выключение. Также вы можете указать дни недели, в которые МЭ «ИКС» будет перезагружаться или выключаться с указанием времени события.

5.5.6. Жесткие диски

Модуль «Жесткие диски» расположен в меню слева «Обслуживание». В этом модуле содержится список всех жестких дисков, физически подключенных к компьютеру, на котором установлен МЭ «ИКС». Список представлен в виде дерева, в котором есть два главных раздела - неиспользуемые диски и основной системный раздел (зеркало). В основном разделе перечислены диски, входящие в зеркальный массив, на котором установлена система. Для того чтобы добавить жесткий диск в систему, необходимо создать пользовательский раздел StrIPe или Mirror. Нажмите «Добавить» и выберите тип создаваемого раздела. Затем при помощи мыши перетащите по очереди неиспользуемые жесткие диски, которые необходимо добавить в раздел. После добавления в модуле «Хранилище файлов» появится дополнительная корневая папка, в которой можно создавать файловые ресурсы.

В МЭ «ИКС» предусмотрена возможность использования подключенных жестких дисков для работы. Например, можно настроить: а) хранение почтовых писем в выбранном разделе (поле «Жесткий диск для хранения почты»); б) сохранение резервных копий МЭ «ИКС» (поле «Жесткий диск для хранения резервных копий»).

Диск из раздела удаляется простым перетаскиванием диска в раздел «Неиспользуемые жесткие диски» либо нажатием кнопки «Удалить» (кроме раздела типа Stripe). Удалить раздел можно по кнопке «Удалить». При этом если удаляемый раздел выбран в настройках почты или резервных копий, на экране появится соответствующая ошибка. Разделы «Неиспользуемые жесткие

диски» и «Основной раздел Mirror», а также «Основной жесткий диск» в «Основном разделе Mirror» не доступны для удаления.

5.5.7. IPSec

Модуль «IPSec» позволяет применять шифрование во всех соединениях, в которых используется набор протоколов IPSec. Модуль расположен в меню Защита – IPSec.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий.

Вкладка «Настройки» предназначена для настройки работы IPSec. При установке флага «Автоматически создавать разрешающее правило» в межсетевом экране автоматически будут созданы разрешающие правила для IPSec-шифрования VPN-подключений и для IPSec-данных VPN-подключений. Названия правил являются гиперссылками, поэтому при нажатии на них можно перейти к списку правил межсетевого экрана.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.5.8. Хранилище файлов

Хранилище файлов представляет собой список всех пользовательских ресурсов, расположенных на МЭ «ИКС». Модуль расположен в меню Файловый сервер – Хранилище файлов.

Модуль «Хранилище файлов» состоит из двух частей: слева расположено общее дерево папок; справа отображается список файлов и папок выделенной папки дерева. Также здесь содержится информация об объеме папки или файла, типе и дате последнего изменения. В модуле можно создавать новые папки и управлять ими (переименовывать, удалять) при помощи соответствующих кнопок, а также открывать доступ к ресурсам. Внимание! Папка primary и папки, соответствующие разделам жестких дисков МЭ «ИКС», являются корневыми и не подлежат редактированию. В хранилище файлов можно добавлять, редактировать и удалять папки.

Хранилище файлов является универсальным центром контроля пользовательских ресурсов, поэтому непосредственно из данного модуля можно предоставлять доступ к определенным ресурсам: веб-ресурс, виртуальный хост, FTP-ресурс, общий ресурс (см. 4.1.7).

Если к папке открыт доступ, то при выделении папки появится информация о ресурсе со ссылкой на него. FTP

FTP-сервер позволяет размещать на сервере файлы и предоставлять доступ к ним по сети. Поддерживается анонимный вход и авторизация по логину и паролю. Пользователям можно задавать различные права доступа. Модуль «FTP» предназначен для настройки и управления FTP-сервером. Модуль расположен в меню Файловый сервер – FTP.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий.

