

Установка ИКС

Запись диска

Для установки «ИКС», необходимо скачать образ установочного диска с <https://xserver.a-real.ru/download>. Затем нужно записать этот образ на компакт-диск.

Чем можно записать .iso-образ?

После скачивания образа, необходимо записать его на компакт-диск. Сделать это возможно практически любой программой для записи компакт-дисков, например: Nero Burning ROM, Alcohol 120%, CDBurnerXP, UltraISO и др.

Внимание! Записывать .iso-образ на диск нужно именно в режиме «записать образ\burn image». После того, как файл на диск будет записан, необходимо загрузиться с компакт-диска на том компьютере, на котором будет работать «ИКС».

Минимальные требования к оборудованию, на котором будет работать «ИКС», представлены на <https://xserver.a-real.ru/download/>. Для загрузки с установочного диска, необходимо включить в BIOS оборудования опцию загрузки с CDROM.

Загрузка

Что должно произойти после загрузки с установочного диска?

После загрузки с установочного диска, вы должны увидеть сообщения загрузчика.

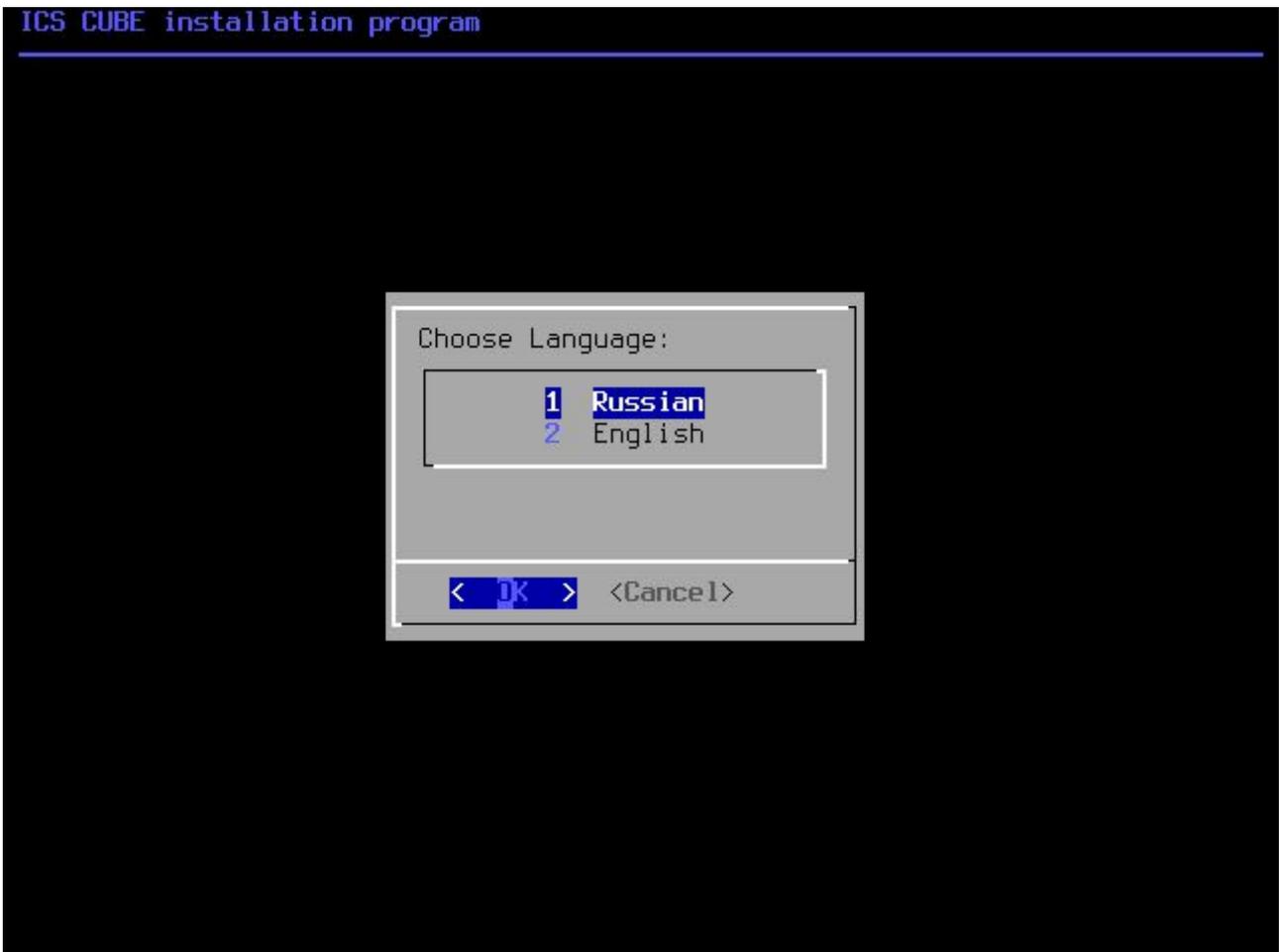
```
CD Loader 1.2

Building the boot loader arguments
Looking up /BOOT/LOADER... Found
Relocating the loader and the BTX
Starting the BTX loader

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive A: is disk0
BIOS drive C: is disk1
BIOS 638kB/260032kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.1
(root@logan.cse.buffalo.edu, Thu Jan  1 09:55:10 UTC 2009)
Loading /boot/defaults/loader.conf
/boot/kernel/kernel text=0x75f60c _
```

Дождитесь окончания процесса загрузки, на экране появится приветствие и окно выбора языка установки



Далее необходимо принять лицензионное соглашение, выбрать вариант работы «Установка».

Затем предлагается выбрать текущий часовой пояс.

Внимательно прочтите текст лицензионного соглашения, приведенный ниже. Нажатием на кнопку "Принимаю", вы обязуетесь соблюдать все условия лицензионного соглашения.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Настоящее лицензионное соглашение является юридическим соглашением, заключаемым между пользователем (физическим или юридическим лицом, далее "ПОЛЬЗОВАТЕЛЬ") и ООО А-Реал Консалтинг (далее "ПРАВООБЛАДАТЕЛЬ"). Действие лицензионного соглашения распространяется на программный комплекс "Интернет Контроль Сервер", включающей в себя программное обеспечение и любую "встроенную" или "электронную" документацию (далее "ПРОДУКТ").

ВНИМАНИЕ: Установка ПРОДУКТА к корпоративной сети ПОЛЬЗОВАТЕЛЯ означает согласие ПОЛЬЗОВАТЕЛЯ с условиями настоящего лицензионного соглашения.

1.1. Исключительное право собственности на ПРОДУКТ принадлежит компании-ПРАВООБЛАДАТЕЛЮ. Право использования одного экземпляра продукта на определенных условиях делегируется ПРАВООБЛАДАТЕЛЕМ ПОЛЬЗОВАТЕЛЮ в виде лицензии на использование ПРОДУКТА.

1.2. Настоящее лицензионное соглашение предоставляется пользователю в электронном виде.

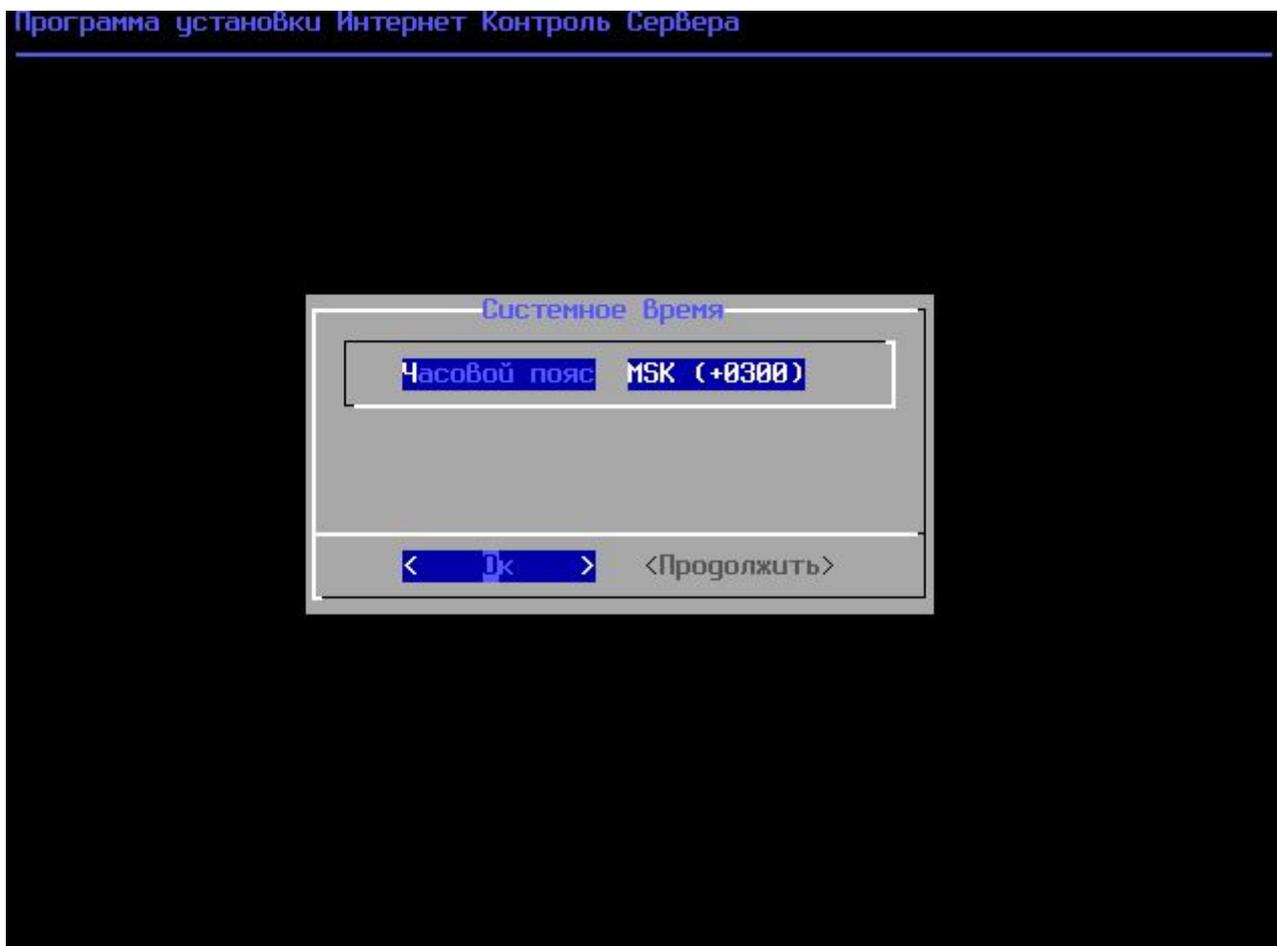
1.3. ПРОДУКТ является неделимым программным комплексом, отдельные

↓(+)

25%

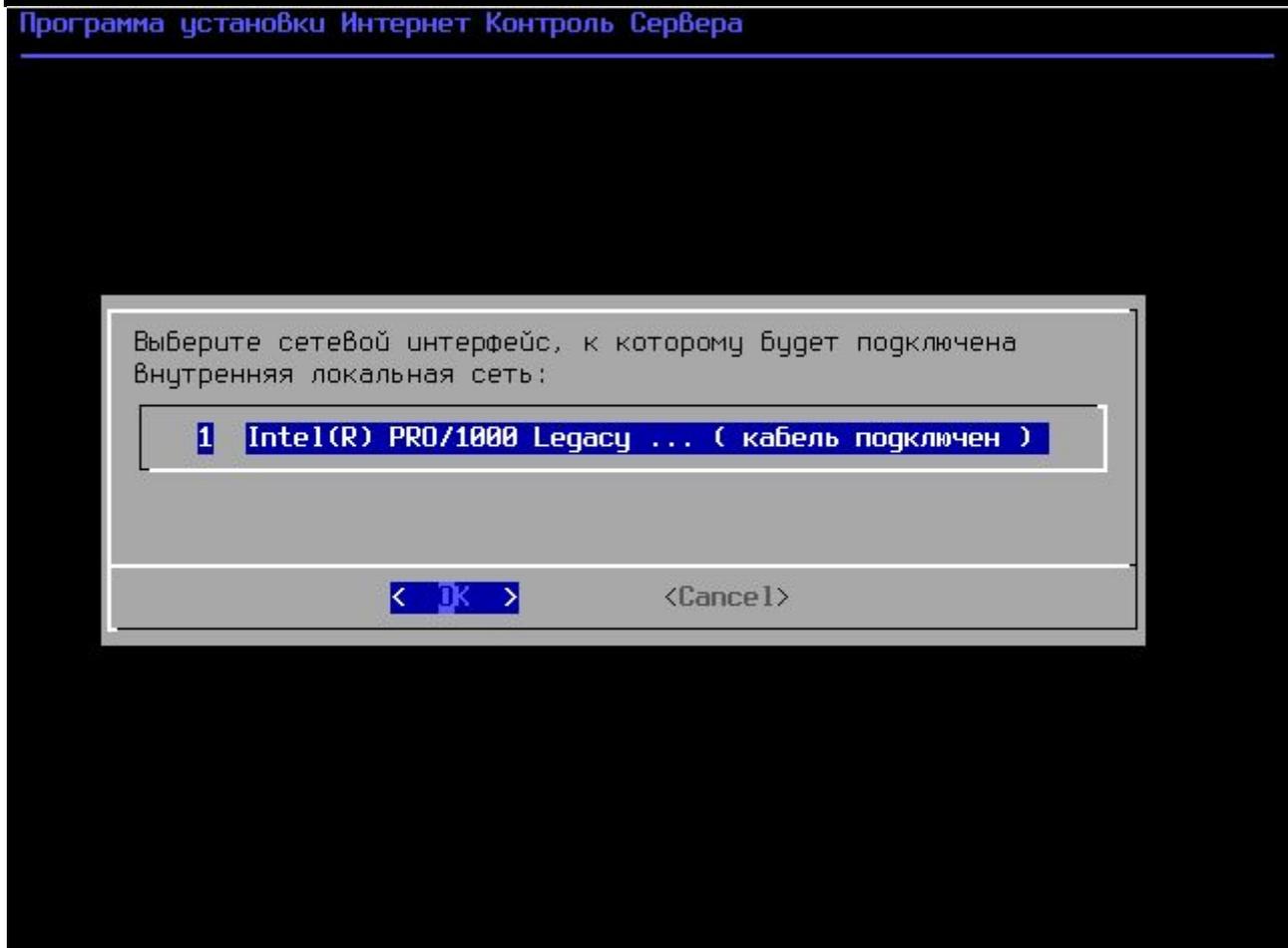
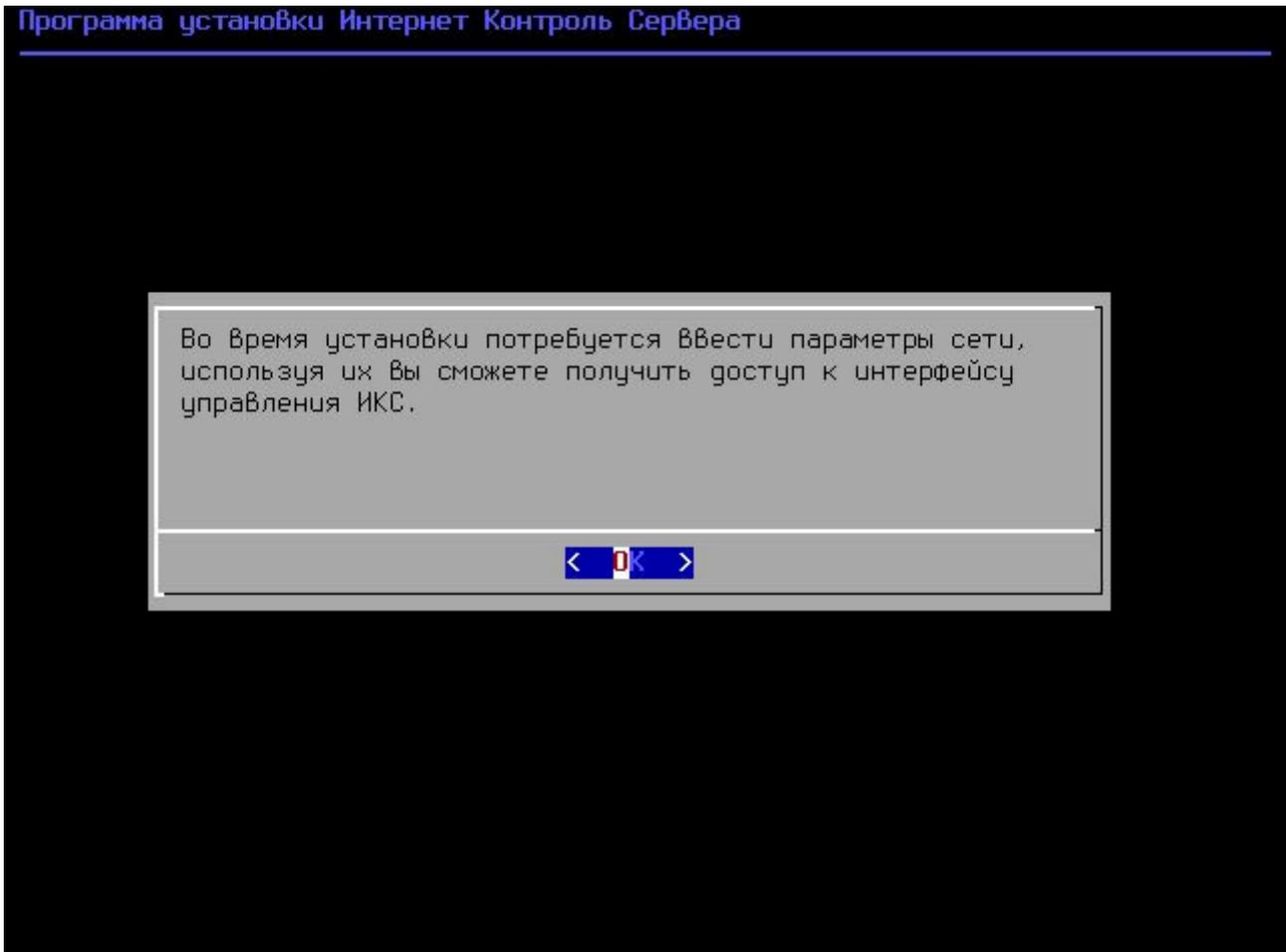
Не принимаю

Принимаю >



Подсказка: переключение между кнопками в режиме установки системы осуществляется при помощи клавиши TAB.

Настройка сети



Программа установки Интернет Контроль Сервера

Введите ip-адрес ИКС для
интерфейса 'Intel(R)
PRO/1000 Legacy Network
Connection 1.1.0':

192.168.0.1

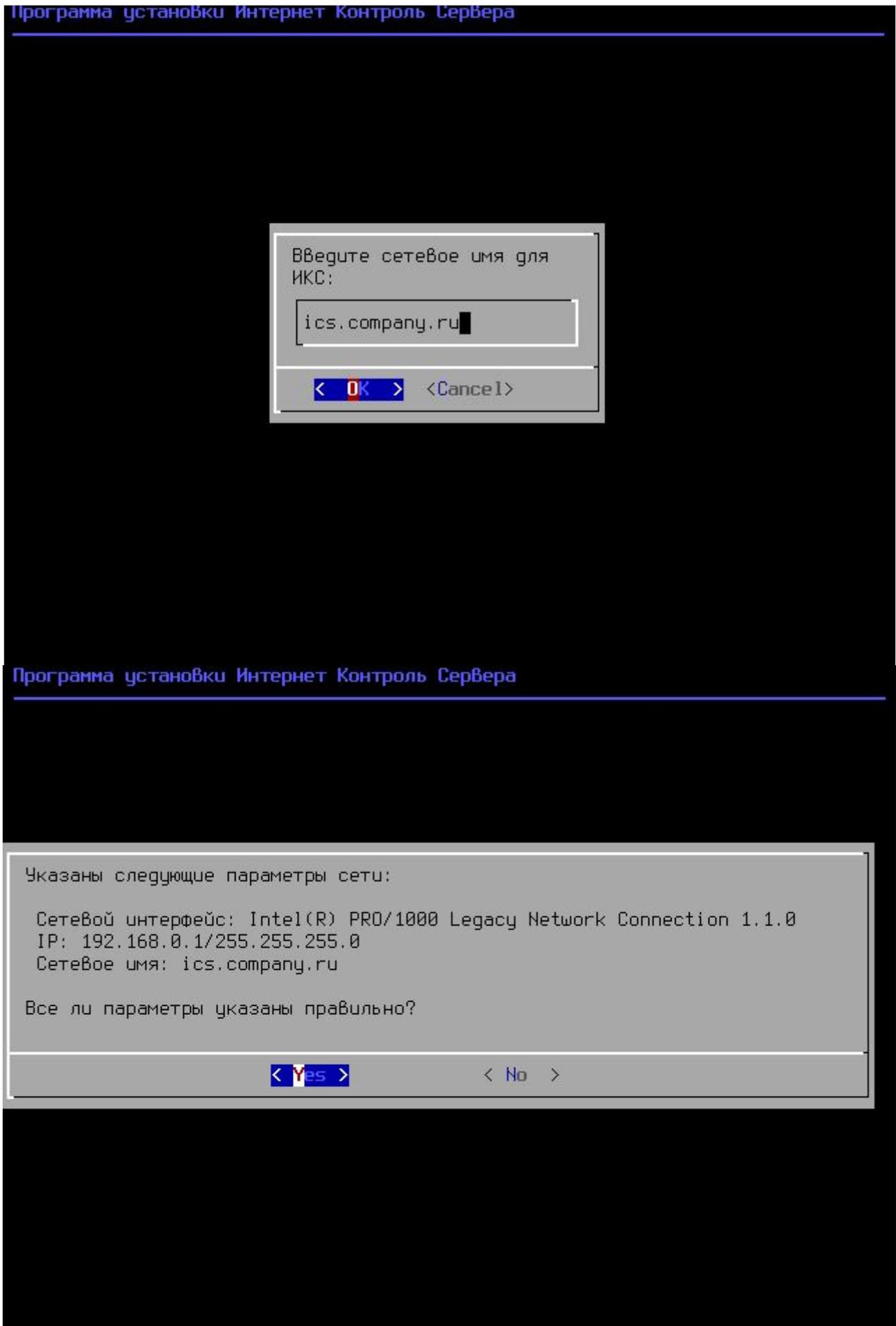
< OK > <Cancel>

Программа установки Интернет Контроль Сервера

Введите ip-адрес ИКС для
интерфейса 'Intel(R)
PRO/1000 Legacy Network
Connection 1.1.0':

192.168.0.1

< OK > <Cancel>



Основное управление сервером будет осуществляться через веб-интерфейс. Для того, чтобы

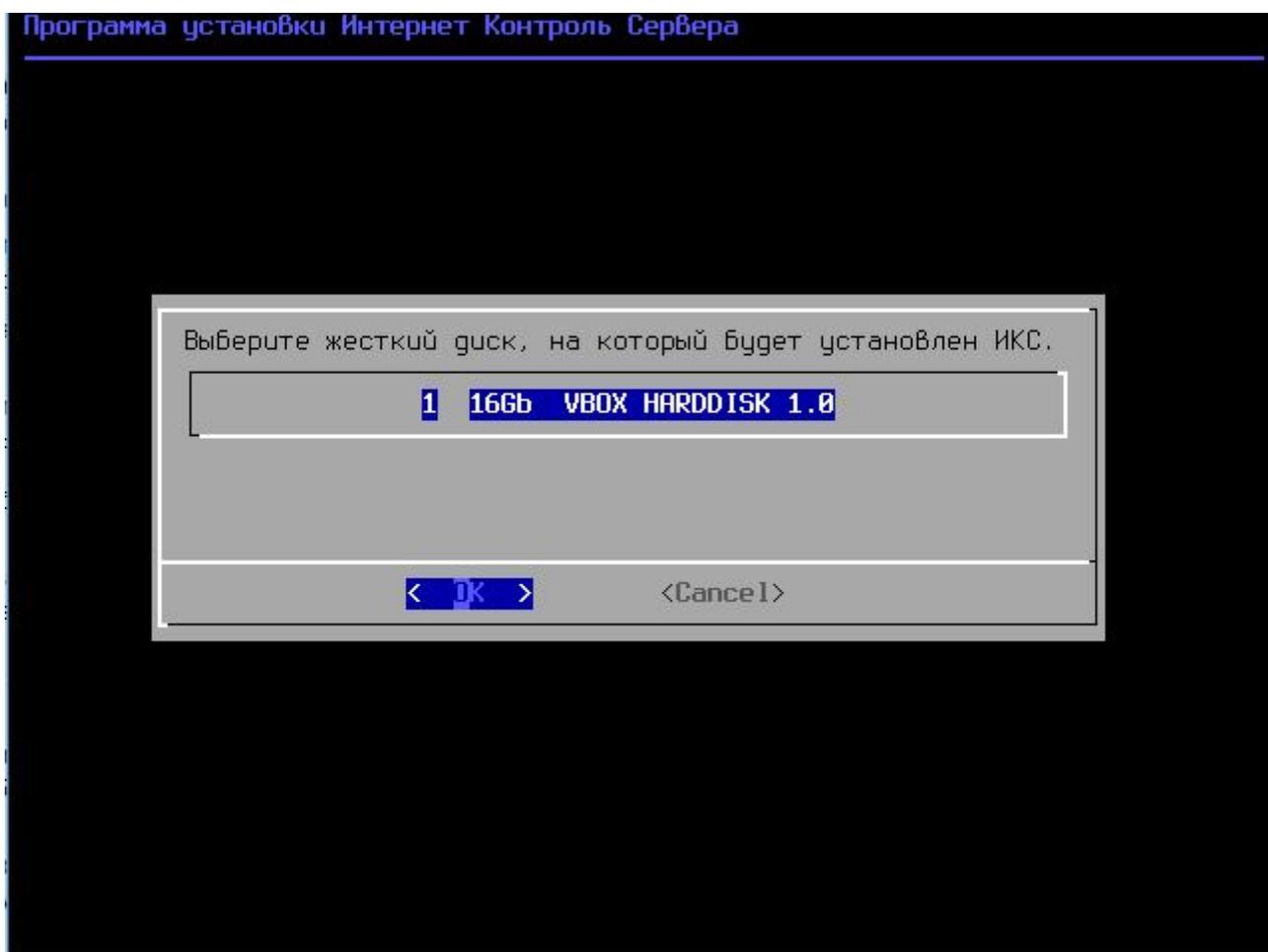
получить доступ к веб-интерфейсу после установки, необходимо указать серверу сетевой адаптер, который подключен **к вашей локальной сети**.