Вкладка «Настройки» предназначена для установки параметров работы FTP-сервера. Поле «Порт» определяет порт передачи данных протокола. По умолчанию установлен стандартный порт 21. В поле «Порты для пассивного FTP» можно указать диапазон портов для FTP passive mode. Изначально протокол предполагал встречное TCP-соединение от сервера к клиенту для передачи файла или содержимого каталога. Это делало невозможным общение с сервером, если клиент находится за NAT. Кроме того, часто запрос соединения к клиенту блокируется межсетевым экраном. Чтобы этого избежать, было разработано расширение протокола FTP passive mode, когда соединение для передачи данных тоже происходит от клиента к серверу. Для этих целей выделяется диапазон портов, к которым могут подключаться клиенты. Чем большее число одновременных соединений устанавливают клиенты, тем шире должен быть данный диапазон. Флаги «Автоматически создавать разрешающее правило» создают разрешающие правила в межсетевом экране на соответствующие порты FTP-сервера из внешних сетей. Поле «Максимальное количество соединений» задает максимальное количество одновременно подключенных клиентов. В поле «Максимальное количество подключений с одного логина» можно ограничить пользователя числом одновременно создаваемых FTP-сессий с его логина. По умолчанию количество не ограничено. Поле «Максимальное количество подключений с одного хоста» ограничивает пользователя числом подключений с одного IP-адреса. По умолчанию количество не ограничено. В поле «Сертификат для FTPS» можно назначить службе заранее созданный сертификат для работы сервера по защищенному протоколу FTPS с использованием SSL.

Вкладка «FTP-ресурсы» предназначена для управления FTP-ресурсами, размещенными на МЭ «ИКС». Добавить FTP-ресурс можно так же, как и в модуле «Хранилище файлов». Единственное отличие — возможность изменить источник. Это директория из структуры хранилища файлов МЭ «ИКС», в которой будет располагаться содержимое FTP-ресурса. При необходимости можно создать новую папку в каталоге.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются

цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.6. Тестирование и контроль целостности программного обеспечения МЭ «ИКС»

Для тестирования и контроля целостности программного обеспечения МЭ «ИКС» в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: Все службы и ARP-таблица.

5.6.1. Все службы

Модуль «Все службы» расположен в меню слева «Обслуживание». В модуле «Все службы» отображается список всех запущенных служб МЭ «ИКС». Здесь можно выбрать, какие службы будут использоваться, а какие можно отключить. Статус службы сохраняется между перезагрузками, отключенная служба не будет запущена при следующем включении питания сервера. Клик по названию службы откроет страницу, с журналом работы службы, а также дополнительными настройками, если они доступны.

5.6.2. ARP-таблица

Модуль «ARP-таблица» расположен в меню слева «Сеть». ARP — протокол сетевого уровня, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP. ARP-таблица отображает IP и MAC подключенных к серверу сетевых устройств. В большинстве случаев в МЭ «ИКС» используется проверка прав доступа на основе IP-адреса пользователя. Однако пользователь может самостоятельно изменить IP адрес своего компьютера (например, чтобы получить доступ к запрещенным для него ресурсам), тогда как MAC адрес является уникальным идентификатором сетевого устройства и изменить его гораздо сложнее. Чтобы предотвратить ситуацию несанкционированной смены IP-адреса, необходимо задать соответствие между MAC-адресом сетевой карты и IP-адресом.

Сделать это можно нажав «Добавить» - «IP и MAC-адрес» и отметить пункт «Связать IP с MAC». Если компьютер пользователя уже есть в списке, и ему назначен желаемый IP - просто нажмите кнопку «Связать IP с MAC». Аналогичную операцию можно сделать и в списке IP-адресов пользователя. Если IP адрес сопоставлен пользователю МЭ «ИКС» в строке «Пользователь», то вам будет показано его имя. Кликнув по имени пользователя, вы переместитесь на его страницу.

Вкладка «Журнал» позволяет отслеживать изменения адресации пользователей. Если пользователь с известным MAC-адресом изменит свой IP-адрес, это отобразится в журнале истории. Сопоставления из ARP-таблицы также используется DHCP-сервером. Именно по MAC-адресу DHCP-сервер определяет, какой IP адрес назначить сетевому устройству. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.7. Преобразование сетевых адресов

Для преобразования сетевых адресов в МЭ «ИКС» применяются следующие модули и функции, обозначенные в меню слева в выпадающих вкладках графического интерфейса МЭ «ИКС» начального экрана: DNS, Провайдеры и сети, DHCP.

5.7.1. DNS

Модуль «DNS» расположен в меню слева «Сеть». DNS (англ. Domain Name System — система доменных имен) — система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации служб и обслуживающих узлах для протоколов в домене (SRV-запись). DNS обладает иерархической структурой. Каждый сервер, отвечающий за доменное имя или зону, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций, отвечающих только за «свою» часть доменного имени. Функции DNS-сервера в МЭ «ИКС» исполняет свободное программное обеспечение bind. При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Вкладка «Настройки». Основной внешний параметр DNS-сервера - список разрешений для трансфера зон. Сюда добавляются адреса других DNS-серверов, которые имеют право получать записи зон от МЭ «ИКС». Если у вас не создано ни одного провайдера, то в данной вкладке вы можете вписать DNS-сервера, которые будет использовать МЭ «ИКС». Также вы можете

определить, устанавливать ли основным DNS-сервером контроллер домена в том случае, если МЭ «ИКС» является его членом. На этой же вкладке задается автоматическое создание разрешающих правил.

Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен, а чаще — одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации, так называемое делегирование. Как связная часть дерева, зона внутри тоже представляет собой дерево. Вкладка «Зоны» позволяет создавать DNS-зоны для работы различных служб МЭ «ИКС». В модуле можно добавить следующие DNS-зоны: DNS-зона, вторичная DNS-зона, обратная DNS-зона, перенаправление DNS-зоны.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.7.2. Провайдеры и сети

Модуль «Провайдеры и сети» расположен в меню слева «Сеть». В модуле «Провайдеры и сети» содержится список всех внешних, внутренних и виртуальных сетей, подключенных к МЭ «ИКС». Для начала рассмотрим, что выступает в качестве объекта маршрутизации. Это:

- WAN-сеть, которая в терминологии МЭ «ИКС» обозначается как «Провайдер»;
- LAN-сеть, directly-connected к МЭ «ИКС»;
- внутренняя сеть - сеть, которая не подключена к МЭ «ИКС» напрямую, а отделена маршрутизатором;
- пользователь - конечный объект маршрутизации.

В «закрытом» состоянии отображается только имя сети, IP-адрес интерфейса, статус сигнала и доступность шлюза (для провайдеров). При выделении объекта кликом мыши показываются все его основные параметры. Любой объект можно отредактировать или удалить при помощи кнопок верхней панели или дублирующих их кнопок напротив имени объекта. Кроме того,

при необходимости его можно выключить, а затем снова включить — это удалит настройки интерфейса без необходимости заново создавать объект. Также на верхней панели находится кнопка запуска мастера настройки сети.

Чтобы добавить новую сеть, нажмите кнопку «Добавить» и выберите нужный тип сети: локальная сеть, внутренняя сеть, Wi-Fi-сеть, VPN-сеть, OpenVPN-сеть, SSTP-сеть, DMZ-сеть.

Провайдер - в терминологии МЭ «ИКС» — это WAN-интерфейс, который обеспечивает работу сервиса NAT для пользователей МЭ «ИКС». Каждому провайдеру при создании назначается один из трех возможных приоритетов, представленных в Таблице 6.

Таблица 6 – Возможные приоритеты.

Приоритет	**Значение**
Основной	Трафик от всех пользователей направляется через данного провайдера. Если у вас два или более интернет-каналов, вы можете назначить обоим провайдерам приоритет «Основной». Трафик, не проходящий через прокси-сервер, будет направляться через каждый из них посредством динамической балансировки, что позволит значительно разгрузить каналы и объединить их для повышения пропускной способности. Трафик прокси-сервера будет направлен через канал «по умолчанию».
Резервный	Трафик через провайдера не направляется до тех пор, пока работает основной. В случае отключения основного провайдера резервный занимает его место.
Дополнительный	Трафик через провайдера не направляется за исключением созданных в веб-интерфейсе статических маршрутов

Вкладка «Внешние устройства» предназначена для управления маршрутизаторами Cisco.

Вкладка «Монитор провайдеров» открывает модуль соответствующей службы, который следит за состоянием провайдеров и их переключением. При необходимости эту службу можно отключить.

Чтобы перейти в настройки провайдера, вы можете нажать на кнопку «Подробнее…» или его имя в общем списке сетей. Откроется персональная страница сведений о данном провайдере. На первой вкладке отобража.тся общее состояние провайдера и сведения о его DynDNS-сервере.

Каким образом МЭ «ИКС» понимает, что основной Провайдер 1 недоступен и пора переключиться на резервного Провайдера 2? Этот критерий определяется в детальных настройках провайдера. Для того чтобы перейти к ним, необходимо нажать кнопку «Подробно» на нужном провайдере. МЭ «ИКС» может определять доступность провайдера по следующим критериям:

- наличие сигнала в линии;
- доступность шлюза провайдера по умолчанию;

– доступность определенных внешних хостов.

Также косвенным критерием для администратора может служить доступность провайдера через сервис DynDNS. Вкладка «DynDNS» позволяет определить параметры подключаемого DynDNS-сервера.

Вкладка «Правила» позволяет назначить правила межсетевого экрана для всего трафика, проходящего через данного провайдера. Вы можете создать запрещающее или разрешающее правило, маршрут, а также ограничение скорости. Все правила, которые вы создадите, также будут отображены в списке правил межсетевого экрана.

Вкладка «События» отображает все изменения, происходящие с провайдером. По функционалу она полностью аналогична вкладке «Журнал», но более привычна для понимания пользователем.