На следующем шаге будет предложено задать настройки IPv4 (IP-адрес, маску сети и, необязательный параметр, шлюз по умолчанию) для выбранного сетевого интерфейса.

Внимание! Шлюз по умолчанию будет удален в случае добавления локальной сети в веб-интерфейсе «ИКС» или изменен в случае добавления провайдера в веб-интерфейсе.

В следующем диалоговом окне будет предложено ввести сетевое имя для «ИКС».

Выбор диска

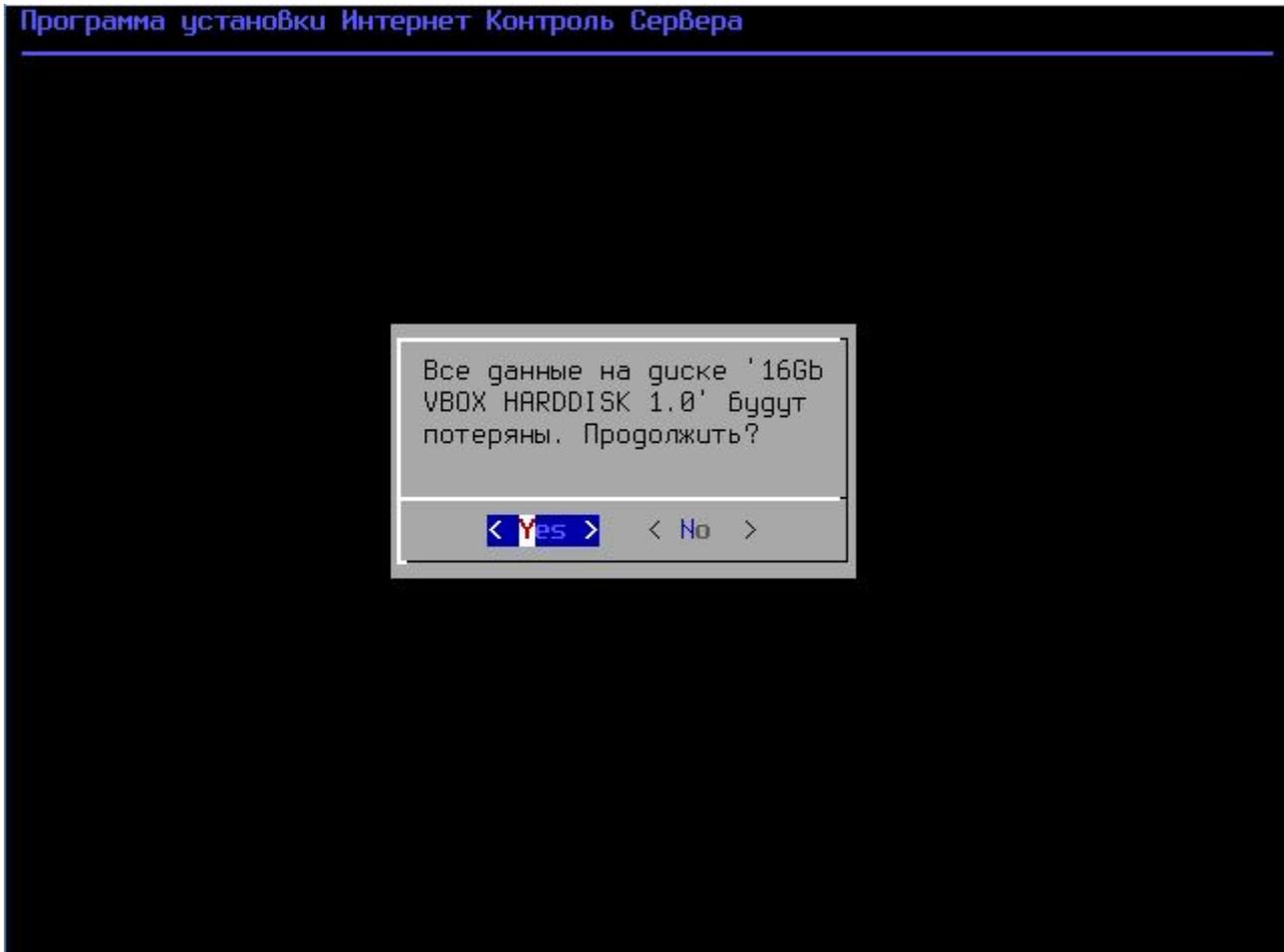


В следующем диалоговом окне необходимо выбрать параметр RAID для «ИКС» (по умолчанию это RAID-1 (mirror)). Параметр RAID-1 не обязывает сразу иметь несколько жестких дисков, их можно добавить со временем.

На следующем шаге программа установки попросит указать жёсткий диск, на который будет производиться инсталляция. В случае установки на RAID-1 возможно выбрать необходимое количество доступных жестких дисков, на которые произойдет установка «ИКС» и они будут объединены в mirror.

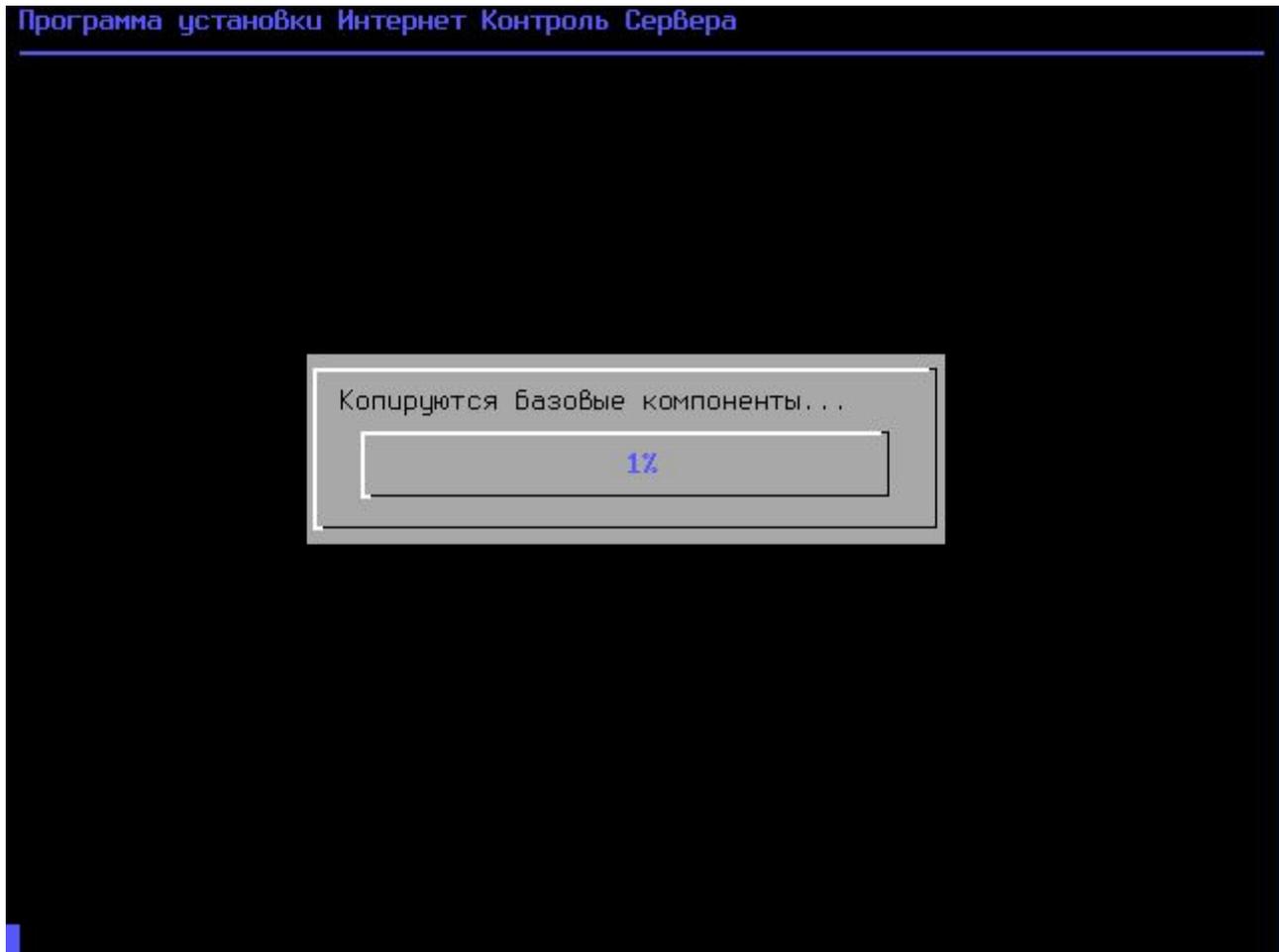
Минимальный объём жёсткого диска зависит от задач, выполняемых сервером. Для большинства задач с небольшим количеством пользователей и без хранения значительного объема данных (почта, файлы, длительное хранение статистики) достаточно жёсткого диска, объёмом **120 Гб**.

Программа установки самостоятельно разметит и отформатирует жёсткий диск. Никакая предварительная разметка **не требуется**.



Внимание! Все данные на выбранном диске будут безвозвратно удалены!

Далее запустится процесс копирования файлов на жёсткий диск. Как правило, этот процесс занимает несколько минут, и по его завершении программа установки попросит вас извлечь установочный диск из дисковод.



После этого последует перезагрузка компьютера и запустится процесс установки компонентов «ИКС».

Завершение установки

По завершении установки сервера, появится сообщение следующего содержания:

```
OK Starting service bind
OK Starting service asterisk
OK Starting service arp
OK Starting service overmind
--- Starting service backup
checkdisks... ok
migrate... create CFilterRegex /usr/local/ics/cf/var/defaults/skydnsSchool.keywo
migrate... .....+.....+.....
.....+.....
.....
migrate... mv: rename /usr/local/*/info/*disabled to /data/settings/services/*di
migrate... INSERT INTO MigrationModel SET `version`="6.1.0.190221",`migrateVersi
migrate... ok
checkdisks... ok
rebuild... ok

Internet Control Server loaded

[F1] message screen
[F2] recovery console

Установка ИКС завершена!
Для входа в web-интерфейс используйте
логин: root
пароль: 00000
URL: https://192.168.0.1:81

Fri Mar 1 22:19:43 MSK 2019
```

На этом установка Интернет Контроль Сервера завершена. Дальнейшую настройку «ИКС» необходимо выполнять через веб-интерфейс.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:setup>

Last update: **2019/11/10 19:25**



Установка ИКС на виртуальную машину

Виртуальная машина (virtual machine) — программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы и исполняющая программы для этой платформы (target — целевая или гостевая платформа) на другой платформе (host — хост-платформа, платформа-хозяин) или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы.

В некоторых случаях нецелесообразно выделять под работу ИКС отдельный физический компьютер, для этой цели подойдет виртуальная машина. К примеру, в небольшом офисе вы можете установить ИКС на виртуальную машину сервера или даже любой рабочей станции, что позволит сэкономить расходы на электроэнергию и покупку дополнительной техники.

В настоящее время ИКС поддерживает установку на следующие системы виртуализации:

- [VMWare Workstation и VMWare ESXi](#)
- [Virtual Box](#)
- [Microsoft Hyper-V](#)

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:virtual_machine

Last update: **2019/11/19 13:48**



Установка ИКС на платформу VMWare

VMWare Workstation

VMware Workstation — виртуальная машина компании VMware для платформ x86 и x86-64.

Для того, чтобы установить ИКС на виртуальную платформу, вам потребуется компьютер с установленной VMWare Workstation.

В нашем примере мы рассмотрим установку на VMWare 5. Запустите виртуальную среду, нажмите File → New... → Virtual machine...

В окне выбора «Select the Appropriate Configuration» укажите «Typical».

В окне выбора операционной системы укажите Other → FreeBSD.

Далее задайте имя создаваемой машины и папку, где будет храниться файл образа.

В окне выбора «Network type» выберите Use bridged networking.

Следующее окно позволит указать размер создаваемого виртуального жесткого диска, после чего виртуальная машина будет создана.

По умолчанию в виртуальной машине создан один сетевой адаптер. Для полноценной работы ИКС необходимо как минимум два. Нажмите правой кнопкой на имя созданной виртуальной машины и выберите пункт Settings... В открывшемся окне во вкладке Hardware нажмите кнопку Add... Выберите в списке создаваемого оборудования Ethernet adapter, в его свойствах выберите Bridged.

Не покидая окно настроек виртуальной машины, выберите в списке виртуальных устройств CD-ROM. В разделе Connection переключите с параметра Use physical drive на Use ISO-image, нажмите кнопку Browse... и укажите файл-образ ИКС, скачанный с нашего сайта.

Нажмите ОК и запустите виртуальную машину. Начнется загрузка установщика ИКС аналогично [обычной установке ИКС на компьютер](#).

Важно: для того, чтобы между физической и виртуальной машинами установилась связь по IP-адресам, необходимо, чтобы в сетевую карту компьютера был вставлен сетевой кабель.

VMWare ESXi

VMware ESX Server — операционная система виртуализации, которая позволяет разделить физический компьютер на логические разделы, называемые виртуальными машинами. Включает в себя средства управления виртуальными ресурсами. По существу представляет собой гипервизор, что подразумевает установку раньше любой другой операционной системы.

Для установки новой виртуальной машины запустите клиент vSphere. В этом примере используется VMWare ESXi 4.0.0.

Нажмите File → New... → Virtual machine...

В окне Configuration укажите «Typical».

Далее задайте имя создаваемой машины.

В окне Resource pool выберите коннективный пул машин, в котором будет находиться новая система.

В окне Datastore укажите жесткий диск, на котором будет создан файл-образ новой виртуальной машины.

В окне выбора операционной системы укажите Other → FreeBSD.

Следующее окно позволит указать размер создаваемого виртуального жесткого диска, подтвердите параметры кнопкой Finish, после чего виртуальная машина будет создана.

Добавьте второй (или несколько) сетевой адаптер и укажите файл-образ ИКС аналогично работе с VMWare Workstation. Запустите виртуальную машину. Начнется загрузка установщика ИКС аналогично [обычной установке ИКС на компьютер](#).

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:vmware>

Last update: **2019/12/12 14:37**



Установка ИКС на VirtualBox

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Microsoft Windows, Linux, FreeBSD, Mac OS X, Solaris/OpenSolaris, ReactOS, DOS и других, разработанный компанией Innotek, в настоящее время принадлежит компании Oracle Corporation.

Для того, чтобы установить ИКС на виртуальную платформу, вам потребуется компьютер с установленной VirtualBox.

В нашем примере мы рассмотрим установку на VirtualBox 3. Запустите виртуальную среду, нажмите Создать.

Присвойте виртуальной машине имя и выберите операционную систему BSD → FreeBSD.

В окне настроек памяти укажите размер оперативной памяти (RAM), используемой новой виртуальной машиной.

Следующее окно позволит выбрать загрузочное устройство, на котором будет располагаться виртуальная машина либо создать новый виртуальный жесткий диск. Если у вас еще нет созданных дисков, выберите создание нового. После выбора этой опции запустится мастер создания виртуального диска. В нем укажите опцию «Образ фиксированного размера» и определите размер создаваемого диска.

После создания диска виртуальная машина будет готова.

По умолчанию в виртуальной машине создан один сетевой адаптер. Для полноценной работы ИКС необходимо как минимум два. Нажмите правой кнопкой на имя созданной виртуальной машины и выберите пункт Свойства. В открывшемся окне в разделе Сеть измените режим работы текущего адаптера на «Сетевой мост» и выберите сетевую карту, которая будет использоваться. Перейдите во вкладку «Адаптер 2», установите флажок «Включить сетевой адаптер» и также выберите режим работы «Сетевой мост» с указанием реального сетевого интерфейса.

Не покидая окно настроек виртуальной машины, выберите раздел CD/DVD-ROM. Установите флажок «Подключить CD/DVD», выберите опцию «Файл ISO-образа», нажмите кнопку выбора виртуальных образов. В открывшемся окне нажмите кнопку «Добавить» и укажите файл-образ ИКС, скачанный с нашего сайта. Отметьте появившийся файл в списке и нажмите кнопку «Выбрать». Подтвердите настройки, нажав кнопку ОК.

Нажмите ОК и запустите виртуальную машину. Начнется загрузка установщика ИКС аналогично [обычной установке ИКС на компьютер](#).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:vbox>

Last update: **2019/11/19 13:49**



Установка на Hyper-V

Microsoft Hyper-V — система аппаратной виртуализации для x64-систем на основе гипервизора. Ранее была известна как виртуализация Windows Server (Windows Server Virtualization)

После запуска гипервизора выбираем Создать - виртуальная машина. Даем ей произвольное имя, нажимаем далее, указываем количество оперативной памяти для работы.

Затем указываем виртуальную сеть, к которой будет подключена машина, определяем размер жесткого диска.

В следующем окне мастер спросит источник установки системы. Выбираем «установить с загрузочного диска», «файл iso-образа» и указываем скачанный образ с ИКС, нажимаем далее и в последнем окне нажимаем Готово.

После создания машины необходимо добавить ей еще один сетевой адаптер. У выделенной машины нажимаем Параметры, в окне редактирования выбираем Установка оборудования - сетевой адаптер и присваиваем его той же виртуальной сети.

Нажимаем ОК, щелкаем правой кнопкой по машине - подключить. В отдельном окне запустится машина. Нажимаем Действие - Пуск. Машина запустилась, началась установка ИКС.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:hyperv>

Last update: **2019/11/19 13:49**



Установка с флешки

Кроме установки с CD-ROM ИКС позволяет записать образ на flash-накопитель и установить с него.

Сначала вам необходимо скачать специальный образ для записи на накопитель. Скачать его можно [здесь](#) (необходимо выбрать образ FLASH).

После этого запишите образ любой утилитой для создания загрузочных носителей (к примеру Rufus)

По окончании процесса установите флешку в USB-порт компьютера, на который будет установлен ИКС и укажите в BIOS'e USB-flash в качестве первичного загрузочного устройства.

Внимание: не все модели материнских плат поддерживают установку с USB-flash-устройств!

Когда образ загрузится с накопителя, начнется установка в [обычном режиме](#).

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:usb_setup

Last update: **2019/11/10 19:25**



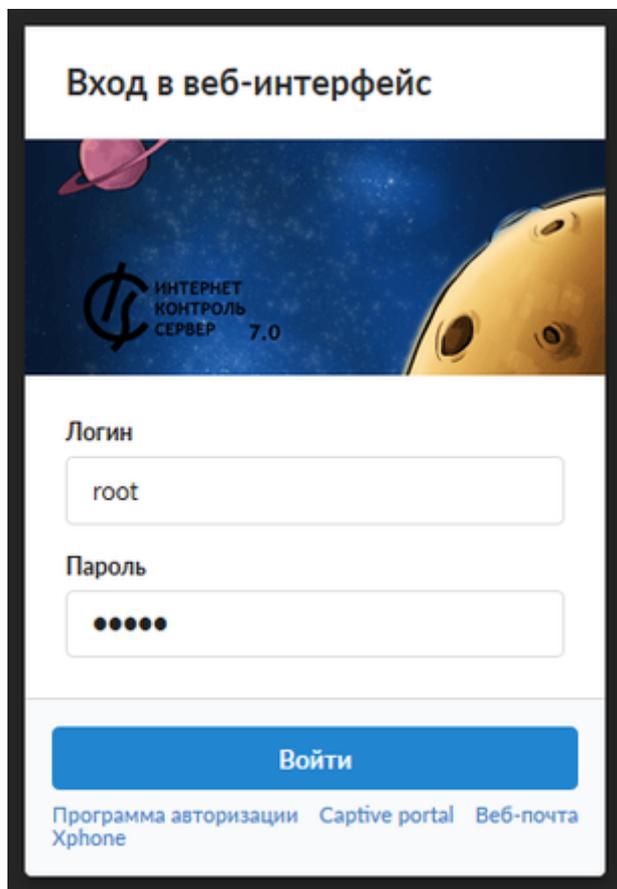
Веб-интерфейс

Вход в веб-интерфейс

После установки, для входа в веб-интерфейс управления необходимо на любом компьютере из локальной сети, в браузере ввести ip-адрес сервера, который был указан при [установке](#) и порт 81 (<ip:81>).

В качестве браузера по умолчанию рекомендуется использовать Mozilla Firefox или Google Chrome.

После этого, начнется процесс загрузки веб-интерфейса и появится окно ввода логина и пароля.



Вход в веб-интерфейс

ИНТЕРНЕТ
КОНТРОЛЬ
СЕРВЕР 7.0

Логин
root

Пароль
•••••

Войти

Программа авторизации Captive portal Веб-почта
Xphone

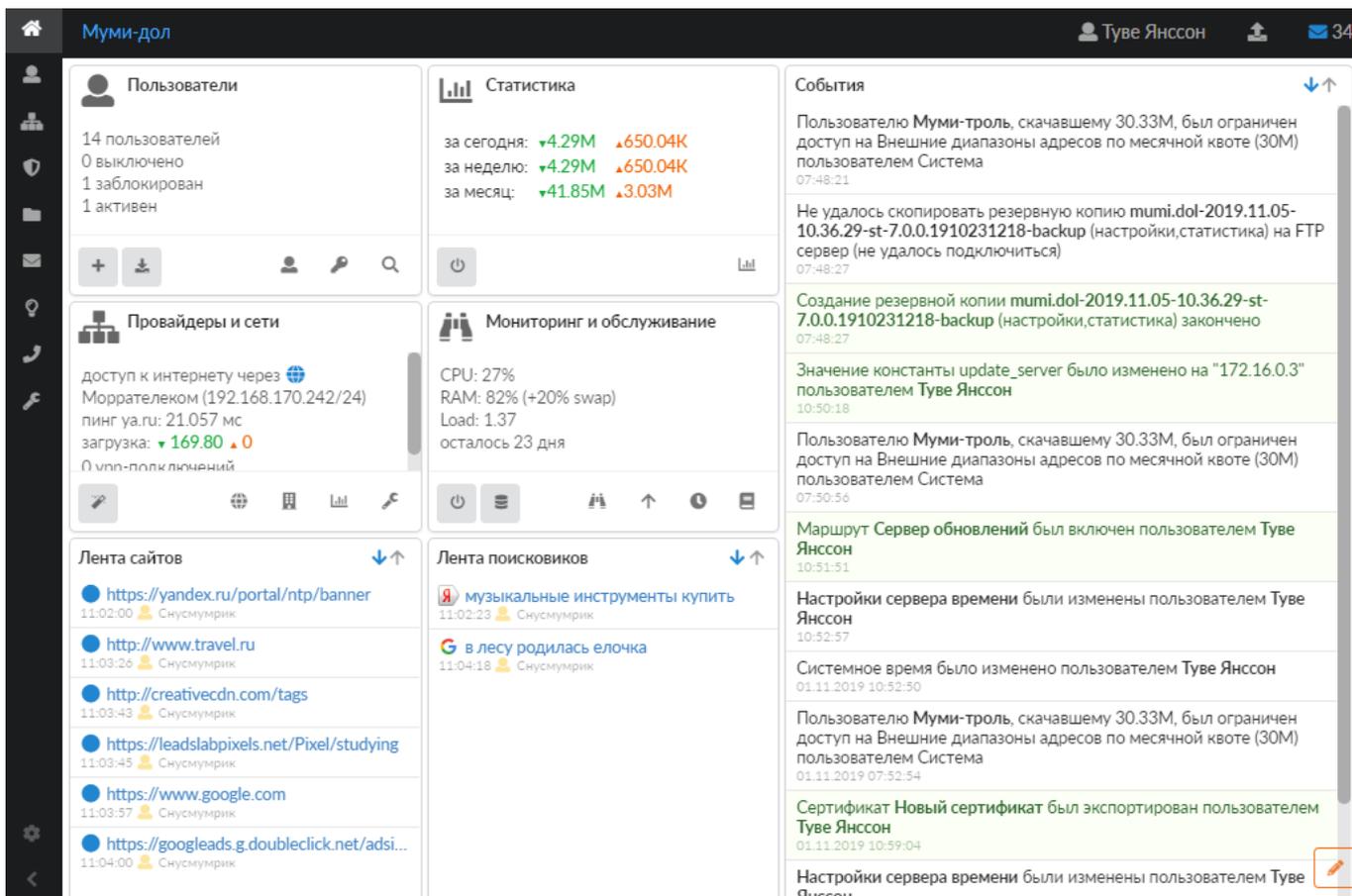
При первом входе в веб-интерфейс, необходимо использовать логин **root** и пароль **00000** (пять нулей).

Внимание! Настоятельно рекомендуется поменять пароль администратора сразу же после первого входа в систему. В противном случае, к интерфейсу управления ИКС смогут получить доступ посторонние лица.

Также, в окне авторизации находится ссылки на [веб-интерфейс почты](#), [страницу авторизации Captive portal](#), [веб-софтфон](#) и [утилиту авторизации](#).

Главная страница

На главной странице веб-интерфейс разделен на две части. В левой находится список модулей системы, разбитый на несколько основных групп – называемый меню, а в правой - окно текущего модуля. На главной странице «ИКС» в окне модуля представлен набор настраиваемых виджетов («Пользователи», «Статистика», «Отчет по категориям», «Безопасность и ограничение доступа», «Провайдеры и сети», «Почта», «Веб и файловый сервер», «Телефония», «Мониторинг и обслуживание», «Лента сайтов», «Лента поисковиков», «События»).



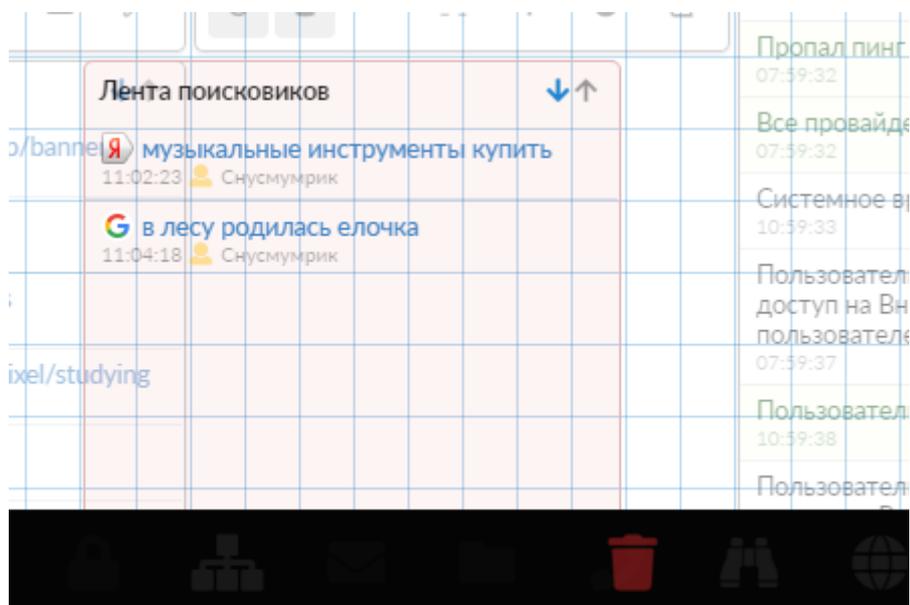
Виджеты

Некоторые из них первоначально скрыты. Все виджеты можно скрывать/добавлять на главную страницу, изменять размер и перемещать по сетке. Для добавления виджетов необходимо нажать на символ карандаша в левом нижнем углу, будет включен режим редактирования главной страницы.



Снизу будет открыта панель с перечислением всех доступных виджетов, а также кнопка восстановления первоначальной настройки виджетов. Отображаемые виджеты на главном экране будут подсвечены на данной панели. При добавлении виджета, он добавится в самый низ экрана. В режиме редактирования главной страницы также появляется сетка, а у каждого

виджета появляются значки удаления и редактирования (шестеренка). Если необходимо убрать виджет с главной страницы, то это можно сделать: нажав на знак корзины, у соответствующего виджета; нажать на соответствующую иконку виджета в панели открытой снизу; «ухватить» и перетащить виджет на нижнюю панель.



При редактировании виджета будет открыто новое диалоговое окно, в котором можно указать ширину и высоту. Задаваемые значения указываются в количестве клеток. Максимальная ширина 36 клеток, что соответствует размеру отображаемой сетки, а максимальная высота одного виджета 3600 клеток. Стоит отметить, что изменить размер виджета возможно только в случае достаточного места. Размер виджета будет рассчитываться от левого верхнего угла, текущего расположения виджета. Если необходимо увеличить виджет, а свободного места не хватает, то стоит перетащить виджет в самый низ и произвести настройку необходимых размеров. В мобильном виде виджеты располагаются по вертикали друг за другом, внесение изменения расположения и размеров не возможно.

Виджет	Информация	Возможные действия	Переход	Зависимые службы
Пользователи	Общее количество, количество активных, заблокированных и отключенных пользователей	Добавить пользователя, импортировать пользователей	Пользователи, Роли, Монитор соединений	-
Статистика	Размер входящего и исходящего трафика за текущие день, неделю и месяц	Включить/отключить службу статистики (Статистика, Счетчики)	Отчеты	Статистика, Счетчики, Прокси-сервер
Отчеты по категориям	Выводит сводную информацию о распознанных категория трафика за текущий день	-	Отчеты (Категории трафика)	-

Безопасность и ограничение доступа	Число обнаруженных атак и вирусов	Включить/выключить систему безопасности (Межсетевой экран, Прокси-сервер, фильтр HTTP-трафика)	Наборы правил, Категории трафика, Межсетевой экран (правила), Прокси (настройки)	Межсетевой экран, Прокси-сервер, фильтр HTTP-трафика, DNS-сервер, Детектор атак Suricata, Антивирусный прокси-сервер, DLP, Контент фильтр
Провайдеры и сети	Провайдер по умолчанию, пинг до шлюза по умолчанию, средняя загрузка интерфейса провайдера, количество VPN - подключений	Запустить мастер настройки сети	Провайдеры и сети, VPN (Пользователи), Управление отчетами (отчет По интерфейсам), Сетевые утилиты	-
Почта	Количество обработанных писем (отправленных, полученных, отправленных в спам, обнаруженных вирусов)	Включить/выключить почтовые службы (Почтовый сервер, Хранилище почты, Сборщик почты, Антиспам SpamAssassin), 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 (Веб-сервер, FTP-сервер, Сетевое окружение), добавить один из ресурсов, добавить раздел и подключить жесткий диск	Хранилище файлов, Веб (Веб-ресурсы), FTP (FTP-ресурсы), Сетевое окружение (идентификация)	Веб-сервер, 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
Мониторинг и обслуживание	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	Выводятся последние зарегистрированные посещения сайтов	-	Отчеты (Активность пользователей)	-

Лента поисковиков	Выводятся последние зарегистрированные запросы в поисковых системах	-	Отчеты (Лента поисковиков)	-
События	Показывает последние события системы из системного журнала	-	Журнал и уведомления (Системный журнал)	-

Все виджеты отображают актуальную информацию и обновляются в реальном времени.

После первого входа в веб-интерфейс необходимо провести [первичную настройку системы](#).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:gui>

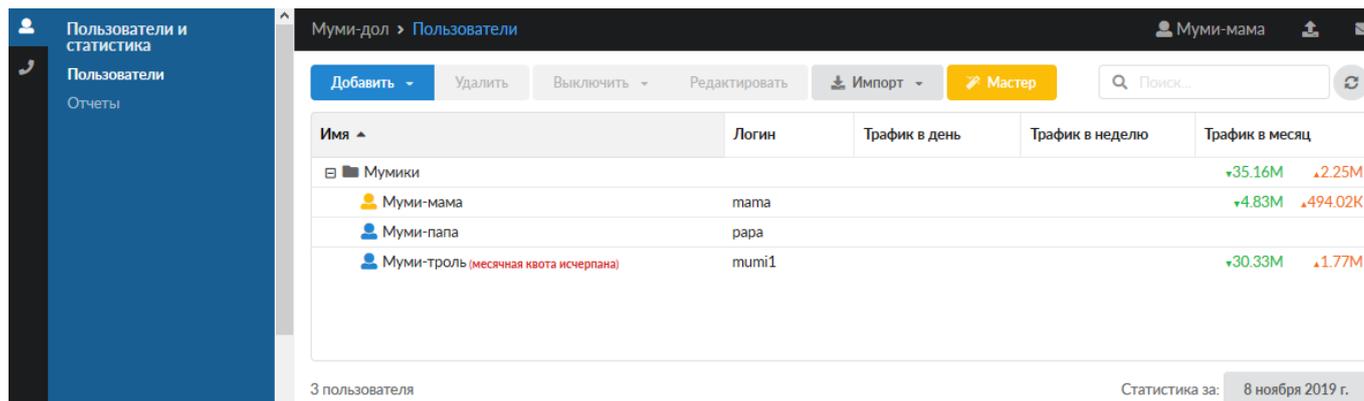
Last update: **2019/11/10 19:25**



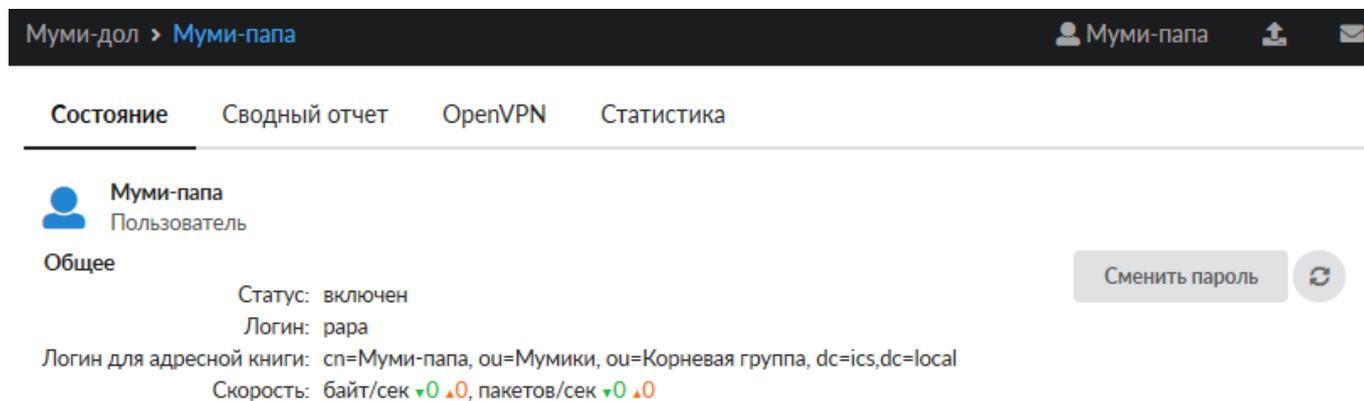
Веб-интерфейс Пользователя

Для каждого Пользователя «ИКС» автоматически создается персональная страница. Вид отображаемой страницы зависит от назначенной роли:

- **Администратор.** Не имеет персональной страницы, так как имеет полный доступ к web-интерфейсу «ИКС».
- **Роль1.** При создании данной роли в правах доступа, в блоке «Администратор группы», установлен флаг «Просмотр дочерних пользователей».



- **Роль2.** При создании данной роли в правах доступа, в блоке «Администратор группы», НЕ установлен флаг «Просмотр дочерних пользователей».



Действия доступные для каждой роли, зависят от выданных привилегий роли.

Флаг «Просмотр звонков дочерних пользователей». Данный флаг может быть установлен у роли - Роль1. При его установке в web-интерфейсе появится пункт меню «Телефония», в нем «Журнал звонков», а отображаться будут лишь те звонки, у которых хотя бы в одном из столбцов «Источник», «Назначение», «Ответил» будут дочерние Пользователи роли Роль1.

Телефония
Журнал звонков

Муми-дол > Журнал звонков

Муми-мама

25.09.2019 - 25.09.2019

Сегодня Неделя Месяц Другой период

Воспроизвести Скачать Экспорт

Детализация звонков

Группировка*
По месяцам

Источник
(любой)

Назначение
(любой)

Отвечил
(любой)

Результат
(любой)

Показать

Начало звонка	Источник	Отвечил	Длительность	Результат
25.09.2019 08:31:21	154	142 Главбух (Телефонные номера)	3 сек	Разговор
25.09.2019 08:31:21	98-961-966-79-90	142 Главбух (Телефонные номера)	9 мин 41 сек	Разговор
25.09.2019 09:01:05		142 Главбух (Телефонные номера)	1 сек	Разговор
25.09.2019 09:01:01	+7-924-188-91-00	142 Главбух (Телефонные номера)	6 мин 13 сек	Разговор
25.09.2019 09:01:02			6 мин 13 сек	Разговор
25.09.2019 09:05:05	+7-924-188-91-00	115 (Телефонные номера)	2 мин 14 сек	Разговор
25.09.2019 09:01:02	+7-924-188-91-00	142 Главбух (Телефонные номера)	6 мин 18 сек	Разговор
25.09.2019 09:08:27	142 Главбух (Телефонные номера)	7-924-188-91-00	1 мин 8 сек	Разговор
25.09.2019 09:23:57		142 Главбух (Телефонные номера)		Разговор

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_gui

Last update: **2019/11/10 19:25**



Пользователи

Модуль «Пользователи» расположен в Меню «Пользователи и статистика». Данный модуль предназначен для присвоения и работы с идентификаторами объектов сетевого взаимодействия. При открытии модуля «Пользователи» в основном окне отобразятся вкладки «Пользователи» и «Роли», при этом вкладка «Пользователи» будет активна.

ООО "Организация" > Пользователи Туде Янссон 11

Пользователи Роли

Добавить Удалить Выключить Редактировать Импорт Мастер Поиск...

Имя	Правила и ограничения	Трафик в день	Трафик в неделю	Трафик в месяц
Корневая группа			↑32.43M	↑2.85M
Долина			↑2.42M	↑329.04K
Вифсла				
Малышка Мю				
Тофсла				
Хемуль			↑2.42M	↑329.04K
Друзья			↑15.63M	↑1.44M
Семья			↑11.36M	↑1.07M
Муми-мама				
Муми-папа				
Муми-троль			↑11.36M	↑1.07M
Муми-туннель			↑3.00M	↑2.13K
Туде Янссон				

13 пользователей Статистика за: 22 ноября 2019 г.

В Окне будет отображено дерево групп и имен Пользователей, а также для каждого из них статистика за день, неделю и месяц. При этом, если нажать на имя группы или Пользователя, то откроется индивидуальный модуль группы или Пользователя. Для управления группами и Пользователями в Окне расположены следующие кнопки:

- «Добавить» позволяет **добавить** Пользователей и группы Пользователей;
- «Удалить», позволяет удалить Пользователей и группы Пользователей, кроме корневой группы;
- «Выключить», позволяет выключить Пользователей и группы Пользователей на 5 минут, на 30 минут, на 1 час, на 1 день или постоянно. При выборе одного из вариантов доступ к сети Интернет пропадет сразу у Пользователя/группы Пользователей;
- «Редактировать», позволяет редактировать Пользователей и группы Пользователей, при нажатии откроется форма редактирования;
- «Импорт», позволяет **импортировать** Пользователей и группы Пользователей из файла, из сети, из LDAP/AD;
- «Экспорт» позволяет экспортировать Пользователей и группы Пользователей из «ИКС» с их настройками, правилами и ограничениями, при этом экспорт производится с выбором сохранения паролей;
- «Мастер» вызывает **мастера** создания Пользователей и групп Пользователей в «ИКС»;

Также, в правом верхнем углу окна, находятся кнопки переключения вида отображения

пользователей: деревом либо списком групп и строка поиска. При выборе отображения пользователей списком окно будет поделено на две части: в левой части будет отображаться дерево групп, а в правой - содержимое выделенной в дереве группы в виде таблицы с основными данными по каждому пользователю/группе.

Пользователи Роли

Добавить Удалить Выключить Редактировать Импорт Мастер Поиск...

Имя	Правила и ограничения	Трафик в день	Трафик в неделю	Трафик в месяц
Долина		▼3.08M ▲115.58K	▼5.51M ▲444.63K	▼5.51M ▲444.63K
Вифсла				
Малышка Мю				
Тофсла				
Жемуль		▼3.08M ▲115.58K	▼5.51M ▲444.63K	▼5.51M ▲444.63K

Стр 1 из 1 Показаны записи 1 - 4 из 4

13 пользователей

Статистика за: 22 ноября 2019 г.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:userlist>

Last update: **2019/11/22 10:01**



Добавление и импорт пользователей

Пользователь - это объект программного комплекса «ИКС», к которому применяются различные политики и правила, а также собираются статистические данные. Пользователей можно объединять в группы для назначения общих правил и ограничений. Для переноса созданного Пользователя в группу необходимо выделить его и перетащить.

Для добавления Пользователей или групп Пользователей в «ИКС» необходимо перейти в модуль «Пользователи» и выбрать один из трех возможных способов добавления:

- При помощи кнопки «[Добавить](#)»
- При помощи кнопки «[Мастер](#)»
- При помощи кнопки «[Импорт](#)»

Добавление пользователя

В основном окне модуля «Пользователи» выбрать «Добавить». Если был выбран пункт «Пользователь», то откроется новая форма, в которой можно будет указать: имя пользователя, задать его описание, указать привилегии (**роль** в «ИКС») пользователя, задать логин и пароль. А также внести дополнительную информацию: должность, телефон, веб-сайт, номер ICQ, адрес и дополнительный комментарий. При добавлении Пользователя минимально можно указывать только его Имя.

Добавление пользователя	
Общее	Информация
Имя * Петрович	Описание Сторож
Роль Пользователь	Должность Складской сторож
Логин petrovich	Телефон 123321
Пароль	Веб-сайт Веб-сайт
	Номер ICQ Номер ICQ
	Адрес Адрес
	Комментарий Алкоголь на складе не оставлять!
Добавить Отмена	Добавить Отмена

Если был выбран пункт «Группа», то откроется новая форма, в которой можно будет указать: имя группы, задать ее описание и комментарий. При добавлении группы минимально можно указывать только Имя создаваемой группы.

Мастер создания пользователя

В основном окне модуля «Пользователи» выбрать «Мастер». Откроется новое окно с предложением выбора что необходимо создать в «ИКС», Пользователя или группу. Если был выбран пункт «Создать пользователя», будет предложено ввести его имя и описание, далее

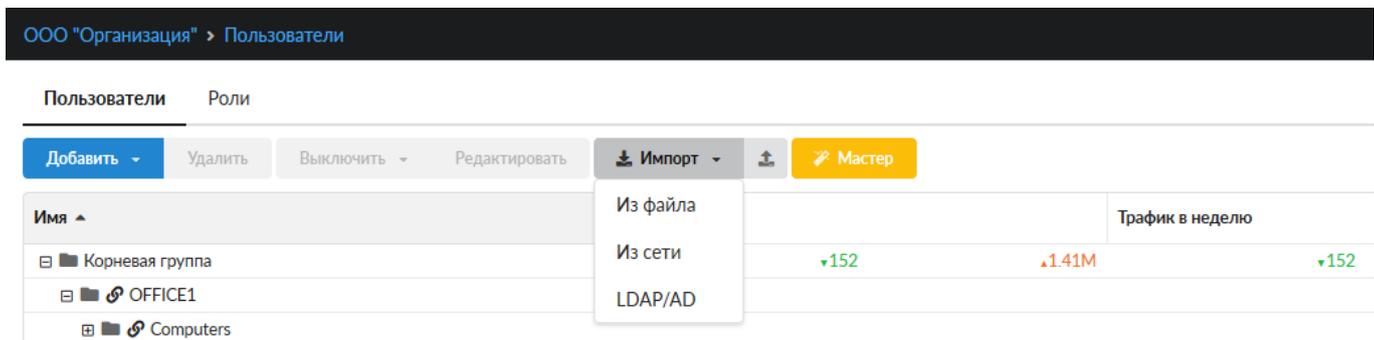
установить привилегию пользователя (**роль** в «ИКС»), далее задать логин и пароль, далее ввести ip-адреса принадлежащие данному пользователю (например, ip-адреса рабочего компьютера, сотового телефона и т.д.), далее назначить набор/наборы правил ограничений созданных в «ИКС» или не назначать ни одного, далее будет предложено создать почтовый ящик, и на последнем шаге будет предложено проверить введенные данные. Если все данные были введены правильно можно нажать «Готово», иначе нажать «Отмена» или «Назад» для возвращения на неправильно введенный пункт.

Если был выбран пункт «Создать группу», будет предложено ввести имя группы и ее описание, далее ip-адреса устройств относящихся к данной группе, далее назначить набор/наборы правил ограничений созданных в «ИКС» или не назначать ни одного, и на последнем шаге будет предложено проверить введенные данные. Если все данные были введены правильно можно нажать «Готово», иначе нажать «Отмена» или «Назад» для возвращения на неправильно введенный пункт.

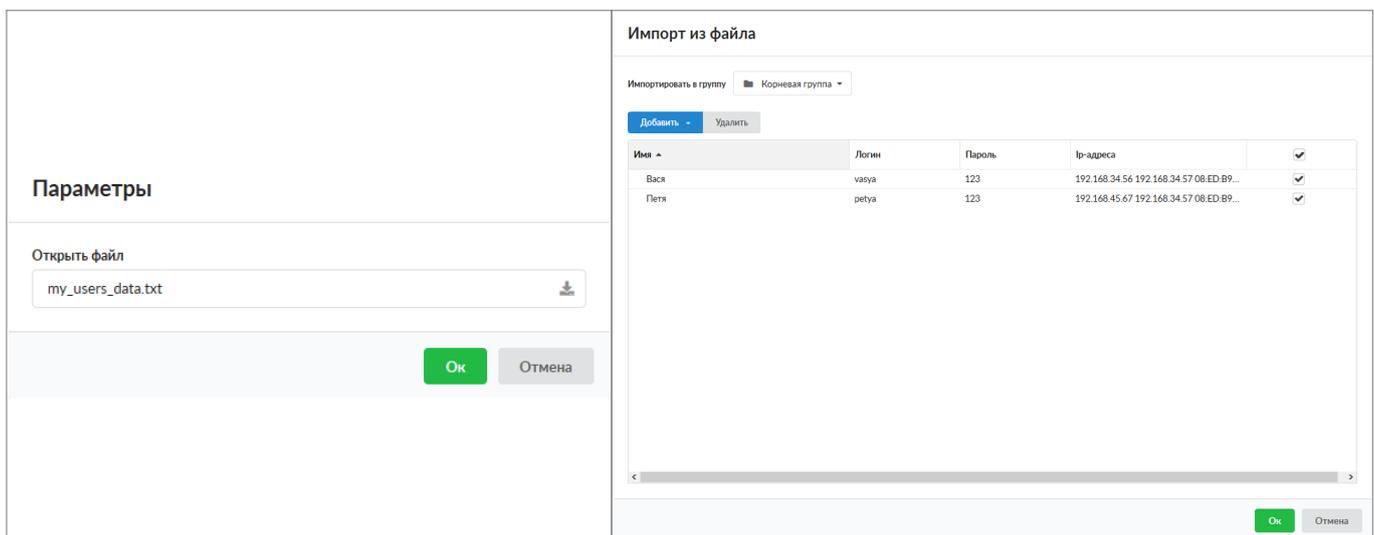
Из всех перечисленных параметров обязательным является только имя Пользователя или группы. Стоит отметить, что в случае, если назначаемый почтовый ящик не может быть присвоен ни одному из созданных в системе почтовых доменов, «ИКС» предложит создать новый почтовый домен.

Импорт пользователей

В основном окне модуля «Пользователи» выбрать «Импорт». Откроется выпадающий список, предлагающий выбрать, каким образом пользователи будут импортированы. Существует три варианта: из файла, из сети, из LDAP/AD.



Из файла. Для импорта из файла источником служит файл формата *.txt, в котором перечислены строки, содержащие параметры (имя, логин, пароль, ip-адреса и mac-адреса разделенные запятыми), все параметры должны быть отделены запятой друг от друга и представлены в указанном порядке, а каждый новый пользователь в отдельной строке. Или файл должен иметь формат как файл создаваемый «ИКС» при экспорте Пользователей. Например – «Вася, vasya, 123, 192.168.34.56, 192.168.34.57, 08:ED:B9:49:B2:E5, 16-ED-C9-4D-52-E5». При этом, если какой-либо параметр в файле будет указан не верно, то в открывшейся форме можно будет внести изменения, а также добавить Пользователей и только после этого сохранить.



Из сети. Будет предложено указать в ручную ip-адреса сети или сканировать локальные сети подключенные к «ИКС». При сканировании локальной сети «ИКС» отобразит все активные ip-адреса в настоящий момент, присвоив им имена и логины в виде rsX-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.