В правой части верхней панели выпадающее меню «Сообщения» позволяет отфильтровать список событий по выбранному критерию: системные сообщения, сервисные сообщения, ошибки, остальные сообщения.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.7.3. DHCP

Модуль «DHCP» расположен в меню слева «Сеть». DHCP — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети. Его использование позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол работает по модели «клиент-сервер»: для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к серверу, и получает от него нужные параметры. В модуле «DHCP» вы можете включить/выключить DHCP-сервер, проконтролировать его работу, а также задать некоторые параметры работы.

Использование DHCP настраивается индивидуально для каждой локальной сети и выполняется в разделе «Провайдеры и сети». Для того чтобы разрешить работу DHCP в какой-то локальной сети, необходимо отредактировать ее, включить опцию «Разрешить DHCP в этой сети»

и задать диапазон адресов, которые будут раздаваться DHCP-сервером (в виде 192.168.1.1-192.168.1.100 или 192.168.1.1\16). Если DHCP не включен ни для одной локальной сети, то сервис будет находиться в состоянии «не настроен».

На вкладке «Настройки» вы можете указать параметры протокола DHCP. Выберите, что будет использоваться в качестве DNS-сервера и сервера времени для всех пользователей, получающих адреса автоматически. Установите переключатель: а) «Использовать МЭ «ИКС» как основной DNS-сервер и сервер времени»; б) «Задать адреса серверов вручную:». В этом случае будут использоваться сторонние серверы. Укажите: предпочитаемый DNS-сервер, альтернативный DNS-сервер, сервер времени. В поле «WINS-сервер» можно указать выдаваемый клиентам WINS-сервер для разрешения NetBIOS-имен. Поле «URL TFTP-сервера» позволяет указать выдаваемый клиентам TFTP, с которого может быть произведена загрузка тонкого клиента. Задайте срок аренды IP-адреса (в минутах). По истечении указанного периода, если клиент с данным адресом отсутствует в сети, запись о выдаче адреса очищается — адрес может быть выдан новому клиенту (если не задано сопоставление IP и MAC-адресов). В поле «DNS-зона для авторегистрации адресов» можно указать одну из предварительно созданных DNS-зон. В данной зоне новые пользователи, получившие адреса по протоколу DHCP, будут регистрироваться как A-записи вида <имя_хоста>.<имя_зоны>. При необходимости установите флаг «Публиковать скрипт автоконфигурации по DHCP» и выберите, каким образом будут переданы пользователю автоматические настройки прокси-сервера: а) автоматически (переключатель «Использовать скрипт автоконфигурации прокси МЭ «ИКС»»); б) вручную, из адреса, по которому находится файл с настройками (переключатель «Указать URL скрипта автоконфигурации вручную:»). Если требуется, укажите поисковый домен.

На вкладке «Адреса» вы можете увидеть всех пользователей, которые в данный момент получили адреса по DHCP. Для того чтобы одному и тому же компьютеру каждый раз выдавался один и тот же IP-адрес, необходимо задать соответствие между MAC-адресом сетевой карты и IP-адресом. Чтобы закрепить за пользователем текущий IP адрес можно воспользоваться кнопкой «Связать IP с MAC». Связи из модуля «ARP-таблица» также будут использоваться DHCP-сервером для выдачи адресов. Для того чтобы задать пользователю другой IP - скопируйте MAC и нажмите «Добавить» - «DHCP адрес». Вставьте MAC и введите новый IP - изменение произойдет по истечению срока аренды, или при повторном подключении пользователя. Для IP-адресов, присвоенных пользователям, будут отображаться имена владельцев. Клик по имени пользователя переместит вас на его страницу. DHCP-сервер использует общий список сопоставлений IP- и MAC-адресов с модулем ARP-таблица.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со

страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.8. Маскирование МЭ «ИКС»

МЭ «ИКС» является сетевым шлюзом и устанавливается на логической границе локальной сети. При этом взаимодействие узлов из разных сетей происходит через МЭ «ИКС». Получая пакеты, МЭ «ИКС» подменяет адрес отправителя на свой, тем самым происходит маскирование сетей.

5.9. Приоритизация информационных потоков, имеющих соответствующие атрибуты

Для приоритизации информационных потоков, имеющих соответствующие атрибуты в МЭ «ИКС», применяются модуль «Пользователи», описанный в разделе 4.1.1, и связанные модули по настройке доступа в сеть для каждого пользователя индивидуально. Таким образом, можно сказать, что приоритизация пользователя А над пользователем В достигается за счет настройки правил и ограничений: запрещающих, разрешающих и исключений правил; запрещающих, разрешающих и исключений правил прокси; ограничения количества соединений; ограничение скорости; выделение полосы пропускания; маршрут; квота; правило контентной фильтрации; набор правил.