Параметры

Сканировать локальные сети
 Указать ручную

Адрес сети *

Импорт из сети

Импортировать в группу Корневая группа ▾

Добавить - Удалить

Имя	Логин	Пароль	Ир-адреса	
rs0-2	rs0-2		10.10.0.2	✓
rs0-3	rs0-3		10.10.0.3	✓
rs0-4	rs0-4		10.10.0.4	✓

Ок Отмена

Из LDAP/AD. Будет открыто новое окно в котором необходимо обязательно указать: ip-адрес контроллера домена, имя домена, логин и пароль администратора домена. А также можно указать: LDAP-группу, установить флажок «Пропускать пустые группы» и флажок «Secure LDAP», последняя предназначена для обмена данными с контроллером домена по протоколу SSL (если такой протокол поддерживается контроллером).

Параметры

Контроллер домена *

Домен *

LDAP-группа

Secure LDAP

Сертификат *

Логин *

Пароль *

Пропускать пустые группы

Ок
Отмена

После ввода данных будет выведен список Пользователей домена, сгруппированных по Organization Unit, а также выбор требуемых действий относительно Пользователя. Будет предложено три возможных действия: «Импортировать», «Синхронизировать» и «Почта». При

установке флажка в графе «Импортировать» будет импортировано имя и логин соответствующего Пользователя. Для синхронизации Пользователя или группы необходимо установить флажки «Импортировать» и «Синхронизировать». При этом Пользователь или группа будут импортированы таким образом, что любое изменение данного объекта в дереве контроллера домена аналогичным образом отразится на объекте в «ИКС». Для импорта почтового ящика из домена необходимо установить все три флажка. При этом для выбранного Пользователя будет создан почтовый ящик с аналогичным именем в том случае, если в «ИКС» был почтовый домен аналогичный домену из Active Directory, иначе почтовый ящик импортирован не будет.

Импорт LDAP/AD

Импортировать в группу

Корневая группа ▾

Поиск...

Имя ▲	Логин	Импортировать	Синхронизировать	Почта
☐ OFFICE1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Computers		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Domain Controllers		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ ForeignSecurityPrincipals		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Managed Service Accounts		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Program Data		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ System		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Users		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ test		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ для автотестов		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ офис		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Ок

Отмена

Пользователи, импортированные и синхронизированные, будут отмечены в списке пользователей специальной иконкой.

После того как Пользователь или группы были добавлены одним из выше перечисленных способов, рекомендуется произвести настройку их [авторизации](#).

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:users>

Last update: **2019/11/10 19:25**



Авторизация пользователей

Авторизация по IP

Самым распространённым способом авторизации является 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.

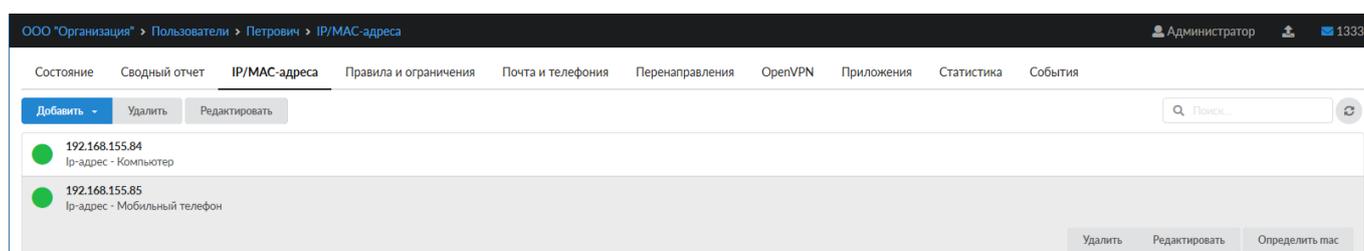
Затем нужно открыть вкладку ip-адреса, нажать кнопку «добавить» и задать адрес, выделенный для этого пользователя.

Добавление ip-адреса

Ip-адрес *

Комментарий

После чего назначенный адрес появится в списке адресов пользователя. Одному пользователю можно назначить любое количество ip-адресов. Также, если записать адрес в формате адрес/префикс возможно назначить пользователю диапазон адресов.



Внимание! Ip-адрес довольно легко подделать. Злонамеренный пользователь может выдать себя за другого, просто поменяв сетевые настройки на своём компьютере. Для того, чтобы это предотвратить, воспользуйтесь функцией [привязки к MAC-адресу](#)

Авторизация по MAC

Данный вид авторизации удобен, когда в сети используются динамические адреса, но в качестве DHCP-сервера выступает не ИКС. Для того, чтобы добавить пользователю mac-адрес, перейдите во вкладку IP-адреса и нажмите Добавить - MAC-адрес.

Добавление mac-адреса

Мас-адрес *

Комментарий

ООО "Организация" > Пользователи > Петрович > IP/MAC-адреса Администратор 1337

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления OpenVPN Приложения Статистика События

192.168.155.84	IP-адрес - Компьютер
192.168.155.85	IP-адрес - Мобильный телефон
02:af:40:f3:23:a0	Мас-адрес - Ноутбук

Авторизация по логину/паролю

После создания пользователя, если ему был задан логин и пароль, мы можем получить доступ к Интернету, прописав в настройках его веб-браузера прокси-сервер: 192.168.17.123 и порт 3128 (по умолчанию).

При попытке выхода в Интернет, ИКС спросит у пользователя его логин и пароль. Такая схема работы называется «авторизацией по логину/паролю».

Сама авторизация может осуществляться двумя методами:

- по логину и паролю пользователя - пользователь, сделавший HTTP-запрос, получает первоначально приглашение на ввод своего логина и пароля доступа, а после успешной идентификации – результат запроса;
- через домен - пользователь, зарегистрированный на сервере Active Directory, автоматически авторизуется на прокси-сервере.

Второй метод возможен лишь в том случае, когда система [присоединена к домену](#) Active Directory и пользователи [импортированы из домена](#).

Внимание! При этой схеме авторизации у пользователя не будет работать ICQ, почта, клиент-банк и другие программы которые работают не по протоколу HTTP.

Одновременная работа с двумя типами авторизации

Вы можете выпускать часть пользователей в интернет с использованием авторизации по логину/паролю, а часть - с использованием авторизации по Ip.

При использовании порядка авторизации «сначала Ip потом логин/пароль»:

1. Сначала проверяется Ip-адрес пользователя. Пользователи с известными Ip-адресами пропускаются.
2. Затем, если в браузере у пользователя в настройках прокси прописан адрес ИКС, то ему выдастся приглашение для ввода логина и пароля. Пользователи, которые ввели правильный логин и пароль пропускаются.
3. Остальные пользователи блокируются.

Более подробно порядок авторизации объясняется на странице описания [настроек прокси сервера](#).

Другие типы авторизации

Для того, чтобы пользователь с динамическим ip-адресом мог авторизоваться по логину/паролю и выходить во внешнюю сеть без ограничений, необходимо использование [утилиты авторизации xauth](#) либо [веб-авторизации](#).

Для ускорения процесса создания пользователей используется функция [импорта](#)

После создания пользователей вы можете задать им правила доступа.

Авторизация пользователей терминального сервера

Для ИКС все пользователи, работающие через терминальный сервер неотличимы друг от друга по своим запросам в сети (в качестве источника выступает один и тот же ip-адрес терминального сервера). Таким образом, для того чтобы разделить статистику и настройки доступа, вам необходимо указать прокси-сервер в настройках браузера каждого из терминальных пользователей. Тогда каждый пользователь будет зарегистрирован под своим логином, и запросы, проходящие через прокси будут идентифицироваться отдельно для каждого из пользователей терминала.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:auth_user

Last update: **2019/11/10 19:25**



Индивидуальный модуль пользователя

Индивидуальный модуль или индивидуальная страница Пользователя/группы предназначена для просмотра и редактирования всевозможных настроек для определенного Пользователя/группы. Для того чтобы открыть индивидуальный модуль необходимо в Меню «Пользователи и статистика» - «Пользователи» выбрать интересующего Пользователя/группу и нажать по его имени. Откроется новое окно, в котором будут следующие вкладки: «Состояние», «Сводный отчет», «IP/MAC-адреса», «Правила и ограничения», «Почта и телефония», «Перенаправления», «Статистика», «События».

Состояние

На данной вкладке возможно: выключить Пользователя (на 5 минут, 30 минут, 1 час, 1 день или задать дату и время до которого будет выключен пользователь) или редактировать (форма редактирования аналогична форме добавления пользователя см.п. 1.1.1). Стоит отметить, что редактирование, выключение или удаление синхронизированных Пользователей из LDAP/AD не возможно. Также на данной вкладке отображается: статус (включен/выключен); логин в «ИКС»; логин для адресной книги; присвоенные IP-адреса Пользователю; статистика за день, неделю, месяц; скорость текущего соединения Пользователя в байт/сек и пакет/сек.

ООО "Организация" > Пользователи > Хемуль Туге Янссон 123

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления >

Хемуль
Пользователь

Общее

Статус: включен

Логин для адресной книги: sp=Хемуль, ou=Долина, ou=Корневая группа, dc=ics,dc=local

Скорость: байт/сек +15.90 +22.92, пакетов/сек +0.03 +0.1

Ip-адреса: 192.168.17.43

Статистика

За день: +2.42M +329.04K

За неделю: +2.42M +329.04K

За месяц: +2.42M +329.04K

Редактировать Выключить ▾

Сводный отчет

Данная вкладка отображает пред настроенный сводный отчет по Пользователю. Который включает в себя: общие данные Пользователя (Статус, Логин, Логин для адресной книги, ip-адреса, Скорость, Статистику за день, неделю, месяц); статистику по часам входящего/исходящего трафика за текущие сутки; топ 5 ip-адресов или доменов; а также топ 5 категорий, к которым относится наработанный трафик. Вкладка «IP/MAC-адреса». На данной вкладке располагаются кнопки: «Добавить», «Удалить» и «Редактировать». При нажатии на «Добавить» возможно задавать ip-адреса конкретному Пользователю, при этом если Пользователь активен в сети, то «ИКС» определить его mac-адрес. При выделении поля с ip-адресом можно связать заданный ip-адрес с mac-адресом устройства или удалить данную информацию. При задании mac-адреса, если Пользователь активен, «ИКС» автоматически

выделить ему ip-адрес. При редактировании или добавлении возможно задать комментарий к ip-адресу или mac-адресу.

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления OpenVPN Приложения >

Хемуль
Пользователь

Статус: включен

Логин для адресной книги: sp=Хемуль, ou=Долина, ou=Корневая группа, dc=ics,dc=local

Скорость: байт/сек ↑36.60 ↓14.16, пакетов/сек ↑0.07 ↓0.07

Статистика: за день ↑2.42M ↓329.04K, за неделю ↑2.42M ↓329.04K, за месяц ↑2.42M ↓329.04K

21.11.2019 - 21.11.2019 **Сегодня** Неделя Месяц Другой период ↻

По часам

Топ 5 ip-адресов и доменов

google.ru	117	↑923.88K	↓129.40K
tripsecrets.ru	69	↑898.37K	↓26.77K
adme.ru	3	↑262.34K	↓1.02K
gstatic.com	33	↑240.75K	↓19.27K

По категориям

- 25%** Поисковые системы (↑944.83K ↓239.42K) Категория трафика
- 25%** Поисковые системы (↑928.67K ↓129.43K) SkyDNS категория трафика
- 24%** Туризм (↑898.37K ↓25.27K) Сайты, посвященные туризму и путешествиям
- 7%** Компьютеры и Интернет (↑290.34K ↓18.00K) Сайты, основной тематикой которых являются информационные технологии, программное обеспечение, интернет, компьютеры
- 17%** Остальные (↑440.37K ↓270.17K)

IP/MAC-адреса

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перен. >

Добавить ▾ Удалить Редактировать

Поиск...

- 192.168.17.43
Динамический ip-адрес Хемуль
- 74:d4:35:3b:0e:2f
Mac-адрес

Правила и ограничения

Позволяет задавать правила, ограничения, квоты и маршруты аналогично модулю «Наборы правил». По умолчанию установлены правила для роли к которой относится данный Пользователь. Правило по умолчанию удалить не возможно.

Состояние Сводный отчет IP/MAC-адреса **Правила и ограничения** Почта и телефония Перенаправления OpenVPN >

Добавить Удалить Выключить Редактировать Подробнее Поиск правил по URL...

Правила

- Разрешить доступ на адрес Дом, семья, хобби, Интернет-библиотеки, Искусство
Разрешающее правило прокси
- Ограничить скорость входящего трафика на адрес Внешние диапазоны адресов до 8 Кбайт/с при превышении входящего в день 50 Мб в неделю 128 Мб в месяц 512 Мб
Квота

Наборы правил

Набор правил для роли Житель
Набор правил

- Сканировать трафик с помощью контент-фильтра, вывести сообщение "Нежелательный контент!"
Правило контентной фильтрации
- Запретить доступ для приложений TELEGRAM, SKYPE
Запрещающее правило Application Firewall
- Ограничить скорость входящего трафика для каждого пользователя до 256 Кбайт/с (выключен)
Ограничение скорости

Удалить Редактировать Выключить

Почта и телефония

Данная вкладка предназначена для создания телефонного номера или почтового ящика Пользователя.

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения **Почта и телефония** Перенаправлен >

Добавить Удалить Выключить Редактировать Отправить факс Поиск...

Почтовые ящики и ссылки

- collectmaster@mumi.dol
Почтовый ящик

Телефонные номера

- 123

Перенаправления

Данная вкладка позволяет задать действие при не ответе на телефонный вызов Пользователя.

[Добавить](#) [Удалить](#) [Выключить](#) [Редактировать](#)

- При неответе номера 111 позвонить на 322, 223 и ждать ответа 15 сек.
Перенаправление при неответе (При неответе Муми-троля переадресовать вызов Сноркам)
- При неответе номера Тусня позвонить на 101
Перенаправление при неответе

Если у пользователя создан телефонный номер и в ИКС созданы [Перенаправления](#), в которых этот номер указан в поле «При неответе номера», то во вкладке будут отображены все такие перенаправления. При этом, те перенаправления, в которых этот номер указан как единственный, будут доступны к редактированию.

OpenVPN

Вкладка «OpenVPN». Отображает доступно ли Пользователю использование OpenVPN соединение. В случае, если не доступно, то во вкладке будет отображено информационное сообщение «Включите OpenVPN-доступ для пользователя в модуле VPN». В случае, если для Пользователя было добавлено разрешение на использование OpenVPN в Меню – Сеть – VPN – вкладка «Пользователи», то станут доступны следующие параметры настройки: флаг «Передать клиенту маршрут по умолчанию» (устанавливает на подключаемом устройстве, в качестве шлюза по умолчанию, «ИКС»); поле «Передать клиенту маршруты до сетей» (позволяет передать Пользователю информацию об указанных LAN); поле «Удаленные сети» (позволяет задать пары IP-адрес/маска, расположенные за устройством Пользователя); поле «Сертификат клиента» (позволяет выбрать конечный сертификат для Пользователя); кнопки «Сохранить», «Обновить» и «Выгрузить сертификаты».

OpenVPN-доступ для пользователя включен в Муми-OpenVPN (10.8.0.0/24)

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей Удаленные сети

Сертификат клиента *

Муми-OpenVPN_Хемуль

[Сохранить](#) [Обновить](#) [Выгрузить сертификаты](#)

Приложения

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления >

Запретить доступ

Приложения и процессы ▲	Соединения	Протокол
☰ ⚙ SkypeApp.exe		
☰ ⚙ System		
☰ ⚙ TeamViewer_Service.exe		
☰ ⚙ Telegram.exe		
	12092 192.168.17.43:49920 → 45.90.173.116:5454	TCP
	12092 192.168.17.43:49921 → 45.90.173.116:5454	TCP
	12092 192.168.17.43:50472 → 45.90.173.116:5454	TCP
☰ ⚙ Не определен		
☰ ⚙ Video.UI.exe		
☰ ⚙ WinSCP.exe		
☰ ⚙ [System Process]		
☰ ⚙ chrome.exe		

Статистика

Данная вкладка представляет конструктор отчета по Пользователю. Настройка аналогична Меню - «Пользователи и статистика» - «Управление отчетами» - «Конструктор отчетов».

< Почта и телефония Перенаправления OpenVPN Приложения **Статистика** События

Добавить Удалить Редактировать 21.11.2019 - 21.11.2019 **Сегодня** Неделя Месяц Другой период ↕

По часам	↓↑
🕒 Топ 5 назначений	🔵 https://googleads.g.doubleclick.net/pagead/conversion 14:09:26 🧑 Хемуль
📊 Топ 5 ip-адресов и доменов	🔵 https://www.google.ru 14:09:35 🧑 Хемуль
📊 Активность пользователей	🔵 https://tripsecrets.ru 14:12:12 🧑 Хемуль

« < Стр 1 из 1 > » Показаны записи 1 - 3 из 3

События

Данная вкладка представляет список событий пользователя.

Почта и телефония Перенаправления OpenVPN Приложения Статистика **События**

21.11.2019 - 21.11.2019

Сегодня

Неделя

Месяц

Другой период ▾



↑ Экспорт

Поиск... 🔍



Mac-адрес 74:d4:35:3b:0e:2f был добавлен пользователю Хемуль пользователем Туве Янссон
14:09:16

Пользователь Хемуль был подключен с адреса 192.168.17.43 через mac-авторизацию
11:09:19

Разрешающее правило прокси на адрес Дом, семья, хобби, Интернет-библиотеки, ... было добавлено пользователю Хемуль пользователем Туве Янссон
15:59:46

Разрешающее правило прокси на адрес Дом, семья, хобби, Интернет-библиотеки, ... пользователя Хемуль было изменено пользователем Туве Янссон
16:00:34

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_mod

Last update: **2019/11/22 09:23**



Запрещающее правило

При добавлении откроется окно настроек запрещающего правила. В данном окне расположены следующие поля:

- адрес назначения,
- протокол,
- порт,
- источник,
- время действия,
- пункт для установки флага «Отправить ICMP Unreachable»;

Добавление запрещающего правила

Адрес назначения

Протокол **Порт**

Источник

Отправить ICMP Unreachable

Время действия

По умолчанию все поля пустые и предполагают любое значение, т.е. если сохранить запрещающее правило по умолчанию и применить его к Пользователю или группе, то межсетевой экран полностью заблокирует все коммуникации Пользователя или группы через «ИКС». Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты.

Установка флага «Отправить ICMP Unreachable» приведет к отправке данного сообщения при попытке одной из сторон произвести ping другой, при этом пакет ICMP будет заблокирован.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:user_deny_rule

Last update: **2019/11/10 19:25**



Запрещающее правило Application Firewall

При добавлении откроется окно настроек запрещающего правила. В данном окне расположены следующие поля:

- протокол (обязательное поле),
- время действия,

Добавление правила Application firewall

Протокол *

WORLDOWARCRAFT ✕

Время действия

(всегда)

Добавить Отмена

Поле «протокол» содержит выпадающий список известных протоколов библиотеки nDPI (<https://github.com/ntop/nDPI>).

Важно: данная библиотека поставляется «как есть», таким образом определение сигнатуры протокола соединения полностью зависит от работы данной библиотеки. Если протокол не может быть определен, то соединение не будет заблокировано.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:appfirewall_rule

Last update: 2019/11/10 19:25



Разрешающее правило

При добавлении откроется окно настроек разрешающего правила. В данном окне расположены следующие поля:

- адрес назначения,
- протокол,
- порт,
- источник,
- время действия,
- пункт для установки флага «Разрешить трафик даже если пользователь отключен»;

Добавление разрешающего правила

Адрес назначения

Протокол **Порт**

Источник

Разрешать трафик даже если пользователь отключен

Время действия

По умолчанию все поля пустые и предполагают любое значение, т.е. если сохранить разрешающее правило по умолчанию и применить его к Пользователю или группе, то межсетевой экран разрешит все коммуникации Пользователя или группы через «ИКС». Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты.

Установка флага «Разрешить трафик даже если пользователь отключен» означает, что если Пользователь был отключен или превысил [квоту](#) в «ИКС», то он будет иметь доступ к ресурсам указанным в данном правиле.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_allow_rule

Last update: **2019/11/10 19:25**



Запрещающее правило прокси

При добавлении откроется окно настроек запрещающего правила прокси. В данном окне расположены следующие поля:

- URL назначения,
- Протокол,
- Метод,
- Ip-адрес пользователя,
- Действие,
- Время действия.

Добавление запрещающего правила прокси

URL назначения

Протокол

Метод

Ip-адрес пользователя

Действие:

Запретить доступ Перенаправить на адрес Вывести сообщение

Доступ запрещен!

Время действия

По умолчанию все поля пустые, кроме поля «Действие» (Запретить доступ), и предполагают любое значение, т.е. если сохранить запрещающее правило прокси по умолчанию и применить его к Пользователю или группе, то прокси сервер запретит все коммуникации идущие через него (по протоколам http, https, ftp и http/https). Стоит отметить, что если не был создан сертификат, то запрещающее правило прокси не будет действовать на https-траффик. Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, введенные на «ИКС» значения и объекты.

Поле «Метод» указывает на основную операцию над ресурсом. Более подробно с различными методами обращения к веб-ресурсам можно ознакомиться на <https://ru.wikipedia.org/wiki/HTTP>.

Поле «Действие» предоставляет возможность выбора ответа Пользователю в браузере: а) «Запретить доступ» - Пользователю будет отображен логотип «ИКС» и сообщение «Доступ запрещен»; б) «Перенаправить на адрес», соединение будет перенаправлено на заданный адрес; в) «Вывести сообщение» - Пользователю будет отображен логотип «ИКС» и сообщение «Доступ запрещен» с заданной надписью.

ВАЖНО! Для корректной работы а) и в) необходимо чтобы метод CONNECT был разрешен, т.е. при создании запрещающего правила, если в поле «Метод» указано «(любой)», то необходимо создать разрешающее правило прокси, в котором указать в поле «Метод» - CONNECT. А также прокси сервер должен работать в режиме «Расшифровка трафика с подменой сертификата».

Комментарий. При создании правил прокси сервера возможно использовать конструкцию типа - <.domain>, данная конструкция означает только под домены. Например, .google.com, в запрещающем правиле прокси, разрешит доступ к google.com, но запретит доступ к mail.google.com, drive.google.com итд.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_deny_proxy

Last update: **2019/11/25 18:05**



Разрешающее правило прокси

При добавлении откроется окно настроек разрешающего правила прокси. В данном окне расположены следующие поля:

- URL назначения,
- Протокол,
- Метод,
- Ip-адрес пользователя,
- Время действия,
- пункт для установки флага «Разрешить трафик даже если пользователь отключен»;

Добавление разрешающего правила прокси

URL назначения

Протокол

Метод

Ip-адрес пользователя

Разрешать трафик даже если пользователь отключен

Время действия

По умолчанию все поля пустые и предполагают любое значение, т.е. если сохранить разрешающее правило прокси по умолчанию и применить его к Пользователю или группе, то прокси сервер разрешит все коммуникации идущие через него (по протоколам http, https, ftp и http/https). Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты.

Установка флага «Разрешить трафик даже если пользователь отключен» означает, что если Пользователь был отключен или превысил [квоту](#) в «ИКС», то он будет иметь доступ к ресурсам указанным в данном правиле.

Комментарий. При создании правил прокси сервера возможно использовать конструкцию типа - <.domain>, данная конструкция означает только под домены. Например, .google.com, в запрещающем правиле прокси, разрешит доступ к google.com, но запретит доступ к mail.google.com, drive.google.com итд.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_allow_proxy

Last update: **2019/11/10 19:25**



Исключение прокси

Данное правило является разрешающим правилом прокси, но больше не будет обрабатываться никакими другими правилами. То есть, например, при создании исключения для какого-либо домена, этот домен не будет проверяться контент-фильтром.

Добавление исключения прокси

URL назначения

mail.ru ✕

Протокол

(любой)

Метод

(любой)

Ip-адрес пользователя

(любой)

Разрешать трафик даже если пользователь отключен

Время действия

(всегда)

Добавить

Отмена

Комментарий. При создании правил прокси сервера возможно использовать конструкцию типа - <.domain>, данная конструкция означает только под домены. Например, .google.com, в запрещающем правиле прокси, разрешит доступ к google.com, но запретит доступ к mail.google.com, drive.google.com итд.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_exeption_proxy

Last update: **2019/11/10 19:25**



Ограничение количества соединений

При добавлении откроется окно настроек ограничения количества соединений. В данном окне расположены следующие поля:

- Адрес назначения,
- Протокол,
- Порт,
- Источник,
- Количество соединений,
- Время действия,
- пункт для установки флага «ограничивать до ИКС»,
- выбор для кого применять;

Добавление ограничения количества соединений

Адрес назначения

(любой) ▾

Протокол **Порт**

(любой) ▾

● dns (53) × ▾

Источник

(любой)

Количество соединений* **Применять**

1000 ▴ ▾

для каждого ip ▾

Ограничивать до ИКС

Время действия

(всегда) ▾

Добавить
Отмена

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты. Применение данного правила может трактоваться тремя способами (в зависимости от выбора к кому оно применимо):

Способ	Действие
Для объекта	Применяется к группе или Пользователю. При таком способе ограничения, каждая группа (даже если содержит другие подгруппы) получает ограничение количества соединений указанное в правиле.

Для каждого пользователя	Применяется к группе или Пользователю. При таком способе ограничения, каждый Пользователь, в том числе и в группах, получает ограничение количества соединений указанное в правиле.
Для каждого ip	Применяется к группе или Пользователю. При таком способе ограничения, каждый ip-адрес, записанный за Пользователем (или за Пользователями в группе), получает ограничение количества соединений, равное указанному в правиле.

При установке флага «Ограничивать до ИКС», правилом также будут учитываться соединения входящие на «ИКС» (например, при доступе к ftp-ресурс или графическому интерфейсу).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_states

Last update: **2019/11/10 19:25**



Ограничение скорости

При добавлении откроется окно настроек ограничения скорости. В данном окне расположены следующие поля:

- Направление,
- Адрес назначения,
- Протокол,
- Порт,
- Скорость,
- Включать после (только для HTTP/HTTPS),
- Время действия,
- пункт для установки флага «ограничивать до ИКС»
- выбор для кого применять;

Добавление правила ограничения скорости

Направление	Применять *
<input type="text" value="Входящий"/>	<input type="text" value="для объекта"/>
Адрес назначения	
<input type="text" value="(любой)"/>	
Протокол	Порт
<input type="text" value="(любой)"/>	<input type="text" value="(любой)"/>
Скорость *	Включать после (только для HTTP/HTTPS)
<input type="text" value="256"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Кбайт/с	<input type="text" value="1024"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Кб
<input checked="" type="checkbox"/> Ограничивать до ИКС	
Время действия	
<input type="text" value="(всегда)"/>	

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты. Применение данного правила может трактоваться тремя способами (в зависимости от выбора к кому оно применимо):

Способ	Действие
--------	----------

Для объекта	Применяется к группе или Пользователю. При таком способе ограничения, каждая группа (даже если содержит другие подгруппы) получает ограничение скорости указанное в правиле.
Для каждого пользователя	Применяется к группе или Пользователю. При таком способе ограничения, каждый Пользователь, в том числе и в группах, получает ограничение скорости указанное в правиле.
Для каждого ip	Применяется к группе или Пользователю. При таком способе ограничения, каждый ip-адрес, записанный за Пользователем (или за Пользователями в группе), получает ограничение скорости, равное указанному в правиле.

При установке флага «Ограничивать до ИКС», правилом также будут учитываться соединения входящие на «ИКС» (например, при доступе к ftp-ресурс или графическому интерфейсу).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_pipe

Last update: **2019/11/10 19:25**



Выделение полосы пропускания

При добавлении откроется окно настроек правила выделения полосы пропускания. В данном окне расположены следующие поля:

- Адрес назначения,
- Протокол,
- Порт,
- Скорость,
- Приоритет,
- Время действия,
- пункт для установки флага «Заимствовать пропускную способность у родителя»;

Добавление правила выделения полосы пропускания

Адрес назначения

Протокол

Порт

Скорость



Кбит/сек.

Заимствовать пропускную способность у родителя

Приоритет

Время действия

Добавить

Отмена

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты. Выделение полосы пропускания используется для обеспечения QoS (от англ. quality of service) в отношении резервирования канала связи, например, для качественной работы IP-телефонии, необходимо задать требуемую скорость полосы пропускания и указать используемые порты IP-телефонии, назначив данное правило на соответствующих Пользователей «ИКС».

При установке флага «Заимствовать пропускную способность у родителя», трафик, указанный в правиле, может использовать большую полосу пропускания, чем указано в правиле, при условии, что интернет-канал свободен.

Поле «Приоритет» позволяет при перегрузке канала пропускать трафик с более высоким приоритетом с наименьшей задержкой.

Важно: Данное правило работает не на всех сетевых картах, на ИКС версии 6 поддерживаются драйвера следующих карт:

ae, age, alc, ale, an, ath, aue, axe, bce, bfe, bge, bxe, cas, cxgbe, dc, de, ed, em, ep, epair, et, fxp, gem, hme, igb, ipw, iwi, ixgbe, jme, le, msk, mxge, my, nfe, nge, npe, qlxgb, ral, re, rl, rum, sf, sge, sis, sk, ste, stge, ti, txp, udav, ural, vge, vr, vte, wi, xl.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:user_width

Last update: **2019/11/10 19:25**



Маршрут

При добавлении откроется окно настроек маршрутизации трафика. В данном окне расположены следующие поля:

- Направление,
- Адрес назначения,
- Протокол,
- Порт,
- Время действия,
- выбор «кому» отправлять трафик;

Добавление маршрута

Направление

Входящий на ИКС

Адрес назначения

172.16.5.0/24 ✕

Протокол

(любой)

Порт

(любой)

Через шлюз

Через интерфейс

Через провайдера

192.168.1.1

Не обрабатывать трафик
межсетевым экраном

Время действия

(всегда)

Добавить

Отмена

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты. Правило «Маршрут» используется для маршрутизации трафика как между сегментами сети, так и для перенаправления трафика на различных провайдерах. При установке правила «Через шлюз» необходимо указать IP-адрес устройства, выполняющего функцию шлюза. Чаще всего данное правило используется если «ИКС» установлен на сервере имеющем один сетевой интерфейс.

При установке флага «Не обрабатывать трафик межсетевым экраном», для данного правила, ко всему проходящему трафику через «ИКС» не будут применяться правила межсетевого

экрана. Стоит отметить, если не устанавливать данный флаг и через «ИКС» проходит TCP трафик, то межсетевой экран при простое в 30 секунд разорвет данное соединение.

При установке правила «Через интерфейс» создаст правило маршрута через один из сетевых интерфейсов «ИКС».

При установке правила «Через провайдера» сетевой трафик будет направлен через одного из заведенных провайдеров на «ИКС».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:user_route

Last update: **2019/11/10 19:25**



Квота

При добавлении откроется окно настроек квоты. В данном окне расположены следующие поля:

- Адрес назначения,
- Протокол,
- Порт,
- Квота в день,
- Квота в неделю,
- Квота в месяц,
- выбор действия,
- пункт для установки флага «Создать разрешающее правило на метод CONNECT»;

Добавление квоты

Адрес назначения	Направление	
<input type="text" value="Внешние диапазоны адресов ✕"/>	<input type="text" value="Входящий"/>	
Протокол	Порт	
<input type="text" value="(любой)"/>	<input type="text" value="(любой)"/>	
Квота в день	Квота в неделю	Квота в месяц
<input type="text" value="50"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб	<input type="text" value="128"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб	<input type="text" value="512"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб
Действие:		
<input type="radio"/> Запретить доступ	<input checked="" type="radio"/> Ограничить скорость	
	<input type="text" value="256"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Кбайт/с	
	Направление	
	<input type="text" value="Входящий и исходящий"/>	
	Применять	
	<input type="text" value="для каждого ip"/>	
<input checked="" type="checkbox"/> Создавать разрешающее правило на метод CONNECT		
		<input type="button" value="Добавить"/> <input type="button" value="Отмена"/>

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС»

значения и объекты. Правило квоты используются для ограничения количества скачиваемой Пользователем или группой информации. При создании квоты, необходимо задать ограничение на объём скачиваемых данных в день/неделю/месяц, также возможно указание ресурса, протокола и порта, по которым будет учитываться квота. При установке любого из значений в «0», квота по этому периоду срабатывать не будет.

При превышении квоты Пользователем/группой, будет произведено выбранное действие в правиле. Или доступ Пользователя/группы будет заблокирован (при этом доступ остаётся только до ресурсов, на которые создано разрешающее правило «разрешить всегда»), или произойдет ограничение скорости (аналогичное созданию правила – ограничение скорости).

Установка флага «Создать разрешающее правило на метод CONNECT» означает, что пакеты с методом CONNECT будут разрешены для того, чтобы определить URL назначения при действующей HTTPS-фильтрации. В ином случае URL у HTTPS-трафика не будет определен. Это необходимо для того, чтобы выдать Пользователю страницу с сообщением «Квота превышена» при открытии HTTPS-страницы.

Примечание. Квота не будет работать в случае использования прозрачного прокси с установленным флагом «[Фильтровать без подмены сертификата](#)».

Примечание. Подсчет квоты происходит только на внешние диапазоны адресов, трафик до «ИКС» и из кэша прокси не входит в подсчет.

From:
<https://doc.a-real.ru/> - **Документация**

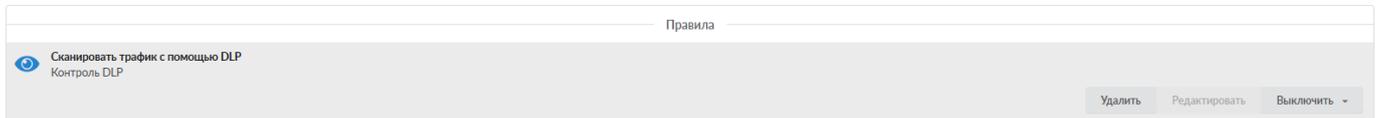
Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_quota

Last update: **2019/11/10 19:25**



Контроль DLP

Добавив данное правило, оно будет действовать если была произведена настройка модуля DLP, при настройке был установлен флажок «Использовать DLP для прокси», а также весь трафик идет через прокси.



При создании правила не появляется диалоговое, правило просто добавляется выбранному элементу (пользователю, группе или набору правил).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_dlp_rule

Last update: **2019/11/10 19:25**



Правило контентной фильтрации

Добавив данное правило, для данного пользователя начнет действовать контентная фильтрация содержимого страниц, если контент-фильтр был настроен.

Добавление правила контентной фильтрации

Действие:

Запретить доступ

Перенаправить на адрес

Вывести сообщение

Время действия

(всегда)

Добавить

Отмена

From:

<https://doc.a-real.ru/> - Документация

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:user_content_rule

Last update: **2019/11/10 19:25**



Все правила прокси и межсетевого экрана хранятся в профилях. Профиль - это простой набор правил. Профили могут принадлежать Пользователю, группе Пользователей и роли Пользователя. Пользователю, группе Пользователей и роли Пользователя при создании назначается свой личный профиль, в него добавляются персональные правила. Пользователю при создании назначается роль, соответственно к Пользователю применяется профиль этой роли. Помимо личных профилей Пользователю и группе можно добавлять произвольное количество отдельно созданных профилей. В результате Пользователь имеет: личный профиль, профиль назначенной роли, отдельно добавленные профили. Группа имеет: личный профиль, отдельно добавленные профили. Приоритет профилей при анализе трафика для Пользователей:

1. Личный профиль Пользователя
2. Профиль назначенной роли и добавленные профили для Пользователя. ВАЖНО: эти профили объединяются и проверяются как один профиль
3. Профиль родительского группы
4. Профили, добавленные на родительскую группу. ВАЖНО: данные профили объединяются и проверяются как один профиль
5. Повторение шагов 3 и 4 пока не достигнется корневая группа

В каждом профиле правила проверяются в следующем порядке:

1. Исключения
2. Разрешающие
3. Запрещающие
4. Контент-фильтр и DLP

Если совпало разрешающее или запрещающее правило, то проверка всех правил текущего и последующих профилей завершается на этом моменте, кроме правил контент-фильтра и правил DLP текущего профиля. Если совпало правило исключения, то проверка ВСЕХ последующих правил в текущем профиле пропускается и процесс проверки правил переходит к следующему профилю.

From:
<https://doc.a-real.ru/> - **Документация**

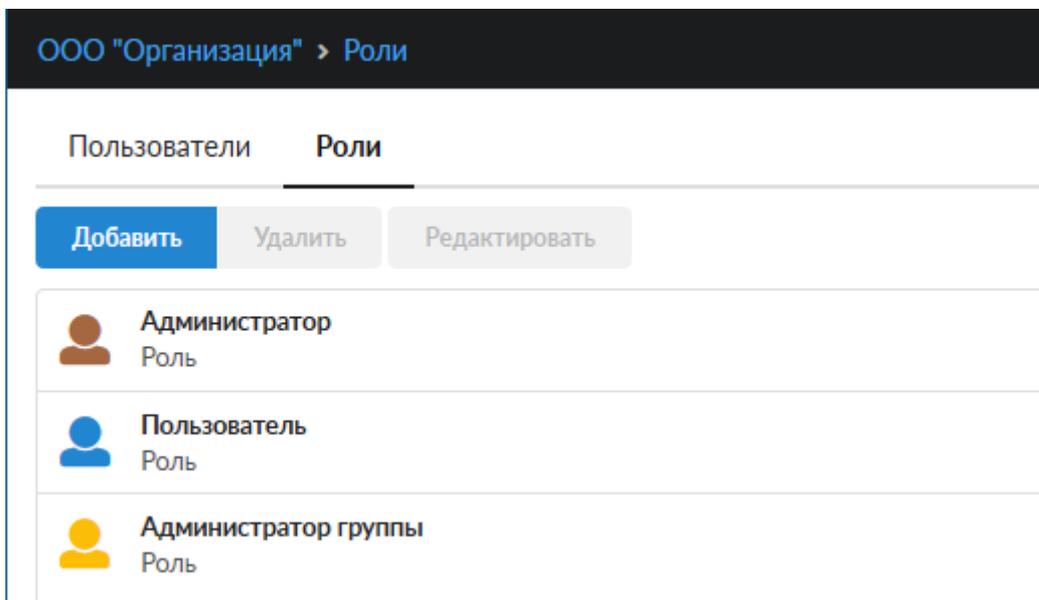
Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:user_rules_execution_order

Last update: **2019/11/10 19:25**



Роли

Модуль «Роли» расположен в Меню «Пользователи и статистика». Данный модуль определяет привилегии Пользователей «ИКС» по управлению УТМ. По умолчанию доступны следующие роли Пользователей «ИКС»: «Администратор», «Пользователь», «Администратор группы».



Роль	Возможности
«Администратор»	Пользователь «ИКС» имеет полный доступ ко всем функциям веб-интерфейса УТМ-изделия
«Пользователь»	Пользователь «ИКС» имеет доступ только к своей персональной странице, к изменению собственного пароля, к просмотру статистики
«Администратор группы»	Пользователь «ИКС» имеет доступ к функциям создания, удаления, редактирования, назначения правил, квот и просмотра статистики Пользователей, объединённых в группу, при этом администратор также находится в данной группе.

Добавление роли

Название *	Описание	Иконка
<input type="text" value="Смотритель"/>	<input type="text" value="Все видит, но ничего не может"/>	 <input type="text"/>

Права доступа

Администратор группы

- Просмотр дочерних пользователей
- Редактирование дочерних пользователей
- Просмотр звонков дочерних пользователей

Ip-адреса пользователя

- Просмотр ip и mac-адресов пользователя
- Редактирование ip-адресов пользователя
- Редактирование связи ip с mac

Правила пользователя

- Просмотр правил пользователя
- Редактирование правил пользователя

Для того чтобы создать собственную роль в «ИКС», необходимо нажать «Добавить». Будет открыто новое окно, в котором будет предложено ввести: название добавляемой роли, описание, выбрать иконку и выбрать привилегии, которые получит Пользователь «ИКС» в этой роли.

 **Смотритель**
Роль - Все видит, но ничего не может

- Просмотр дочерних пользователей
- Просмотр звонков дочерних пользователей
- Просмотр ip и mac-адресов пользователя
- Просмотр правил пользователя
- Просмотр почтовых ящиков пользователя
- Просмотр телефонных номеров пользователя
- Просмотр перенаправлений телефонии
- Просмотр событий пользователя
- Просмотр статистики пользователя

После добавления новой роли, в модуле «Наборы правил», создается пустой набор правил, жестко закрепленный за созданной ролью, аналогично наборам правил для «Пользователей», «Администраторов» и «Администраторов группы». Редактировать или удалять роли возможно

все, кроме ролей «Пользователь» и «Администратор».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:roles>

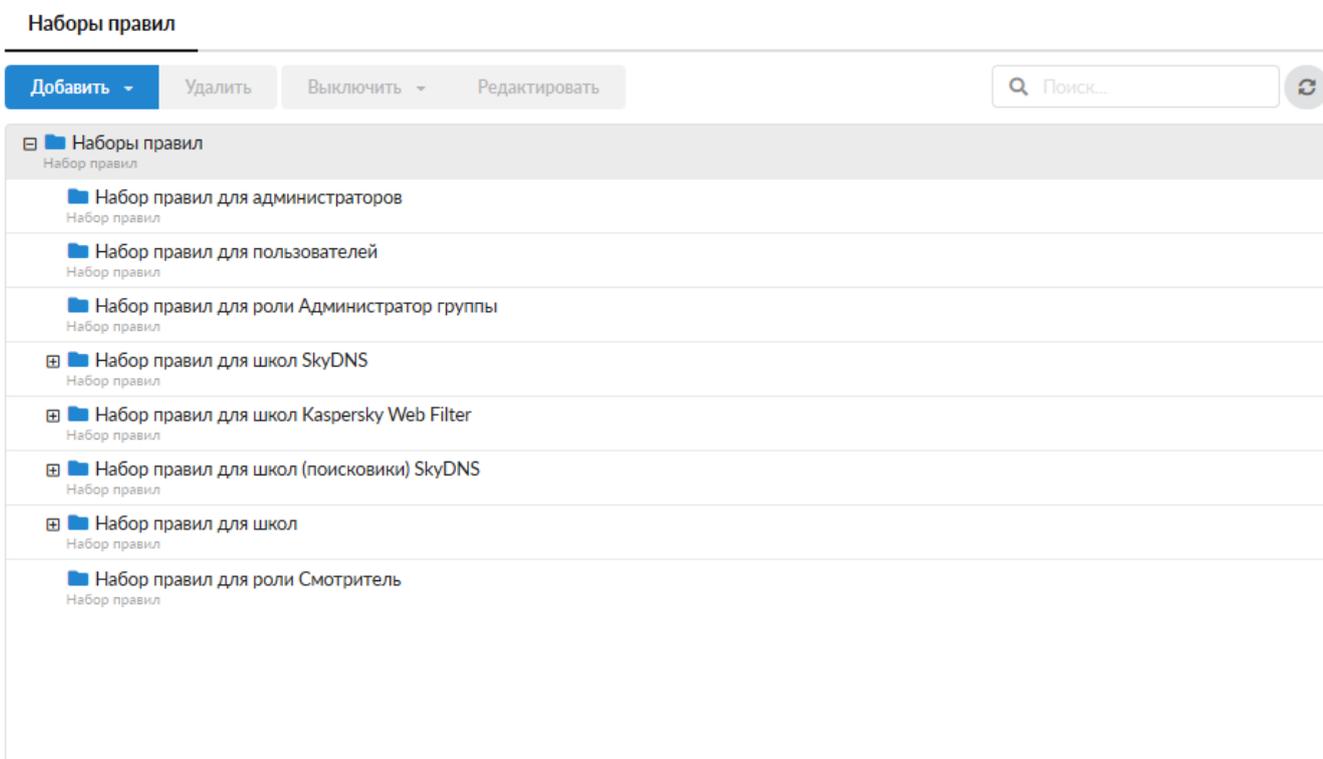
Last update: **2019/11/10 19:25**



Наборы правил

Общая информация

Модуль «Наборы правил» расположен в Меню «Пользователи и статистика». Данный модуль предназначен для создания наборов правил – глобальные объекты, позволяющие сохранить любое количество Пользовательских правил под указанным именем и применить без повторной настройки сразу к нескольким Пользователям или группам Пользователей. При этом под Пользовательским правилом может пониматься следующее: запрещающее правило, запрещающее правило Application firewall, разрешающее правило, исключение, запрещающее правило прокси, разрешающее правило прокси, исключение прокси, ограничение количества соединений, ограничение скорости, выделение полосы пропускания, маршрут, квота, контроль DLP, правило контентной фильтрации.



По умолчанию в модуле «Наборы правил» созданы пустые наборы правил для каждой роли заведенный в «ИКС», а также четыре пред настроенных набора: набор правил для школ SkyDNS, набор правил для школ Kaspersky Web Filter, набор правил для школ (поисковики) SkyDNS, набор правил для школ. Стоит отметить, что наборы правил для ролей нельзя удалить, возможно удалить роль (кроме, «Администратор» и «Пользователь»), при этом удалиться набор правил связанных с данной ролью. При добавлении новой роли будет автоматически создан пустой набор правил.

Набор правил для школ SkyDNS

- Разрешить доступ используя метод CONNECT
- Разрешить доступ на адрес /[^](https?:\|/)?(.\|/)?yandex\.ru\|.\|?.*&family=yes/
- Разрешить доступ на адрес /[^](https?:\|/)?www\.google\.(ru|com)\|.\|&safe=active/
- Запретить доступ на адрес Черные сайты, Информация для взрослых, Запрещено по законодательству
- Перенаправить на адрес <url>&family=yes при обращении на адрес /[^](https?:\|/)?(.\|/)?yandex\.ru\|yandsearch\|?.*|, /[^](https?:\|/)?(.\|/)?yandex\.ru\|search\|?.*|
- Перенаправить на адрес <url>&family=yes при обращении на адрес /[^](https?:\|/)?(.\|/)?yandex\.ru\|[A-Za-z]+\|search\|?.*|
- Перенаправить на адрес <url>&safe=active при обращении на адрес /[^](https?:\|/)?www\.google\.(ru|com)\|search.*|
- Сканировать трафик с помощью контент-фильтра

Набор правил для школ SkyDNS. Данный набор правил предоставляет доступ к поисковым системам в безопасном режиме; блокирует доступ к интернет ресурсам из набора **категорий** (общие, черные сайты, сайты для взрослых, мошенничество, вирусы), в том числе от сервиса SkyDNS; сканирует трафик с помощью **контент-фильтра** (если контент-фильтр включен).

Набор правил для школ Kaspersky Web Filter. Данный набор правил аналогичен набору правил для школ SkyDNS, основным отличием является использование наборов категорий трафика, предоставляемых компанией Kaspersky.

Набор правил для школ (поисковики) SkyDNS. Данный набор правил аналогичен набору правил для школ SkyDNS, основным отличием является перенаправление запросов к любой поисковой системе на поисковую систему SkyDNS (search.skydns.ru).

Набор правил для школ. Данный набор правил предоставляет доступ к поисковым системам в безопасном режиме; разрешает доступ на адреса из реестра безопасных образовательных сайтов (РБООС); блокирует доступ к интернет ресурсам из набора **категорий** (списки сайтов для блокировки от Минюста и Роскомнадзора, мошенничество, порно, вирусы); сканирует трафик с помощью **контент-фильтра** (если контент-фильтр включен).

Набор правил для школ (поисковики) SkyDNS

- Разрешить доступ используя метод CONNECT
- Разрешить доступ на адрес search.skydns.ru
- Запретить доступ на адрес Черные сайты, Информация для взрослых, Запрещено по законодательству
- Перенаправить на адрес search.skydns.ru при обращении на адрес /[^](https?:\|/)?(.\|/)?yandex\.ru.*|
- Перенаправить на адрес search.skydns.ru при обращении на адрес /[^](https?:\|/)?(.\|/)?google\.(ru|com).*|
- Перенаправить на адрес search.skydns.ru при обращении на адрес /[^](https?:\|/)?(.\|/)?rambler\.ru.*|
- Перенаправить на адрес search.skydns.ru при обращении на адрес /[^](https?:\|/)?(.\|/)?mail\.ru.*|
- Перенаправить на адрес search.skydns.ru при обращении на адрес Поисковые системы
- Сканировать трафик с помощью контент-фильтра

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 Пользовательских правил, в качестве сравнения можно привести создание каталога для файлов. Для добавления определенного Пользовательского

правила, необходимо выделить имя набора и нажать «Добавить» или 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. Также в данном модуле будут доступны вкладки «Пользователи» и «События».

Для применения созданных правил к Пользователю существует два похода. Во-первых, в меню «Пользователи» выбрать соответствующего Пользователя двойным нажатием, в открывшемся модуле, перейти во вкладку «Правила и ограничения» и в данной вкладке нажать «Добавить», в выпавшем списке выбрать «Набор правил», и затем выбрать нужный набор правил из списка. Во-вторых, в модуле «Наборы 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.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:rulesets>

Last update: **2019/11/10 19:25**



Категории трафика

Модуль «Категории трафика» расположен в Меню «Пользователи и статистика». Данный модуль служит для объединения множества IP адресов, URL (Uniform Resource Locator) и содержащихся в URL расширений, поисковых запросов, mime-типов в единую категорию. Данные категории трафика применяются при создании запрещающих правил, разрешающих правил или исключений прокси в модуле «Наборы правил» в поле «URL назначения» для Пользователей или групп Пользователей.