5.10. Графическое отображение и управление всеми функциями

Для управления всеми функциями МЭ «ИКС» используется графический интерфейс. После установки МЭ «ИКС» графический интерфейс будет доступен из настроенной локальной сети через любой браузер. Для этого необходимо ввести в адресной строке браузера IP-адрес МЭ «ИКС», назначенный при его установке. В результате должен открыться графический интерфейс, если графический интерфейс не открылся, то в адресной строке следует указать порт 81, например, 192.168.0.1:81. При открытии графического интерфейса будет предложено ввести имя пользователя и пароль, по умолчанию логин – root, пароль – 00000. Стоит отметить, что после первого входа стоит изменить пароль администратора, для этого необходимо в модуле «Пользователи» выбрать пользователя «Администратор» и нажать «Редактировать», в открывшемся окне в поле пароль ввести новый пароль и сохранить.

Для настройки графического интерфейса необходимо в меню слева перейти «Обслуживание» - «Настройки интерфейса». Веб-интерфейс МЭ «ИКС» поддерживает два языка: русский (по умолчанию) и английский. Таймаут сессии определяет время бездействия пользователя, по окончании которого будет произведен автоматический выход из веб-интерфейса. Параметр «Разрешить авторизацию по IP» позволяет всем заведенным и авторизованным по IP-адресам пользователям получать доступ к веб-интерфейсу МЭ «ИКС» и почты. Вы можете изменить HTTP и HTTPS порты веб-интерфейса на случай, если хотите использовать порт 81 в других целях (например, для перенаправления порта или привязки виртуального хоста), а также порты для веб-интерфейса почты. Для входа в веб-интерфейс и веб-интерфейс почты по протоколу HTTPS может быть назначен заранее созданный сертификат.

Блок «Ссылки в окне авторизации». Флаг «Скрывать ссылку на веб-почту» позволяет скрывать ссылку на веб-почту в окне авторизации МЭ «ИКС». Флаг «Скрывать ссылку на Xphone» позволяет скрывать ссылку на Xphone в окне авторизации МЭ «ИКС». Флаг «Скрывать ссылку на Captive Portal» позволяет скрывать ссылку на программу авторизации Captive Portal в окне авторизации МЭ «ИКС». Флаг «Скрывать ссылку на Xauth» позволяет скрывать ссылку на программу авторизации Xauth в окне авторизации МЭ «ИКС».

5.10.1. Удаленное управление

Модуль «Удаленное управление» позволяет из веб-интерфейса главного МЭ «ИКС» заходить по защищенному каналу на веб-интерфейсы подчиненных МЭ «ИКС». Модуль расположен в меню Сеть – Удаленное управление.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий.

На вкладке «Настройки» можно включить удаленное управление и настроить его параметры. Предварительно создайте сертификаты в меню Защита - Сертификаты. В общем случае для функционирования удаленного управления необходимо создать три сертификата на МЭ «ИКС» с ролью «Сервер»: корневой сертификат, конечный сертификат для сервера, конечный сертификат для клиента. При создании корневого сертификата выберите тип «CA». При создании конечного сертификата для сервера в поле «Имя или адрес хоста» укажите доменное имя системы либо внешний IP-адрес МЭ «ИКС» с ролью «Сервер». Выберите тип сертификата «Конечный сертификат». В качестве шаблона рекомендуется выбрать «VPN-сервер». При создании конечного сертификата для клиента укажите тип сертификата «Конечный сертификат». В качестве шаблона рекомендуется выбрать «VPN-клиент». В меню Сеть - Удаленное управление - Настройки установите флаг «Использовать удаленное управление». Выберите режим работы МЭ «ИКС»: сервер либо клиент. Если выбран режим «Сервер», данный МЭ «ИКС» будет выступать в роли сервера, а остальные МЭ «ИКС» будут подключаться к нему. Также станет доступен флаг

«Автоматически создавать разрешающее правило» для создания разрешающего правила в наборе правил межсетевого экрана. Для данного режима работы выберите корневой сертификат и конечный сертификат для сервера. Если выбран режим «Клиент», данный МЭ «ИКС» будет выступать в роли клиента и им можно будет управлять с МЭ «ИКС», который выступает в роли сервера. Также станут доступными для заполнения поля «ID» и «IP сервера». В поле «ID» указывается уникальный идентификатор клиента, генерируемый автоматически, но его можно изменить. ID устанавливается в формате «node- * * * * * * * *», где '*' — это цифра или любой латинский символ (регистр учитывается). В поле «IP сервера» можно указать как IP-адрес, так и доменное имя сервера. Для данного режима работы выберите корневой сертификат и конечный сертификат для клиента.

В МЭ «ИКС» с ролью «Сервер» на вкладке «Узлы» содержится перечень всех МЭ «ИКС» с ролью «Клиент», которые были подключены к удаленному управлению. Перечень представлен в виде таблицы с указанием следующих данных о клиентах: имя, ID, IP-адрес, статус (подключен, не подключен), описание (для занесения пометок от системного администратора). На вкладке также можно редактировать либо удалять доступные поля клиентов. Чтобы перейти в веб-интерфейс удаленного клиента, дважды нажмите на него левой кнопкой мыши.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.10.2. Application Firewall

Модуль «Application Firewall» предназначен для отслеживания и блокирования трафика пользователей на основании категорий библиотеки nDPI, а также соединений пользователей, которые подключаются к МЭ «ИКС» через утилиту Xauth. Модуль расположен в меню Защита - Application Firewall.

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий.

Вкладка «Настройки» предназначена для настройки работы Application Firewall. На вкладке можно выбрать доступные сети, в которых будет производиться сканирование соединений пользователей. По умолчанию установлены локальные сети.

На вкладке «Заблокированные соединения» отображается список заблокированных соединений тех пользователей, которым назначены запрещающие правила Application Firewall или у которых заблокированы процессы Xauth.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.10.3. Техподдержка

Модуль «Техподдержка» расположен в меню Обслуживание – Техподдержка и предназначен для предоставления доступа к МЭ «ИКС» сотруднику технической поддержки. Это может быть полезно для получения помощи по настройке МЭ «ИКС» или устранения каких-либо возникающих проблем в тех случаях, когда МЭ «ИКС» находится:

– за межсетевым экраном, который запрещает входящие соединения;

– в серой сети за NAT-устройством (модем, роутер).

На главной вкладке модуля отображается следующая информация: статус службы, кнопки «Включить» и «Выключить» службу, журнал последних событий. После старта модуля в сводке под названием службы отобразится порт подключения (обычно это порт 20xxx). Для удаленного подключения сообщите номер порта сотруднику технической поддержки: наши контакты.

Вкладка «Журнал» отображает сводку всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение, подключение пользователя) - зеленым, предупреждения – желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные

журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

5.10.4. О программе

В модуле «О программе» отображается основная информация об установленной версии МЭ «ИКС». Модуль расположен в меню Обслуживание – О программе.

На вкладке «О программе» отображаются следующие сведения:

- текущая версия МЭ «ИКС»;
- серийный номер;
- срок действия модуля «Техподдержка» либо тестового периода;
- количество подключенных к системе пользователей;
- кнопка «Переактивация»/«Получить лицензию» — позволяет активировать сервер;
- телефон технической поддержки;
- ссылка на главную страницу официального сайта;
- кнопка «Задать вопрос» — переводит на форму для отправки вопроса.

На вкладке «Лицензионное соглашение» можно прочесть лицензионное соглашение, заключенное с правообладателем программы МЭ «ИКС».

5.11. Взаимодействие с другими средствами защиты информации, такими как антивирусные программные продукты

Для управления средствами защиты информации в МЭ «ИКС» были разработаны следующие модули: Антивирус ClamAV, Антивирус Касперского, Антиспам Касперского, Веб-фильтр Касперского. Настройка всех модулей происходит в меню слева «Защита».

5. АВАРИЙНЫЕ СИТУАЦИИ. ВОССТАНОВЛЕНИЕ МЭ «ИКС»

5.1. Процедура резервного копирования и восстановления

В случае программных или аппаратных сбоев, когда загрузка штатным образом МЭ «ИКС» или ОС невозможна, необходимо заново установить МЭ «ИКС» и провести процедуру восстановления:

Процедуры аварийного восстановления выполняются при помощи модуля «Резервные копии» с использованием ранее созданных резервных копий ПО МЭ «ИКС» или образа системы.

5.2. Выключение аппаратной платформы

Для корректного выключения аппаратной платформы необходимо нажать кнопку «Выключить МЭ «ИКС»» или «Перезагрузить МЭ «ИКС»» в меню «Обслуживание» – «Управление питанием» или аналогичные пункты в меню «Настройка сервера» консоли восстановления.

5.3. Создание резервных копий

Процедура резервного копирования МЭ «ИКС».

Для создания резервной копии ПО МЭ «ИКС» в веб-интерфейсе перейдите в меню «Обслуживание» - «Резервные копии».