Встроенные категории трафика

ООО "Организация" > Категории трафика Администратор 161

Категории трафика Категории трафика SkyDNS Категории трафика Касперского

Добавить

	Адреса
Аудио-видео	02birish.com, 02musiccrew.com, 04849.com.ua, 05161.com.ua, 061.ua, ...
Баннеры	01sexe.com, 0b02c65aa00d.sgizmo..., Oriflaine.ru, 1.im.cz, 1.photoshop-m...
Веб-почта	004.com, 005.com, 006.com, 10jqka.com, 121-free-email.com, ...
Вирусы	1000turov.ru, 1xgya.top, 1xvoh.top, 21art.cn, 21ebuild.com, ...
Игры	00000onlinecasino.co..., 02casino.com, 0x10c-zone.ru, 1-bingo-online.com,...
Мошенничество	0fees.net, 200btc.ru, 5sec.info, 75tz.com/feat, 75tz.com/z, ...
Поисковые системы	104591677.keywordblo..., 123coimbatore.com, 1c-kursy.ru, 1gs.ru, 1sberb...
Порно	0--gratis.dk, 0--oralsex.dk, 0-0-6.dk, 0-0-adult-superstore..., 0-0adultsexvid...
Прокси	0-5.us, 0.0dt.net, 000.baboproxy.com, 000.myspacepro.info, 000.publicpro...
Реестр безопасных образовательных сайтов	.детсад-уфа.пф/, .dou-nn.ru/, 0.детсад-уфа.пф, 01.maam.ru/, 1.35337.ds...
Социальные сети	*.love-germany.com, 1000personals.com, 100druzei.com, 11a.ru, 12.com.u...
Список сайтов для блокировки от Минюста	06-ingushetiya.livej..., 14.ucoz.ru, 2britney.ru/La+Vida+..., 2ch-b.ru/2013/1...
Список сайтов для блокировки от Роскомнадзора	0.new-rutor.org/torr..., 0.the-rutor.org/torr..., 0.the-rutor.org/torr..., 0.the-r...
Файлообменники	000.myspacepro.info, 247proxy.info, 24f.ru, 2baksa.net, 2baksa.net, ...
Фотогалереи	10f.ru, 10f.ru/gallery/3, 1den.ru, 1zoom.ru, 35photo.ru, ...
Чаты	0chan.ru, 13397.chatcity.ru, 4at.zp.ua, 4bb.ru, 4livegaysex.com, ...

В окне модуля отображены все заведенные группы категорий трафика. Встроенные группы редактировать и удалить нельзя, возможно только экспортировать содержимое категории.

Категории трафика SkyDNS

Группы обозначенные логотипом компании «СкайдНС» (щит сине-черный) будут заполнены в случае приобретения соответствующего модуля.

Поиск...  

<input type="checkbox"/>  Запрещено по законодательству
<input type="checkbox"/>  Информация для взрослых
<input type="checkbox"/>  Алкоголь и табак <small>Сайты с информацией об алкоголе, табаке. Табачные и алкогольные интернет-магазины</small>
<input type="checkbox"/>  Астрология <small>Сайты, посвященные оккультизму и астрологии, сайты астрологов</small>
<input type="checkbox"/>  Знакомства <small>Сайты знакомств</small>
<input type="checkbox"/>  Казино, лотереи, тотализаторы <small>Сайты казино и прочих игровых систем</small>
<input type="checkbox"/>  Порнография и секс <small>Сайты, содержащие порнографию в любом виде</small>
<input type="checkbox"/>  Сайты для взрослых <small>Сайты с информацией для взрослых, чаще всего по вопросам секса</small>
<input type="checkbox"/>  Пожиратели времени
<input type="checkbox"/>  Пожиратели трафика
<input type="checkbox"/>  Прочие сайты
<input type="checkbox"/>  Черные сайты

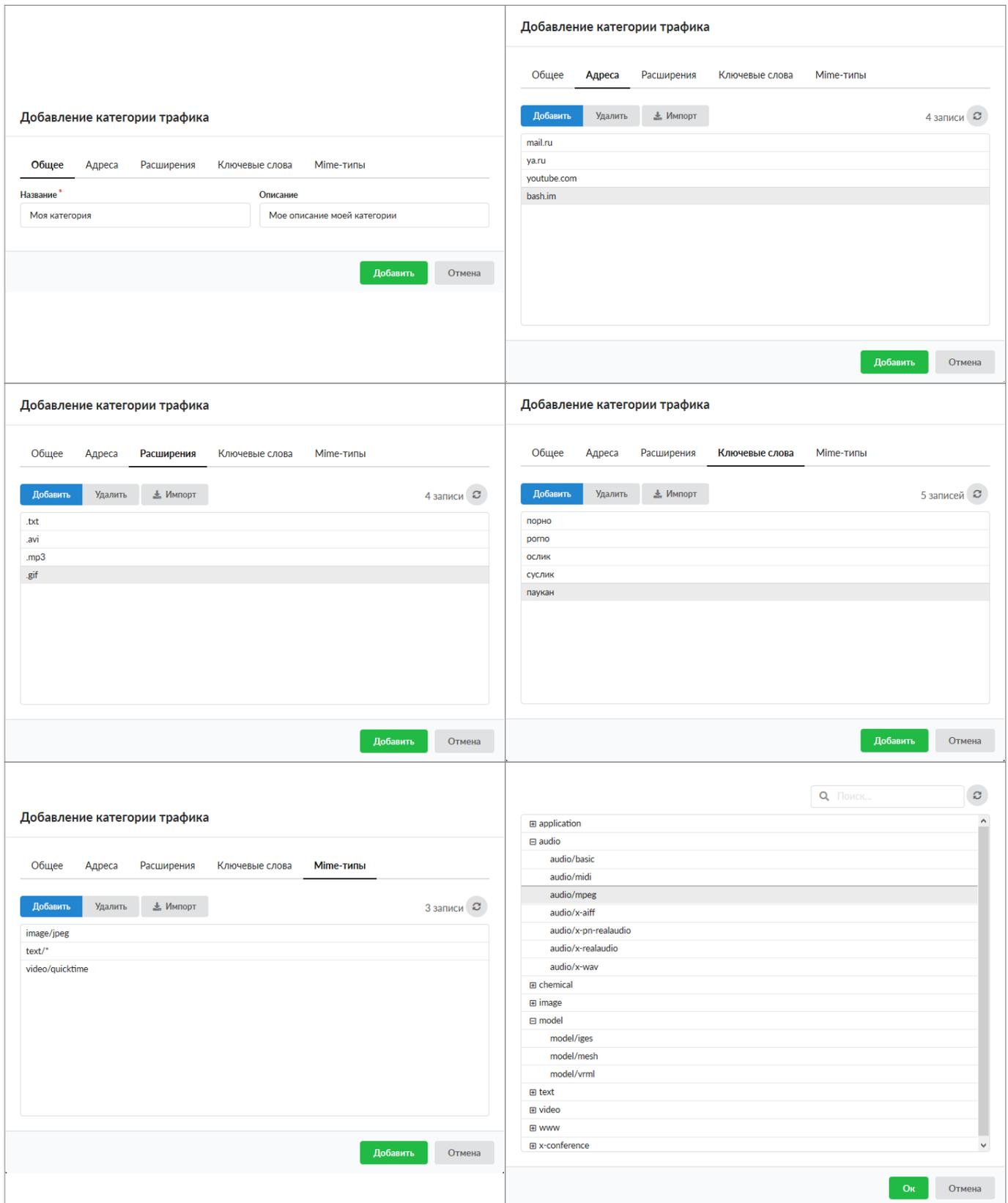
Категории трафика Касперского

Группы обозначенные логотипом компании «Лаборатория Касперского» будут заполнены в случае приобретения соответствующего модуля.

Поиск...  

<input type="checkbox"/>  Азартные игры, лотереи, тотализаторы
<input type="checkbox"/>  Алкоголь, табак, наркотики и психотропные вещества
<input type="checkbox"/>  Для взрослых
<input type="checkbox"/>  Запрещено законами Российской Федерации <small>Контент, заблокированный по законам Российской Федерации</small>
<input type="checkbox"/>  Информационные технологии
<input type="checkbox"/>  Красота, здоровье, здоровый образ жизни
<input type="checkbox"/>  Культура, общество
<input type="checkbox"/>  Ненависть, дискриминация
<input type="checkbox"/>  Образование
<input type="checkbox"/>  Программное обеспечение, аудио и видео
<input type="checkbox"/>  Средства интернет-коммуникации
<input type="checkbox"/>  Хобби и развлечения
<input type="checkbox"/>  Электронная коммерция
<input type="checkbox"/>  Tor <small>Узлы Tor</small>
<input type="checkbox"/>  Вредоносные сайты <small>Вредоносные ресурсы или ссылки на скачивание вредоносного ПО</small>
<input type="checkbox"/>  Динамические DNS <small>Ресурсы, предоставляемые сервисами динамических DNS</small>
<input type="checkbox"/>  Для детей <small>Контент для детей. Включает образовательный и развлекательный контент, чаты</small>
<input type="checkbox"/>  Инструменты удалённого администрирования <small>Ресурсы, содержащие инструменты удалённого администрирования</small>
<input type="checkbox"/>  Потенциально опасное ПО <small>Контент, относящийся к легитимным программам, которые могут причинить вред, если будут использоваться злоумышленниками (для удаления, блокировки, модификации или копирования данных, для нарушения производительности компьютеров или сетей)</small>
<input type="checkbox"/>  Реклама <small>Контент, относящийся к ПО, которое загружает или отображает нежелательную рекламу, когда пользователь онлайн, собирает маркетинговые данные и другую информацию без ведома пользователя или перенаправляет поисковые запросы на конкретные рекламные сайты</small>
<input type="checkbox"/>  Фишинговые сайты

Для того, чтобы создать собственную категорию трафика, содержащую набор IP адресов, набор URL, расширений, поисковых запросов или mime-типов, необходимо нажать кнопку «Добавить» и выбрать пункт «Категория трафика».



Выбрав данный пункт откроется диалоговое окно со вкладками. На первой, предлагается ввести название новой категории и при необходимости добавить ее описание. На вкладке «Адреса» задаются URL и IP адреса. На вкладке «Расширения» задаются всевозможные расширения, данная возможность позволяет прокси серверу при обработке URL обнаружить соответствующее расширение и произвести соответствующее действие (разрешить/запретить/исключить). На вкладке «Поисковый запрос» задаются слова или словосочетания и при обнаружении прокси сервером соответствующих слов в URI произойдет соответствующее действие (разрешить/запретить/исключить). На вкладке «Mime-типы»

возможно задать mime-заголовки и mime-расширения файлов, определенные по стандартам. При обнаружении соответствующего mime-типа в URL прокси сервер произведет соответствующее действие (разрешить/запретить/исключить). 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 «Импорт».

Если необходимо объединить несколько категорий трафика под одним именем, то необходимо нажать кнопку «Добавить» и выбрать пункт «Группа категорий трафика». В «ИКС» реализована функция drag-and-drop, поэтому созданные категории легко можно переместить в группу.

Добавление категории трафика

Название *	Описание
<input type="text" value="Моя классная автоматическая категория"/>	<input type="text" value="Описание"/>
URL для адресов	URL для расширений
<input type="text" value="http://test.local/url.txt"/>	<input type="text" value="http://test.local/ext.txt"/>
URL для ключевых слов	URL для mime-типов
<input type="text" value="http://test.local/keys.txt"/>	<input type="text" value="URL для mime-типов"/>
<input checked="" type="checkbox"/> Автоматически обновлять категорию	
Период	
<input type="text" value="раз в неделю"/>	
День недели	
<input checked="" type="radio"/> Пн <input type="radio"/> Вт <input type="radio"/> Ср <input type="radio"/> Чт <input type="radio"/> Пт <input type="radio"/> Сб <input type="radio"/> Вс	
Время	
<input type="text" value="00:00"/>	

Для оптимизации процесса составления, изменения и актуализации в группах значений во вкладках «Адреса», «Расширение», «Поисковые запросы» или «Mime-типы», необходимо выбрать пункт «Автоматическая категория трафика» и указать путь URL, на вкладке «Общее», где расположены соответствующие текстовые файлы, а также указать частоту обновления данных файлов. Автоматические категории будут иметь логотип в виде тома с цепью. Выделив автоматическую категорию, ее можно будет обновить, не дожидаясь заданного временного интервала.

Важно: категории «Список сайтов для блокировки от Минюста», «Список сайтов для

блокировки от Роскомнадзора» и «Реестр безопасных образовательных сайтов» первоначально не содержат URL. Для доступа к спискам URL и фильтрации по перечисленным категориям необходим модуль «Техподдержка» для ИКС (первый год активен по умолчанию у всех клиентов, далее требуется его ежегодное приобретение).

Примечание

Категория «Реестр безопасных образовательных сайтов» соответствует *Методическим рекомендациям по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью или развитию детей, а также не соответствующей задачам образования* (<http://www.скф.единыйурок.рф>). Из категории исключен адрес **yandex.ru**, чтобы исключить конфликт с перенаправлением на безопасный поиск яндекс (<https://yandex.ru/?family=yes>) в наборах правил для школ.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:category>

Last update: **2019/12/03 15:25**



Монитор соединений

Модуль «Монитор соединений» расположен в Меню «Пользователи и статистика». Монитор соединений предназначен для контроля потоков трафика.

Отображать только активные соединения

Поиск...

Имя ^	Кол-во соед.	Время соед.	Пакеты	Байты	Пакетов/сек	Байт/сек
ИКС	988		1953119	1.09Г		
Корневая группа	1017		2154155	1.05Г	+21.21	+23.98 +302.94K +41.14K
CloudX	0		0			
build_server	5		156274	82.80M	+0.13	+0.13 +10.05K +855.66
ИКС	492		960060	610.30M	+7.16	+9.64 +149.13K +27.23K
Менеджеры	354		525741	348.87M	+5.16	+5.20 +89.90K +4.15K
Серверная	144		419364	33.61M	+5.38	+5.54 +1.75K +1.74K
Тех.поддержка	22		92716	8.11M	+3.37	+3.47 +52.09K +7.17K

Верхняя панель модуля позволяет выбрать, каким образом отображать рабочие соединения - деревом или списком, а также выбрать опцию «отображать порт источника». Причем в списке будут отображены только те пользователи, которые имеют соединения в реальном времени.

В таблице соединений могут отображаться следующие столбцы: имя пользователя, количество соединений, протокол, состояние, время соединения, оставшееся время соединения, число прошедших пакетов, объем скачанной информации по соединению в байтах, скорость соединения в пакетах/секунду и в байтах/секунду. Также, как и в других модулях, таблица соединений состоит из столбцов, видимость которых регулируется выпадающим меню.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:pftop>

Last update: **2019/11/10 19:25**



Диапазоны адресов

Модуль «Диапазоны адресов» расположен в Меню «Пользователи и статистика». Данный модуль содержит список всех объектов тарификации, по которым «ИКС» ведет учет. По умолчанию созданы следующие категории объектов: DMZ-сети; внешние диапазоны адресов (провайдеры), ИКС, корневая группа (содержит всех заведенных Пользователей «ИКС» и группы, в которых они состоят), локальные сети, пользовательские диапазоны адресов. Все категории объектов, кроме категории «Пользовательские диапазоны адресов», заполняются автоматически из соответствующих модулей и не могут быть изменены в данном модуле. Категория «Пользовательские диапазоны адресов» предназначена для создания объектов тарификации «ИКС», к которым можно применять различные правила и использовать для оптимизации действий в других модулях. В основном окне модуля также присутствует строка поиска и кнопки «Добавить», «Удалить» и «Редактировать».

The screenshot shows the 'Addresses Ranges' module interface. At the top, there is a breadcrumb 'Муми-дол > Диапазоны адресов' and user information 'Туве Янссон'. Below the breadcrumb are buttons for 'Добавить', 'Удалить', and 'Редактировать', along with a search bar and a refresh icon. The main content is a table with the following data:

Имя	Трафик в день		Трафик в месяц	
DMZ сети				
Внешние диапазоны адресов	▼2.92M	▲2.92M	▼2.92M	▲2.92M
Интернет	▼878.51K	▲878.51K	▼878.51K	▲878.51K
Моррателеком (192.168.170.242/24)	▼1.06M	▲1.06M	▼1.06M	▲1.06M
социалочки	▼1.05M	▲1.05M	▼1.05M	▲1.05M
ИКС	▼70.56M	▲12.21M	▼70.56M	▲12.21M
Корневая группа	▼37.00M	▲2.33M	▼37.00M	▲2.33M
Локальные сети	▼9.68M	▲514.58K	▼9.68M	▲514.58K
Муми-локалка (192.168.17.242/24)	▼9.68M	▲514.58K	▼9.68M	▲514.58K
Пользовательские диапазоны адресов				

The second screenshot shows the same interface but with a sidebar menu on the left containing items like 'Пользователи и статистика', 'Пользователи', 'Роли', 'Наборы правил', 'Категории трафика', 'Монитор соединений', 'Диапазоны адресов', 'Отчеты', 'Управление отчетами', and 'Синхронизация'. The table data in this view is as follows:

Имя	Трафик в день		Трафик в месяц	
DMZ сети				
Внешние диапазоны адресов	▼2.62M	▲2.62M	▼56.06M	▲56.06M
Интернет	▼1.73M	▲1.73M	▼36.50M	▲36.50M
Новый провайдер	▼912.49K	▲912.49K	▼19.55M	▲19.55M
ИКС	▼17.79M	▲12.66M	▼237.27M	▲212.05M
Корневая группа	▼4.22M	▲685.47K	▼12.72M	▲1.20M
Локальные сети	▼0	▲2.44M	▼1.37K	▲62.35M
Новая локальная сеть	▼0	▲2.44M	▼1.37K	▲62.35M
Пользовательские диапазоны адресов	▼1.23K	▲1.65K	▼164.14K	▲50.75K
Новый диапазон адресов77	▼1.23K	▲1.65K	▼164.14K	▲50.75K

Для добавления категории «Пользовательский диапазон адресов» необходимо нажать кнопку «Добавить» и выбрать соответствующий пункт. Будет открыто новое диалоговое окно, в котором будет предложено ввести: название диапазона; указать является ли данный диапазон

внешним или внутренним; добавить, удалить или импортировать диапазон адресов. По умолчанию любой создаваемый диапазон адресов является внутренним (не тарифицируемым). В качестве примера, внутреннего диапазона адресов, можно привести создание диапазона адресов, предоставляемых оператором связи к своим внутренним ресурсам, которые не тарифицируются оператором и соответственно не оплачиваются по тарифу. Для того чтобы диапазон адресов приобрел статус «внешний», необходимо установить соответствующий флаг «Внешний диапазон адресов» при настройке.

Добавление диапазона адресов

Название *

 Внешний диапазон адресов
Адреса:

Добавить Удалить Импорт

Сохранить Отмена

При добавлении диапазона адресов допускаются следующие варианты: произвольные IP-адреса (например, 192.168.1.123), подсети (например, 192.168.1.1/24 или 192.168.1.1/255.255.255.0), доменные имена (например, ya.ru), диапазоны (например, 192.168.1.53-192.168.1.87). Если диапазон адресов слишком велик, чтобы вводить их по одному в веб-интерфейсе «ИКС», возможно загрузить его из текстового файла формата *.txt нажав «Импорт». В нем должны быть перечислены с каждой новой строки: ip-адреса, подсети, доменные имена или диапазоны.

From:
<https://doc.a-real.ru/> - **Документация**

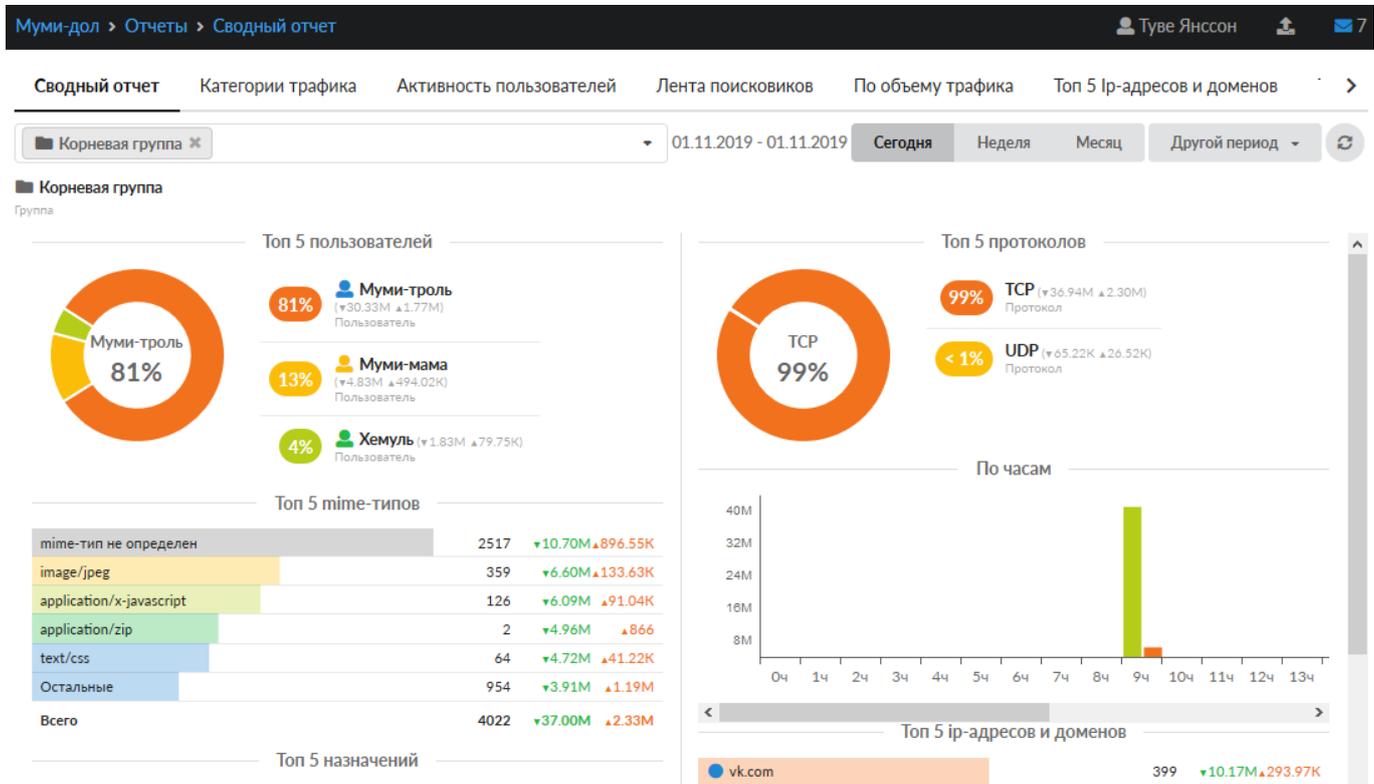
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:diapazones>

Last update: **2019/11/10 19:25**



Отчеты

Система статистики пользователей в ИКС может быть как настроена вручную, так и выведена с помощью нескольких стандартизованных отчетов. Все они представлены в модуле «Отчеты», который находится в Меню «Пользователи и статистика».



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.

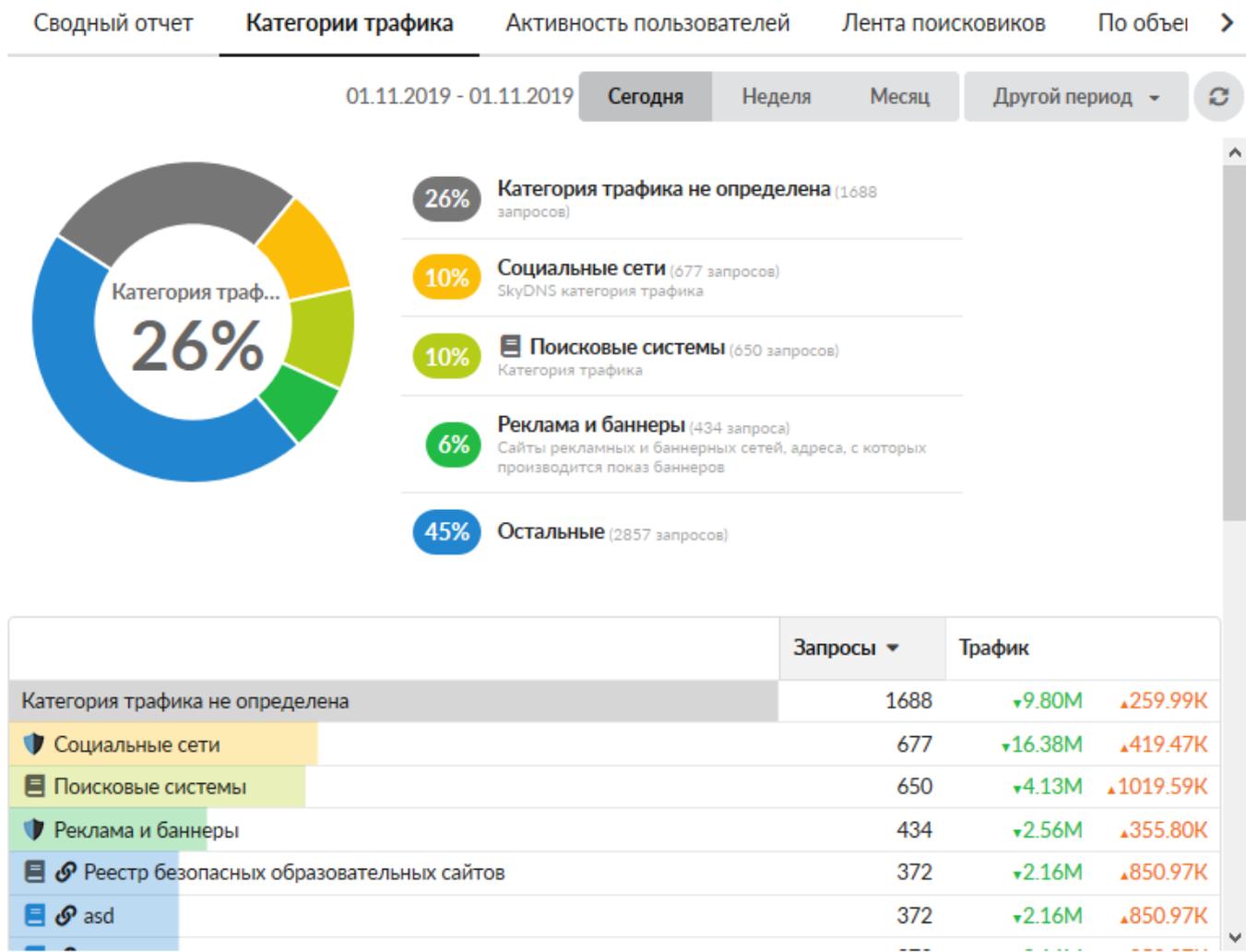
Сводный отчет

Вкладка «Сводный отчет». На данной вкладке отображаются основные данные по трафику пользователей:

- Топ 5 пользователей - пользователи с самым большим общим трафиком за период, с процентным отношением к общему трафику всех пользователей
- Топ 5 IP-адресов и доменов - самые часто запрашиваемые сайты
- Топ 5 mime-типов - самые распространенные типы запрашиваемых данных
- Топ 5 назначений - самые распространенные назначения запросов - диапазоны адресов
- Топ 5 протоколов - самые распространенные протоколы, по которым идут соединения
- По часам - почасовая статистика за период

В левой верхней части вкладки находится поле для указания группы пользователей, по которым будет построен отчет. По умолчанию это корневая группа пользователей.