В данном разделе необходимо выполнить следующие действия:

- нажать копку «Добавить» и выбрать пункт «Резервная копия»;
- в открывшемся окне выбора данных для резервирования отметить флажками нужное;
- нажать кнопку «Добавить». Начнется резервное копирование данных. Будет создана резервная копия в формате <имя системы>-<дата>-<время создания>-<обозначение содержания резервной копии>-<версия «ИКС»>-backup. Если в резервную копию не попали какие-либо папки, это будет отмечено в описании к копии (например, Резервная копия (настройки, файлы: primary/First_level(-primary/First_level/Second_level))). При создании резервной копии происходит сжатие данных;
- во избежание потери резервных копий в случае аппаратного сбоя МЭ «ИКС» рекомендуется сохранить резервную копию системы на отдельном носителе. Для этого следует выделить требуемую резервную копию, нажать кнопку «Скачать» и указать место, куда будет сохранена копия.

Автоматизация резервного копирования.

В программе реализована возможность автоматического создания резервных копий с указанной частотой и на указанные носители информации.

Вкладка «Шаблоны» позволяет гибко настроить автоматическое резервное копирование

выбранных данных в указанное время. В МЭ «ИКС» есть два предустановленных шаблона: «Резервная копия настроек» (сохраняет только настройки МЭ «ИКС») и «Полная резервная копия» (сохраняет полную резервную копию МЭ «ИКС»). Для активации одного из шаблонов укажите время его срабатывания в окне редактирования.

Во вкладке «Настройки» можно указать периодичность создания копии (только настройки, полная резервная копия, остальные резервные копии).

Резервную копию можно сохранять как на жесткий диск МЭ «ИКС» (блок «Жесткий диск для хранения резервных копий»), так и на съемный носитель (блок «Автоматически копировать резервную копию на флеш-накопитель») либо на удаленный FTP-сервер (блок «Копировать резервные копии на FTP-сервер»). Это позволит обезопасить данные резервных копий на случай разрушения жесткого диска.

5.4. Восстановление настроек системы

При установке программы на другую аппаратную часть или восстановления системы после сбоя необходимо произвести развертывание резервной копии системы:

- в модуле «Резервные копии» нажать кнопку «Загрузить» и указать место хранения резервной копии;
- после того как резервная копия появится в списке доступных резервных копий программы, выберите ее и нажмите кнопку «Восстановить», на запрос системы о целесообразности выполняемого действия ответьте «Да»;
- второй метод восстановления системы – из консоли восстановления. В ней нужно выбрать меню Управление сервером – Резервные копии. Появится список доступных резервных копий.

5.5. Восстановление свойств МЭ «ИКС» после сбоев и отказов оборудования

Процедура восстановления свойств МЭ «ИКС» после сбоев и отказов оборудования:

- осуществить отключение ПЭВМ 5 от электропитания;
- осуществить подключение ПЭВМ 5 к сети электропитания;
- осуществить включение ПЭВМ 5;
- дождаться загрузки ПО МЭ «ИКС»;
- в случае выявления ошибок во время загрузки ПО МЭ «ИКС» необходимо переустановить ПО МЭ «ИКС».

5.6. Использование консоли восстановления

Консоль восстановления — это служебный интерфейс МЭ «ИКС», работающий в

текстовом режиме. Для того чтобы воспользоваться средствами консоли, существуют два способа:

- подключить к МЭ «ИКС» монитор и клавиатуру;
- воспользоваться любым SSH-клиентом (например, Putty) и подключиться на 22 порт МЭ «ИКС» (в этом случае в модуле «Межсетевой экран» → «Настройки» должен быть разрешен доступ по протоколу SSH с хоста, с которого производится подключение), по умолчанию логин - recshell, пароль - recovery.

Консоль восстановления позволяет произвести следующие операции:

- Проверка и корректировка таблицы маршрутизации МЭ «ИКС» (пункт меню Настройка сети - Маршрутизация). Здесь администратор может просмотреть текущую таблицу маршрутизации, удалить какой-либо из маршрутов либо добавить новый.
- Проверка и корректировка сетевых интерфейсов МЭ «ИКС» (пункт меню Настройка сети - Сетевые интерфейсы). Пользователь может вывести информацию по состоянию каждого из интерфейсов, проверить, подключен ли сетевой кабель (у подключенного интерфейса status: active), верно ли назначены IP-адреса, при необходимости удалить IP-адрес с интерфейса, а также назначить новый.
- Выключение межсетевого экрана (пункт меню Настройка сети - Межсетевой экран). В случае, если МЭ «ИКС» по каким-либо причинам блокирует доступ к веб-интерфейсу, можно временно отключить межсетевой экран до устранения причины блокировки.