Категории трафика



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

Активность пользователей

Сводный отчет Категории трафика **Активность пользователей** Лента поисковиков По объему т >

Корневая группа x 01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период x ↻

↑ Экспорт ▾

↓ ↑
http://htmlbook.ru 09:31:48 Муми-троль
https://video-play.ru/rollscript.php 09:37:19 Муми-троль
https://www.povarenok.ru/recipes/find 09:41:57 Муми-мама
http://www.rusmarka.ru/catalog/marki.aspx 09:43:41 Хемуль

Вкладка «Активность пользователей». На данной вкладке отображаются страницы, загруженные пользователями. В левой верхней части вкладки находится поле для указания группы пользователей, по которым будет построен отчет. По умолчанию это корневая группа пользователей. При необходимости можно сохранить данные отчета в файл, нажав кнопку «Экспорт».

Лента поисковиков

Сводный отчет Категории трафика Активность пользователей **Лента поисковиков** По объему т >

Корневая группа x 01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период x ↻

↑ Экспорт ▾

↓ ↑
где искать шляпу волшебника 09:37:03 Муми-троль
куда ушел Выхухоль 09:38:15 Муми-троль
облака из скорлупы 09:41:12 Муми-мама
рецепты онлайн 09:41:54 Муми-мама
марки 09:43:38 Хемуль
бабочки почтой 09:43:58 Хемуль

Вкладка «Лента поисковиков». На данной вкладке отображаются поисковые запросы пользователями. В левой верхней части вкладки находится поле для указания группы пользователей, по которым будет построен отчет. По умолчанию это корневая группа пользователей. При необходимости можно сохранить данные отчета в файл, нажав кнопку «Экспорт».

По объему трафика

< Лента поисковиков **По объему трафика** Топ 5 Ip-адресов и доменов Топ 5 пользователей

01.11.2019 - 01.11.2019

Сегодня

Неделя

Месяц

Другой период ▾



Экспорт ▾

	Запросы	Трафик ▾	
Муми-троль	2949	▼30.33M	▲1.77M
Муми-мама	887	▼4.83M	▲494.02K
Хемуль	186	▼1.83M	▲79.75K
Всего	4022	▼37.00M	▲2.33M

« < Стр 1 из 1 > »

Показаны записи 1 - 3 из 3

Вкладка «По объему трафика». На данной вкладке отображается объем входящего и исходящего трафика пользователей. При необходимости можно сохранить данные отчета в файл, нажав кнопку «Экспорт».

Топ 5 ip-адресов и доменов

Лента поисковиков По объему трафика **Топ 5 ip-адресов и доменов** Топ 5 пользователей

01.11.2019 - 01.11.2019

Сегодня

Неделя

Месяц

Другой период



Экспорт

	Запросы	Трафик	
vk.com	399	▼10.17M	▲293.97K
userapi.com	540	▼4.58M	▲106.84K
gvt1.com	4	▼4.53M	▲751
yandex.ru	542	▼2.16M	▲852.32K
vkuservideo.net	23	▼1.51M	▲7.18K
Остальные	2514	▼14.03M	▲1.10M
Всего	4022	▼37.00M	▲2.33M

Топ 5 пользователей для vk.com ▼10.17M ▲293.97K



- 76% Муми-троль (▼7.77M ▲228.70K)
- 23% Муми-мама (▼2.38M ▲62.87K)
- < 1% Хемуль (▼6.43K ▲2.39K)

Вкладка «Топ 5 ip-адресов и доменов». На данной вкладке отображается трафик пользователей, сгруппированный по ip-адресам и доменам. Под сводкой адресов можно увидеть краткую сводку по пользователям, запрашивающим каждый адрес. При необходимости можно сохранить данные отчета в файл, нажав кнопку «Экспорт».

Топ 5 пользователей

01.11.2019 - 01.11.2019

Сегодня

Неделя

Месяц

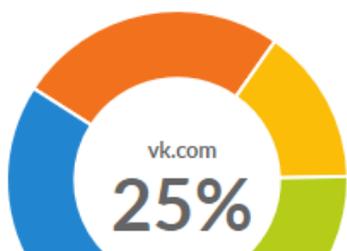
Другой период



Экспорт

	Запросы	Трафик	
Муми-троль	2949	▼30.33M	▲1.77M
Муми-мама	887	▼4.83M	▲494.02K
Хемуль	186	▼1.83M	▲79.75K
Всего	4022	▼37.00M	▲2.33M

Топ 5 IP-адресов и доменов для Муми-троль ▼30.33M ▲1.77M



- 25% vk.com (▼7.77M ▲228.70K)
- 14% gvt1.com (▼4.53M ▲751)
- 14% userapi.com (▼4.25M ▲80.78K)

Вкладка «Топ 5 пользователей». На данной вкладке отображается краткая сводка входящего и исходящего трафика пользователей. Под сводкой можно увидеть краткую сводку по IP-адресам и доменам, запрошенным каждым пользователем. При необходимости можно сохранить данные отчета в файл, нажав кнопку «Экспорт».

From: <https://doc.a-real.ru/> - Документация

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:statistics>

Last update: 2019/11/10 19:25



Управление отчетами

Модуль «Управление отчетами» расположен в Меню - «Пользователи и статистика». Данный модуль позволяет управлять и настраивать службы «Статистика» и «Счетчики», а также предоставляет возможность формирования отчетов работы данных служб как в произвольной форме, так и в предустановленных формах. Данный модуль содержит вкладки: «Управление отчетами», «Конструктор отчетов», «Службы», «Настройки», «Журнал».

Муми-дол > Управление отчетами
Тыве Янссон 12

Управление отчетами
Конструктор отчетов
Службы
Настройки
Журнал

Добавить
Удалить
Редактировать
01.11.2019 - 01.11.2019
Сегодня
Неделя
Месяц
Другой период ▾

Экспорт ▾

		Запросы	Трафик ▾	
По пользователям				
По интерфейсам	Корневая группа	4250	+37.55M	+2.40M
Топ 20 пользователей	Мумики	3836	+35.16M	+2.25M
Топ 20 доменов	Муми-троль	2949	+30.33M	+1.77M
Топ 5 пользователей	Муми-мама	887	+4.83M	+494.02K
Топ 5 протоколов	Муми-папа	0	+0	+0
Топ 5 mime-типов	Муми-дол	414	+2.38M	+151.13K
Топ 5 ip-адресов и доменов (по пользователям)	Тыве Янссон	0	+0	+0
Топ 5 пользователей (по ip-адресам и доменам)	Liza	0	+0	+0
	Снусмумрик	0	+0	+0
По часам	Снорки	0	+0	+0
Топ 5 назначений	Морра	0	+0	+0
Топ 5 ip-адресов и доменов	Тыве Янсон	0	+0	+0
Активность пользователей	Всего	4250	+37.55M	+2.40M

Вкладка «Управления отчетами». Данная вкладка разделена на два окна. В первом, отображается список всех отчетов – предустановленных системой и созданных Пользователем «ИКС» с ролью «Администратор». Во втором, отображается значение выбранного отчета из первого окна. Предустановленные отчеты нельзя редактировать или удалить. Для добавления нового отчета необходимо нажать кнопку «Добавить» (будет открыта вкладка «Конструктор отчетов»), для удаления – «Удалить», для редактирования – «Редактировать» (будет открыта вкладка «Конструктор отчетов» с заполненными полями соответствующими выбранному отчету).

Также на данной вкладке предлагается выбрать временной интервал отображения отчета (в качестве примера текущей даты используется 01.11.19): «Сегодня» (отобразится отчет за 01.11.19), «Неделя» (отобразиться отчет 28.10.19-03.11.19), «Месяц» (отобразиться отчет 01.11.19-30.11.19), «Другой период» (необходимо указать период).

При нажатии кнопки «Экспорт», отображаемый отчет возможно экспортировать в один из следующих форматов: *.csv, *.txt, *.xls. Стоит учесть, что круговые диаграммы, при экспорте, будут преобразованы в табличный вид.

Конструктор отчетов

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить ▾ 01.11.2019 - 01.11.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

Экспорт ▾

Вид

Таблица ▾

Группировка*

По назначениям × ▾

Источник

(любой) ▾

Назначение

(любой) ▾

Интерфейс

(любой) ▾

Ip-адрес или домен

Показать

	Запросы	Трафик ▾	
Внешние диапазоны адресов	53953	▼126.64M	▲20.34M
ИКС	52829	▼93.08M	▲83.89M
Локальные сети	43091	▼11.06M	▲26.75M
Корневая группа	36431	▼7.74M	▲107.54M
Мумики	9227	▼6.54M	▲78.34M
Муми-троль	7381	▼5.29M	▲70.12M
Муми-мама	1846	▼1.24M	▲8.21M
Муми-папа	0	▼0	▲0
Муми-дол	27204	▼1.19M	▲29.19M
Туве Янссон	0	▼0	▲0
Liza	0	▼0	▲0
Снусмумрик	0	▼0	▲0
Снорки	0	▼0	▲0
Морра	0	▼0	▲0
Туве Янсон	0	▼0	▲0
DMZ сети	0	▼0	▲0

Вкладка «Конструктор отчетов». Данная вкладка позволяет создавать отчеты по заданным параметрам фильтров, которые можно применять к общей статистике в любых комбинациях для отображения необходимых статистических данных. Основное окно «Конструктора отчетов» разделено на два. В первом, задаются параметры настройки элементов фильтрации статистики, см. Таблицу:

Название	Данное поле доступно в случае редактирования ранее созданного отчета. Позволяет изменить название отчета.
Вид	Позволяет задать один из четырех возможных вариантов отображения: «Детализация HTTP», «Детализация IP», «Таблица», «Круг». «Детализация HTTP» - отобразит таблицу со статистикой по HTTP/HTTPS трафику, полученную от прокси-сервера. «Детализация IP» - отобразит таблицу со статистикой всех соединений, прошедших через «ИКС,» по IP-адресам. «Таблица» - в зависимости от настроенных элементов фильтрации статистики, отчет будет отображен в виде таблицы. «Круг» - в зависимости от настроенных элементов фильтрации статистики, отчет будет отображен в виде круговых диаграмм.
Группировка	Группирует все элементы выводимых данных по указанному принципу, во втором окне. Группировка возможна по следующим областям: по назначению, по источнику, по интерфейсу, по ip-адресам и доменам, по протоколам, по портам, по time-типам, по времени. При этом в каждой области возможно задать более мелкую группировку. Группировать выводимые данные можно по нескольким категориям при условии отображения в виде таблицы. Группировка будет производится по следующему принципу: первый уровень отображения в дереве будет сгруппирован по первому значению из данного поля; второй уровень – по второму значению; итд. Группировка является единственным обязательным параметром при составлении отчета.

Источник	Позволяет отфильтровать сгруппированную статистику по источнику их генерации. В качестве источника указывается диапазон адресов или ip-адрес, заведенный на «ИКС».
Назначение	Позволяет отфильтровать сгруппированную статистику по назначению. В качестве назначения указывается диапазон адресов или ip-адрес, заведенный на «ИКС».
Интерфейс	Позволяет отфильтровать сгруппированную статистику по интерфейсу, заведенному на «ИКС». В качестве интерфейса возможно указать: туннели, DMZ, VPN, внешние и внутренние интерфейсы.
Ip-адрес или домен	Позволяет отфильтровать сгруппированную статистику по ip-адресу или домену.
Протокол/порт	Первое поле позволяет отфильтровать сгруппированную статистику по одному из протоколов (IP, ICMP, TCP, UDP, GRE, IPIP, L2TP). Второе поле позволяет отфильтровать сгруппированную статистику по порту: используемому службой «ИКС», общепринятому или любому указанному.
Mime-тип	Позволяет отфильтровать сгруппированную статистику по одному из установленных mime-типов.
Результат	Позволяет отфильтровать сгруппированную статистику по коду ответа от стороннего веб-сервера.
Время (с...по)	Позволяет отфильтровать сгруппированную статистику относящуюся только к выбранному временному периоду, шаг указывается в часах.

После выбора всех необходимых фильтров и нажатии кнопки «Показать», во втором окне отобразится соответствующий отчет. Если отчет был выведен в виде таблицы, то предоставляется возможно управлять видимостью столбцов, порядком отображения и форматом выводимых данных как и в других таблицах графического интерфейса «ИКС». Для того, чтобы запомнить выбранный набор фильтров, чтобы не настраивать его в дальнейшем заново, необходимо нажать кнопку «Сохранить отчет». «ИКС» предложит задать категорию отчета («Общий отчет» или «Пользовательский отчет»), далее ввести имя нового отчета и сохранит его среди прочих стандартных отчетов. Созданный отчет будет доступен на вкладке «Управление отчетами».

Полученные данные, в результате фильтрации детализированной статистики, можно экспортировать в файл (.csv, .txt, .xls) для дальнейшей распечатки. При выборе одного из форматов, будет открыто новое диалоговое окно «Настройки», в котором будет предложено уточнить как экспортировать таблицу («Экспортировать все страницы», «Экспортировать в виде дерева» с выбором уровня вложенности детализации в дерево). Также на данной вкладке предлагается выбрать временной интервал отображения отчета (в качестве примера текущей даты используется 01.11.19): «Сегодня» (отобразится отчет за 01.11.19), «Неделя» (отобразится отчет 28.10.19-03.11.19), «Месяц» (отобразится отчет 01.11.19-30.11.19), «Другой период» (необходимо указать период). Стоит учесть, что круговые диаграммы, при экспорте, будут преобразованы в табличный вид.

Службы

Статистика Отвечает за сохранение целостности статистики запущен <div style="text-align: right;">Выключить</div>	Счетчики Снимают статистику с сетевых интерфейсов запущен <div style="text-align: right;">Выключить</div>
---	--

Журнал ↓↑ ↻

SquidLog: category logging enabled 11:23:08
CacheLoader: loading counter data from koldun for 1572555600 1572210000 1572555600 11:23:08
config loaded 11:23:34
SitesFeed: sessid loaded 73 skip CONNECT true 11:23:34
SquidLog: category logging enabled 11:23:34

Вкладка «Службы». На данной вкладке отображаются состояния служб «Статистика» и «Счетчики» с возможностью «Выключить» (или «Включить» если служба выключена) и последние сообщения в журнале.

Настройки

Пользователи, для которых не отображать URL

(нет) ▼

- Логировать блокировки межсетевого экрана
- Отчеты по категориям трафика

Автоматически удалять:

Логи статистики

старше 6 месяцев ▼

Квота (сейчас занято 45.41M)

(нет) ^ ▼ M6

Логи детализированной статистики

никогда ▼

Квота (сейчас занято 103.54M)

10240 ^ ▼ M6

Сохранить Обновить

Вкладка «Настройки». Данная вкладка предназначена для определения параметры

отображения и хранения журналов вышеописанных служб и записей статистики.

В поле «Пользователи, для которых не отображать URL» возможно задать Пользователей и/или группы Пользователей, для которых не будет отображаться URL посещенных ресурсов при формировании отчета. В отчете будет отображаться «hidden.url», в который будут попадать все URL. Стоит отметить, что данное отображение будет работать только с момента его применения.

Если установлен флаг «Логировать блокировки межсетевого экрана», то в отчетах кроме обычных запросов также будут отображаться блокировки произведенные межсетевым экраном. Для их отображения возможно во вкладке «Конструктор отчетов» задать: в поле вид - «Детализация IP», в поле результат - «403 Forbidden».

Если установлен флаг «Отчеты по категориям трафика», то при формировании отчета, у которого вид указан как «Детализация HTTP», в отчете будет указана категория к которой относится соответствующий URL.

Блок «Автоматически удалять:» позволяет установить временные рамки или квоту на хранение данных статистики и детализированной статистики, также данные рамки настраиваются в Меню - «Система» - «Удаление данных».

Журнал

Управление отчетами Конструктор отчетов Службы Настройки **Журнал**

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ↻

↑ Экспорт Удалить логи Поиск...

config loaded 31.10.2019 23:03:08
SitesFeed: sessid loaded 11 skip CONNECT true 31.10.2019 23:03:08
SquidLog: category logging enabled 31.10.2019 23:03:08
CacheLoader: loading counter data from koldun for 1572469200 1572210000 1569877200 31.10.2019 23:03:08
config loaded 31.10.2019 23:03:10
SitesFeed: sessid loaded 11 skip CONNECT true 31.10.2019 23:03:10

Вкладка «Журнал». Данная вкладка 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:stat_setup

Last update: **2019/11/10 19:25**



Просмотр объема трафика за определенный период

Чтобы вывести суммарное значение выбранного трафика без использования стандартных отчетов за выбранный период времени, перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Мульти-дол > Управление отчетами > Конструктор отчетов Туге Янссон 12

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 01.11.2019 - 01.11.2019 **Сегодня** Неделя Месяц Другой период Экспорт

Вид: Таблица

Группировка: По источникам

Источник: (любой)

Назначение: Внешние диапазоны адресов

Интерфейс: (любой) **Показать**

	Запросы	Трафик	
ИКС	24274	↓73.92M	↑13.95M
Корневая группа	4022	↓37.00M	↑2.33M
Локальные сети	2601	↓9.68M	↑548.59K
Внешние диапазоны адресов	20246	↓2.68M	↑2.68M
DMZ сети	0	↓0	↑0
Пользовательские диапазоны адресов	0	↓0	↑0
Всего	51143	↓123.30M	↑19.51M

В поле «Группировка» выберите - «По источникам».

В поле «Назначение» выберите - «Внешние диапазоны адресов».

В полях «Дата» укажите начальную и конечную дату периода времени, за который вас интересует статистика пользователей.

Нажмите кнопку «Показать».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:1time_statistics

Last update: **2019/11/10 19:25**



Просмотр объема трафика по часам

Чтобы вывести статистику пользователя по часам, перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Муми-дол > Управление отчетами > Конструктор отчетов Туге Янссон 12

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период Экспорт

Вид	Запросы	Трафик
Таблица		
Группировка: По часам		
Источник: Хемуль		
Назначение: Внешние диапазоны адресов		
Интерфейс		
Показать		
01.11.2019 08:00	0	0
01.11.2019 09:00	186	1.83M / 79.75K
01.11.2019 10:00	0	0
01.11.2019 11:00	0	0
01.11.2019 12:00	195	549.18K / 55.50K
01.11.2019 13:00	0	0
01.11.2019 14:00	0	0
01.11.2019 15:00	0	0
01.11.2019 16:00	0	0
01.11.2019 17:00	0	0
01.11.2019 18:00	0	0
01.11.2019 19:00	0	0
01.11.2019 20:00	0	0
01.11.2019 21:00	0	0
01.11.2019 22:00	0	0
01.11.2019 23:00	0	0

В поле «Группировка» укажите - «По часам».

В поле «Источник» выберите интересующего вас пользователя или группу.

В поле «Назначение» укажите - «Внешние диапазоны адресов».

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:2time_statistics

Last update: **2019/11/10 19:25**



Просмотр списка запросов пользователей на ip-адреса и домены

Чтобы вывести список запросов пользователей на ip-адреса и домены, посещенных пользователем или группой пользователей, перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Вид	Запросы	Трафик
Таблица		
Группировка: По ip-адресам и доменам		
Источник: Муми-троль		
Назначение: HTTP		
Интерфейс: Показать		
gvt1.com	4	↓4.53M ↑751
userapi.com	413	↓4.25M ↑80.78K
vkuservideo.net	23	↓1.51M ↑7.18K
vcdn.biz	59	↓1.51M ↑7.91K
yandex.ru	280	↓1.50M ↑584.22K
taboola.com	107	↓849.34K ↑101.67K
htmlbook.ru	72	↓641.58K ↑25.39K
google.ru	95	↓626.98K ↑66.75K
serving-sys.com	51	↓547.35K ↑35.94K
googlesyndication.com	37	↓493.78K ↑21.78K
bitrix24.ru	157	↓493.14K ↑80.65K
yandex.net	62	↓480.12K ↑21.97K
openh264.org	1	↓442.89K ↑423
googleapis.com	15	↓376.23K ↑6.82K

В поле «Группировка» укажите - «По ip-адресам и доменам».

В поле «Источник» выберите интересующего вас пользователя или группу.

В поле «Назначение» укажите - «Внешние диапазоны адресов» → «Интернет» → HTTP.

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:1site_statistics

Last update: **2019/11/10 19:25**



Просмотр запросов пользователей на определенный IP-адрес или домен

Чтобы вывести список обращений пользователей к определенному ip-адресу или домену, перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Муми-дол > Управление отчетами > Конструктор отчетов Тыве Янссон 12

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 01.11.2019 - 01.11.2019 **Сегодня** Неделя Месяц Другой период Экспорт

Источник: Корневая группа

Назначение: Внешние диапазоны адресов

Интерфейс: (любой)

IP-адрес или домен: vk.com

Протокол: (любой)

Показать

	Запросы	Трафик	
Корневая группа	420	↓10.17M	↑293.97K
Мумики	394	↓10.16M	↑291.58K
Муми-троль	323	↓7.77M	↑228.70K
Муми-мама	71	↓2.38M	↑62.87K
Муми-папа	0	↓0	↑0
Муми-дол	26	↓6.43K	↑2.39K
Тыве Янссон	0	↓0	↑0
Снусмумрик	0	↓0	↑0
Снорки	0	↓0	↑0
Морра	0	↓0	↑0
Тыве Янсон	0	↓0	↑0
Всего	420	↓10.17M	↑293.97K

В поле «Группировка» укажите - «По источникам».

В поле «Источник» выберите «Корневая группа» .

В поле «Назначение» укажите «Внешние диапазоны адресов»

В поле «IP-адрес или домен» укажите доменное имя сайта или его ip-адрес.

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

Просмотр запросов пользователей на определенный IP-адрес или домен по времени

Чтобы вывести список посещений сайта, сделайте следующее:

В поле «Группировка» укажите - «По часам/дням/месяцам».

В поле «Источник» выберите интересующего вас пользователя или группу.

В поле «Назначение» укажите «Внешние диапазоны адресов»

В поле «IP-адрес или домен» укажите доменное имя сайта или его ip-адрес.

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

Муми-дол > Управление отчетами > Конструктор отчетов Туге Янссон 12

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 28.10.2019 - 03.11.2019 Сегодня Неделя Месяц Другой период Экспорт

Вид: Таблица

Группировка: По дням

Источник: Корневая группа

Назначение: Внешние диапазоны адресов

Интерфейс: (любой)

Показать

	Запросы	Трафик	
31.10.2019	3588	+42.80M	▲2.52M
01.11.2019	4250	+37.55M	▲2.40M
28.10.2019	0	+0	▲0
29.10.2019	0	+0	▲0
30.10.2019	0	+0	▲0
02.11.2019	0	+0	▲0
03.11.2019	0	+0	▲0
Всего	7838	+80.36M	▲4.92M

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:2site_statistics

Last update: **2019/11/10 19:25**



Просмотр статистики по портам

Чтобы вывести список запросов по портам перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Муми-дол > Управление отчетами > Конструктор отчетов Тыве Янссон 12

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 28.10.2019 - 03.11.2019 Сегодня Неделя Месяц Другой период Экспорт

Вид: Таблица

Группировка: По портам

Источник: Корневая группа

Назначение: Внешние диапазоны адресов

Интерфейс: Показать

	Запросы	Трафик	
● 443	7548	▼76.50M	▲4.78M
● 80	174	▼3.66M	▲69.78K
Всего	7816	▼80.19M	▲4.88M

В поле «Группировка» укажите - «По портам».