Утилиты Ping и Trace (Настройка сети - Утилиты). Позволяют проверить доступность локального или удаленного хоста.

Смена пароля на аккаунт администратора и на вход в консоль восстановления (Управление сервером - пароли).

Добавление диска в зеркальный массив (Управление сервером - RAID).

Обновление конфигурации МЭ «ИКС» (Управление сервером - обновление всех настроек).

Перезагрузка (Управление сервером - перезагрузка).

Выключение (Управление сервером - выключение).

Консоль восстановления является вспомогательным инструментом для диагностики неисправностей МЭ «ИКС». Все изменения, произведенные в ней, за исключением смены паролей и установки дисков в массив, будут сброшены при любом изменении в веб-интерфейсе МЭ «ИКС» или после перезагрузки.

5.7. Инструменты виртуализации

МЭ «ИКС» может быть установлено на виртуальную машину. Если в качестве основной системы используется VmWare, то для более тесной интеграции систем в МЭ «ИКС» установлены Vmware Tools 5.

МЭ «ИКС» поддерживает установку на следующие системы виртуализации:

- VMware Workstation и VMware ESXi
- VirtualBox
- Hyper-V

6. СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

В зависимости от ситуации, в графическом интерфейсе, МЭ «ИКС» может выдавать: предупреждающие сообщения, которые требуют вмешательства системного администратора; информационные сообщения; сотрясание (shake) диалогового окна – отказ МЭ «ИКС» принять введенные данные.

«До окончания срока активации осталось … дней» – сообщение, напоминающее об оставшемся сроке эксплуатации незарегистрированного МЭ «ИКС».

«Тестовый срок истек» – сообщение, информирующее о том, что срок эксплуатации незарегистрированного МЭ «ИКС» истек, и дальнейшая эксплуатация возможна только после регистрации программы.

«Вы действительно хотите выключить сервис?» – система запрашивает администратора подтверждение выключения выбранной службы.

«Вы действительно хотите удалить эти элементы?» – система запрашивает администратора подтверждение удаления выбранных данных.

«Вы действительно хотите удалить файл лицензии?» – запрос на подтверждение удаления лицензионного регистрационного файла модуля.

«Не удалось зарегистрироваться на сервере активации» – нет интернет-доступа к серверу активации компании «А-Реал Консалтинг».

«Вы действительно хотите добавить диск в раздел?» – запрос на подтверждение перемещения неиспользуемого диска в созданный раздел.

«Данная операция необратима. Удалить диск из раздела можно будет только удалив сам раздел!» – сообщение о невозможности обратного процесса при перемещения дополнительного жесткого диска в раздел.

«Не удалось получить список пользователей домена. Возможно МЭ «ИКС» не является членом домена» – сообщение появляется при импорте пользователей из домена в случае, если программа не подключена к контроллеру домена.

«Вы действительно хотите выключить (перезагрузить) сервер?» – система запрашивает администратора подтверждение выключения (перезагрузки) аппаратной части МЭ «ИКС».

«Конфликт со следующими сетевыми интерфейсами:» – в программе назначены IP-адреса одного сетевого диапазона на разных сетевых интерфейсах.

«Вы действительно хотите восстановить резервную копию?» – запрос на подтверждение восстановления системы из сохраненной резервной копии.

«Не удалось загрузить статистику» – сообщение появляется в модуле «Пользователи» во время динамической загрузки статистики в том случае, если связь с сервером утеряна.

«Не удалось сохранить» – при нормальной работе программы сообщение возникает в двух

случаях: если утеряна связь с сервером в момент сохранения какого-либо параметра либо в случае слишком долгого выполнения запроса за время, превышающее допустимое. В ином случае данное сообщение свидетельствует о неверной работе МЭ «ИКС».

«Не удалось получить пользователей. Проверьте параметры подключения.» – сообщение, возникающее при указании не верных настроек подключения к контроллеру домена.

«Сохранение настроек…» – модуль сохраняет настройки и недоступен для редактирования и просмотра.

«Загрузка…» – модуль загружает данные и недоступен для редактирования и просмотра.

«Выполняется активация» – идет процесс активации программы.

«Восстановление резервной копии...» – идет процесс развертывания сохраненной резервной копии.

«Синхронизация…» – идет процесс синхронизация сервера времени с выбранным внешним сервером.

«Удаление…» – идет процесс удаления элемента программы.

«Перемещение…» – идет процесс перемещения пользователя или группы на другой уровень.

А все системные сообщения МЭ «ИКС» можно просмотреть в меню слева «Обслуживание» – «Журнал и уведомления».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводит. докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					