В поле «Источник» выберите интересующего вас пользователя или группу.

В поле «Назначение» укажите - «Внешние диапазоны адресов».

В поле «Протокол/порт» укажите - протокол и порт.

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:port_statistics

Last update: **2019/11/10 19:25**



Просмотр детализированной статистики

Чтобы вывести детализированный список обращений пользователя к доменам, перейдите во вкладку «Конструктор отчетов» модуля «Управление отчетами».

Время	URL	Категория трафика	Трафик
09:31:22	https://snippets.cdn.mozilla.net:443		↕0 ↗0
09:31:22	https://snippets.cdn.mozilla.net:443		↕0 ↗0
09:31:18	https://client.wns.windows.com:443		↕0 ↗0
09:31:23	https://snippets.cdn.mozilla.net/us-west/...	Бизнес, экономика, маркетинг	↕8.23K ↗424
09:31:23	https://snippets.cdn.mozilla.net:443		↕0 ↗0
09:31:23	https://snippets.cdn.mozilla.net:443		↕0 ↗0
09:31:26	https://client.wns.windows.com:443		↕0 ↗0
09:31:27	https://cdn.bitrix24.ru:443		↕0 ↗0
09:31:27	https://ics5areal.bitrix24.ru:443		↕0 ↗0
09:31:27	https://ics5areal.bitrix24.ru:443		↕0 ↗0
09:31:27	https://ics5areal.bitrix24.ru:443		↕0 ↗0
09:31:27	https://bitrix2.cdnvideo.ru:443		↕0 ↗0
09:31:27	https://tiles.services.mozilla.com:443		↕0 ↗0
09:31:27	https://ics5areal.bitrix24.ru/stream/?	Компьютеры и Интернет	↕1.35K ↗657

В поле «Вид» выберите «Детализация HTTP».

В поле «Источник» выберите интересующего вас пользователя или группу.

В поле «Назначение» укажите «Внешние диапазоны адресов».

В поле «Дата» укажите интересующий период времени.

Нажмите кнопку «Показать».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:detailed_statistics

Last update: **2019/11/10 19:25**



Сервер авторизации (xauth)

Модуль «Сервер авторизации (Xauth)» расположен в Меню «Пользователи и статистика».

Данный модуль отвечает за сервер авторизации Пользователей Xauth, по средствам которого Пользователи могут быть авторизованы на «ИКС» через утилиту авторизации Xauth.

Данный модуль содержит три вкладки:

1. Сервер авторизации
2. Настройки
3. Журнал

Сервер авторизации

На вкладке **Сервер авторизации** отображаются:

- статус сервера (запущен/выключен);
- кнопка «Включить» / «Выключить». Позволяет запустить и остановить сервер авторизации соответственно. По умолчанию сервер авторизации запущен;
- журнал событий за текущую дату.

ООО "Организация" > Сервер авторизации Администратор

Сервер авторизации | Настройки | Журнал

Сервер авторизации
Отвечает за авторизацию пользователей запущен
Выключить

Журнал ↓ ↑ ↻

- User User2 autologged from 192.168.17.19
13:30:49
- [uid: 0] TLS is started
13:30:49
- [uid: 0] new connection from 192.168.17.19
13:30:49
- config loaded
13:30:07
- Listening on 0.0.0.0:4888
13:30:01
- config loaded
13:30:01
- locale loaded
13:30:01
- started
13:30:01

Настройки

На вкладке **Настройки** представлен выбор «Автоматически создавать разрешающее правило». Если флаг установлен, то в разрешающих правилах [межсетевого экрана](#) будет добавлено правило «Доступ для программы авторизации» (Направление – Входящие на ИКС; Источник – Локальные сети, DMZ сети; Назначение – self; Протокол – TCP; Порт назначения – Порт программы авторизации; Интерфейс – Внутренние интерфейсы, VPN-интерфейсы, DMZ). Если флаг не установлен, то данное правило будет удалено из разрешающих правил межсетевого экрана.

Автоматически создавать разрешающее правило

Доступ для программы авторизации

Сохранить

Обновить

Журнал

На вкладке **Журнал** отображается сводка 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. 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».

09.09.2019 - 09.09.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 Экспорт Удалить логи

Поиск... 

↓↑
User User2 autologged from 192.168.17.19 15:30:46
[uid: 0] TLS is started 15:30:46
[uid: 0] new connection from 192.168.17.19 15:30:46
config loaded 15:30:07
Listening on 0.0.0.0:4888 15:30:01
config loaded 15:30:01
locale loaded 15:30:01
started 15:30:01
exiting 15:29:59

« < Стр 1 из 1 > »

Показаны записи 1 - 9 из 9

From:
<https://doc.a-real.ru/> - **Документация**

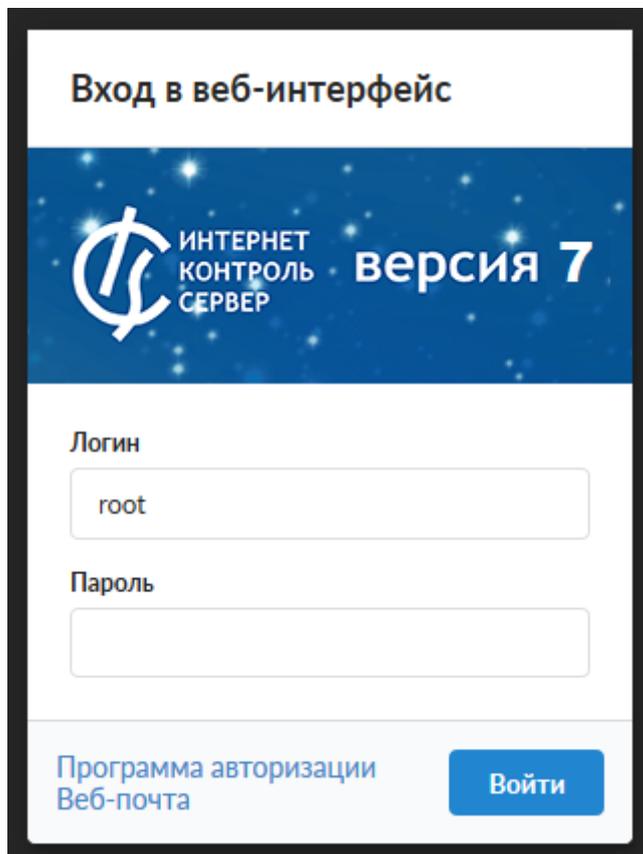
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:xauth>

Last update: **2019/11/21 16:11**

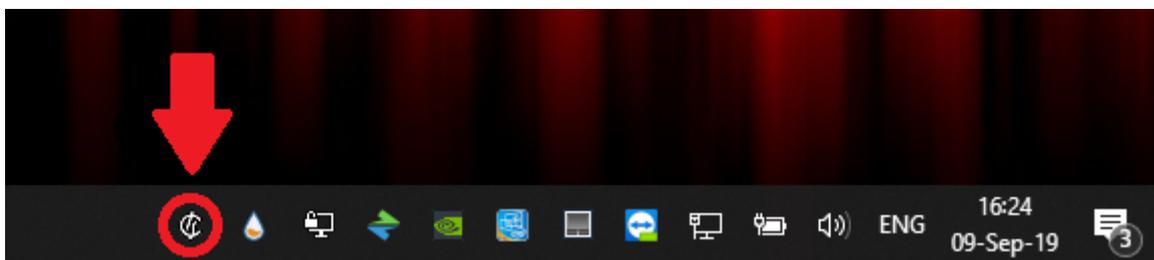


Утилита авторизации Xauth

Утилита авторизации Xauth (далее «клиент Xauth») предназначена для авторизации пользователей на ИКС. Скачать утилиту можно кликнув по ссылке «Программа авторизации» на странице входа в веб-интерфейс ИКС.

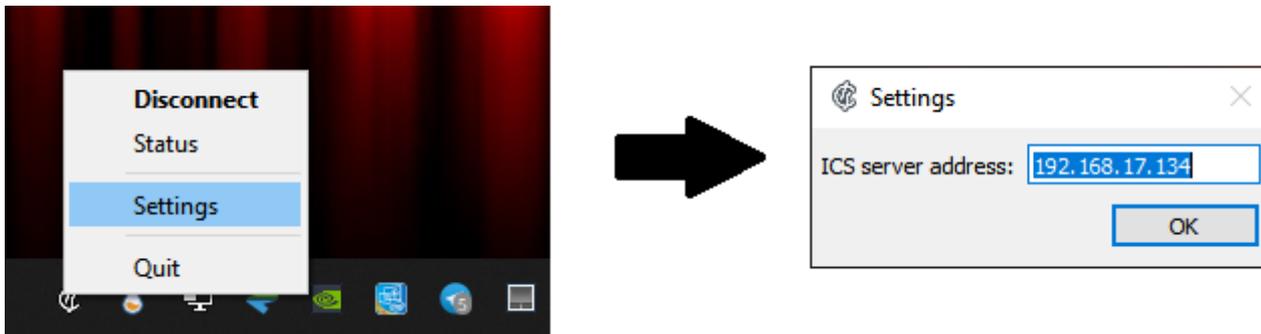


После скачивания клиент Xauth можно запускать. Установки утилита не требует и поставляется непосредственно в виде исполняемого файла. После запуска при загрузке на короткое время появится логотип ИКС, после этого программа продолжит работу в минимизированном виде в трее.



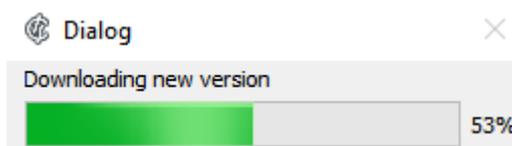
Подключение к серверу авторизации

Для подключения к серверу авторизации клиент Xauth по умолчанию попытается использовать маршрут до шлюза по умолчанию. Изменить адрес сервера авторизации можно кликнув правой кнопкой мыши по иконке клиента Xauth и выбрав меню настройки (settings) изменить адрес в строке ввода на необходимый. Затем необходимо переподключиться к новому серверу нажав «Отключиться» (Disconnect) и «Подключиться» (Connect) в том же меню.



Обновление клиента Xauth

При подключении к серверу клиент Xauth проверит наличие обновлений для себя. Если таковых не обнаружится, то программа продолжит работу. В противном случае автоматически запустится процесс загрузки новой версии. Обычно этот процесс не занимает много времени и зависит от скорости подключения к серверу. Во время процесса скачивания появляется полоса прогресса, которая отображается текущий процент загруженных данных.



После загрузки программа автоматически завершится, осуществит обновление и снова включится. Следует обратить внимание, что вновь запущенная программа будет использовать шлюз по умолчанию для подключения, таким образом, если адрес сервера авторизации был изменен, операцию по изменению адреса необходимо повторить.

Авторизация пользователя

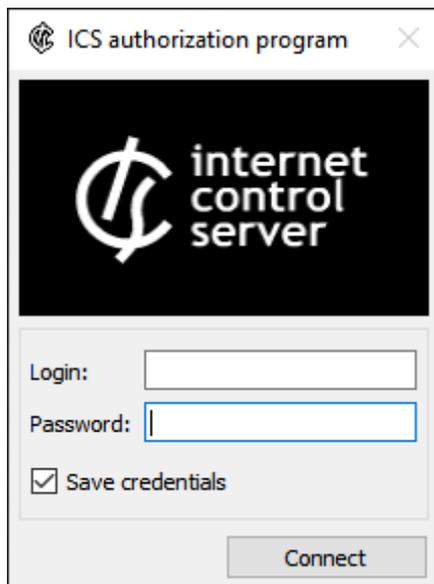
Клиент Xauth позволяет провести авторизацию тремя способами:

- По IP-адресу устройства на котором запущен клиент Xauth
- С использованием доменной авторизации
- По логину и паролю пользователя

В первую очередь происходит попытка авторизации по IP-адресу. Авторизация по IP-адресу используется, если в ИКС существует пользователь, которому назначен IP-адрес машины на которой запущен клиент Xauth.

В случае если авторизация по IP-адресу не была осуществлена, то происходит попытка авторизации через домен. Для данного типа авторизации должен быть настроен домен.

Если оба вышеперечисленных способа не были осуществлены, то пользователю будет предложено ввести логин и пароль для авторизации, которые назначены ему при создании в ИКС.



Ключи запуска клиента Xauth

Клиент Xauth может быть запущен без каких-либо дополнительных параметров, в таком случае поведение программы будет совпадать с описанным выше. Однако в некоторых ситуациях может требоваться иное поведение программы, например при автоматическом и/или удаленном запуске. В таких случаях утилиту можно запускать с одним или несколькими следующими ключами:

- **--server** [server ip]: ключ для задания сервера авторизации по умолчанию;
- **--noauto** : отключение авторизации по IP-адресу (см. пункт «Авторизация пользователя»);
- **--nodomain** : отключение авторизации через домен (см. пункт «Авторизация пользователя»);
- **--nomanual** : отключение авторизации по логину и паролю (см. пункт «Авторизация пользователя»);
- **--nosave** : не сохранять данные, введенные на форме авторизации через логин и пароль;
- **--logs** [NONE, DEBUG, INFO]: уровень логирования, если уровень логирования отличается от NONE (по умолчанию), то создается папка logs в той же директории, что и исполняемый файл и туда помещаются логи работы утилиты;
- **--noclose**: не отключать утилиту авторизации при блокировании ОС и/или смене пользователя (добавлено в версии 7.0.1).

Мониторинг соединений

Служба мониторинга соединений предназначена для постоянного слежения за состоянием соединений, осуществляемых конечным устройством с установленным клиентом Xauth.

Со стороны клиента, в общем случае, не требуется выполнять каких-либо настроек для работы данной службы. Однако существует несколько ключей запуска клиента Xauth, которые влияют на ее работу:

- **--nomonitor** : отключает мониторинг соединений на клиенте;
- **--delay** [delay]: регулировка времени между сканированиями соединений в миллисекундах, значение по умолчанию - 1000 (1 сек.).

Web-интерфейс мониторинга соединений

Данные мониторинга соединений можно просматривать через интерфейс ИКС, для этого необходимо перейти в меню Пользователи и Статистика → Пользователи, выбрать пользователя на машине которого запущен клиент Xauth и перейти во вкладку «Приложения».

ООО "Организация" > Пользователи > TestUser1 > Приложения
Администратор 1

Запретить доступ
🔍 Поиск...
↻

Приложения и процессы	Соединения	Протокол	ID родительского процесса
🔧 NVIDIA Web Helper.exe			
🔧 NetDrive2.exe			
🔧 System			
🔧 TeamViewer_Service.exe			
🔧 Telegram.exe			
🔧 Не определен			
🔧 Video.UI.exe			
9752	192.168.17.19:62311 → 95.100.188.12:443	TCP	616
🔧 [System Process]			
🔧 dasHost.exe			
🔧 firefox.exe			
🔧 nvcontainer.exe			
🔧 svchost.exe			
🔧 xauth.exe			
14704	192.168.17.19:50830 → 192.168.17.134:...	TCP	9244

На данной странице соединения сгруппированы по приложениям, которые эти соединения установили.

Можно посмотреть:

- приложение, установившее соединение
- PID процесса
- основную информацию о соединении (IP-адреса, порты, протокол)
- PID родительского процесса

Также на данной странице можно заблокировать соединения, установленные приложением. Блокаровка осуществляется средствами службы Application Firewall.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:xauth_client

Last update: **2019/12/02 14:30**



Captive Portal

Данная страница актуальна для версии ИКС 6 и выше!

Модуль «Captive Portal» расположен в Меню «Пользователи и статистика». Данный модуль предоставляет возможность авторизации Пользователей на «ИКС» для доступа к сети Интернет, а также объединяет в себе настройку и функциональность двух серверов: SMS-авторизации и веб-авторизации. Все TCP запросы на порты 80 и 443 от всех неизвестных Пользователей перехватывает фаервол и перенаправляет в модуль captive portal. Не авторизованному Пользователю выдаётся окно авторизации в браузере, стоит отметить, что не все браузеры способны автоматически выдать окно авторизации captive portal. В данном случае, Пользователь должен обратиться на: <IP_ICS>:81/portal/. Данный модуль содержит пять вкладок: «Captive Portal», «Настройки», «Активные сессии», «Заблокированные номера», «Журнал».

Captive Portal Настройки Активные сессии Заблокированные номера Журнал

 **Captive portal** запущен
Отвечает за авторизацию пользователей через веб страницу Выключить

Журнал ↓↑ ↻

started
17:13:45
locale loaded
17:13:46
config loaded
17:13:46
[http]: is listening on 127.0.0.1:60180
17:13:46
[https]: is listening on 127.0.0.1:60181
17:13:46

Примечание. Для удобства, вместо обращения <IP_ICS>:81/portal/ на «ИКС» возможно создать [виртуальный хост с перенаправлением](#). Таким образом Пользователь будет обращаться на локально созданное доменное имя, но попадать на <IP_ICS>:81/portal/.

Примечание. Перенаправление на Captive Portal из DMZ сетей работать не будет.

На вкладке «Captive Portal» представлены: статус сервера авторизации (запущен/выключен/не настроен), кнопка «Включить» / «Выключить» и журнал событий за текущую дату.

Настройки

На вкладке «Настройки» представлена возможность выбрать режим работы Captive Portal, только в качестве сервера Web-авторизации (флаг «Авторизация по логину/паролю»), только в

качестве сервера SMS-авторизации (флаг «SMS-авторизация») или совместная работа в качестве двух серверов.

Сертификат	Время жизни сессии *
 Captive ✕	24   ч.

Для корректного перенаправления на страницу авторизации, при обращении Пользователя к https ресурсам, необходимо в поле «Сертификат» установить соответствующий конечный [сертификат](#), а также использовать [прозрачный прокси](#).

Каждый авторизованный Пользователь в Captive Portal сохраняется как сессия на основе MAC-адреса Пользователя. Идентификация по MAC-адресу используется вместо идентификации по ip-адресу, чтобы избежать случаев с подменой ip-адреса или случаев, когда ip-адрес ещё не истёкшей сессии выдаётся другому Пользователю по DHCP. Каждая сессия имеет время жизни, по истечении которого Пользователь автоматически разлогинивается. Также Captive Portal каждую 1 минуту проверяет ARP кэш операционной системы. Если MAC-адрес авторизованного Пользователя отсутствует в кэше, то Captive Portal считает, что Пользователь неактивен и автоматически разлогинивает его. Если MAC-адресу был присвоен другой IP-адрес, то служба Captive Portal обновляет у сессии IP-адрес, при этом сессия не закрывается.

Авторизация по логину/паролю

- Авторизация по логину/паролю
- Запретить множественную авторизацию с одним логином

Если установлен флаг «Авторизация по логину/паролю», то это означает, что в модуле «Captive Portal» 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 «ИКС».

SMS-авторизация

SMS-авторизация

Назначать адреса пользователю *

Администратор ✕

Время действия кода, отправленного в SMS *

180 сек.

Интервал между повторными попытками отправки SMS *

5 сек.

Максимальное число попыток повторной отправки SMS для одного номера *

3

Текст SMS

Код проверки {code}

Если установлен флаг «SMS-авторизация», то Пользователи будут проходить авторизацию через SMS.

Поле «Назначать адреса пользователю» является обязательным и требует выбора одного из Пользователей, заведенных на «ИКС». Данному Пользователю, для каждой новой сессии, будут выдаваться динамические IP-адреса. Поле «Время действия кода, отправленного в SMS» позволяет задать 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 в данном поле установлено 180 секунд. Поле «Интервал между повторными попытками отправки SMS» позволяет задать время блокировки кнопки «Отправить СМС повторно» (см. ниже) для Пользователя при SMS-авторизации. Значение, задаваемое в данном поле, не должно превышать время действия кода, отправленного в SMS. Поле «Максимальное число попыток повторной отправки SMS для одного номера» позволяет задать число попыток повторной отправки SMS-сообщений, 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-сообщений, то ему будет доступна возможность сменить абонентский номер для отправки SMS. При смене абонентского номера число попыток обнулится. Поле «Текст SMS» - содержит текст отправляемого сообщения Пользователю при авторизации. Данное сообщение обязательно должно содержать шаблон - {code}. Вместо этого шаблона SMS-сервер вставит четырехзначное число.

Параметры SMPP:**SMPP-сервер ***

smpp.local

Порт *

2775

Логин/system_id *

mylogin

Пароль *

●●●●●●●●●●

source-addr-ton *

5

source-addr-npi *

1

dest-addr-ton *

1

dest-addr-npi *

1

Блок «Параметры SMPP». SMPP (Short Message Peer-to-Peer) – это протокол, используемый в «ИКС» для передачи SMS-сообщений, являющийся универсальным и наиболее широко используемым протоколом при передаче SMS-сообщений между SMSC (Short Message Service Centers) и SMS application systems. Большинство сервисов, предоставляющих возможность отправки SMS-сообщений, поддерживают SMPP-протокол при передаче коротких сообщений. Для настройки подключения необходимо заполнить обязательные поля: «SMPP-сервер», «Порт», «Логин/system_id» и «Пароль».

Значения дополнительных параметров подключения «source-addr-ton», «source-addr-npi», «dest-addr-ton», «dest-addr-npi» должны быть в документации к подключаемому серверу SMPP. В большинстве случаев они такие:

source-addr-ton	5	source-addr-npi	1
dest-addr-ton	1	dest-addr-npi	1

Для проверки правильности введенных настроек, возможно воспользоваться функцией тестовой отправки. Для этого необходимо нажать «Проверка отправки SMS». Будет открыто новое диалоговое окно, в котором необходимо ввести номер телефона и текст сообщения. Поле «Номер телефона» является обязательным, вводимые номера должны иметь следующий формат - <код страны или выход на зонную/междугороднюю нумерацию> <десятизначный номер абонента в операторской сети>. Все вводимые номера должны содержать только цифры (не менее одиннадцати), без скобок и дефисов (например, +79991112233 или 85554447799). Поле «Текст SMS» является не обязательным и позволяет ввести и отправить любой текст. Если сообщение было успешно отправлено, то будет показано соответствующее сообщение, иначе отображена ошибка отправки с ее кодом. **Важно: Отправка тестового sms-сообщения будет произведена с использованием сохраненных настроек и при включенной службе «Captive Portal».**

Изменение логотипа

Также на данной вкладке возможно изменить приветственный логотип для SMS-авторизации и авторизации по логину/паролю. Для этого необходимо нажать «Изменить логотип». Будет

открыто новое диалоговое окно, в котором отобразятся: текущий логотип (по умолчанию - это логотип «ИКС»); кнопка «Загрузить .png», для загрузки нового логотипа в формате png (рекомендуемый размер загружаемого логотипа 316*118 пикселей); кнопка «Восстановить по умолчанию», позволяет вернуть логотип «ИКС»; кнопка «Закрыть», закрывает текущее диалоговое окно.

Для Пользователя, при SMS-авторизации, в браузере будет открыто окно: с установленным логотипом, с полем куда необходимо ввести свой абонентский номер, в формате обозначенном выше, и кнопка «Получить СМС с кодом». При введении номера в указанном формате и нажатии на кнопку «Получить СМС с кодом», Пользователю будет отправлено SMS-сообщение с кодом, полученный код необходимо ввести в поле «Введите код из СМС». При введении правильного кода, Пользователю будет выдан динамический IP, а сам Пользователь авторизован на «ИКС» и получит доступ к сети Интернет. Если Пользователь не смог ввести код за отведенное время, то он может запросить код повторно нажав на кнопку «Отправить СМС повторно» или изменить абонентский номер, нажав на кнопку «Изменить номер».

IP-адреса Пользователей

Ip-адрес	Пользователь
 192.168.17.62 Динамический ip-адрес (веб-авторизация)  Администратор Mac-адрес: d8:cb:8a:7d:0b:4a Будет отключен через 23 часа 59 минут 43 секунды	

На вкладке «Активные сессии» отображаются текущие сеансы Пользователей авторизованных через Captive Portal с присвоенными им динамическими ip-адресами в «ИКС».

На вкладке «Заблокированные номера» отображаются номера абонентов, которые исчерпали все попытки ввода кода. Блокировка, на данные номера, устанавливается на время жизни сессии. Блокировка может быть принудительно снята Пользователем «ИКС», имеющим административные права.

Журнал

01.11.2019 - 01.11.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи 🔍

started 17:13:45
locale loaded 17:13:46
config loaded 17:13:46
[http]: is listening on 127.0.0.1:60180 17:13:46
[https]: is listening on 127.0.0.1:60181 17:13:46
[webauth]: auth [ip: 192.168.17.62, mac: d8:cb:8a:7d:0b:4a, user: Администратор] successfull 17:30:59

На вкладке «Журнал» отображается сводка всех системных сообщений соответствующих серверов 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 журнала 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:captive_portal

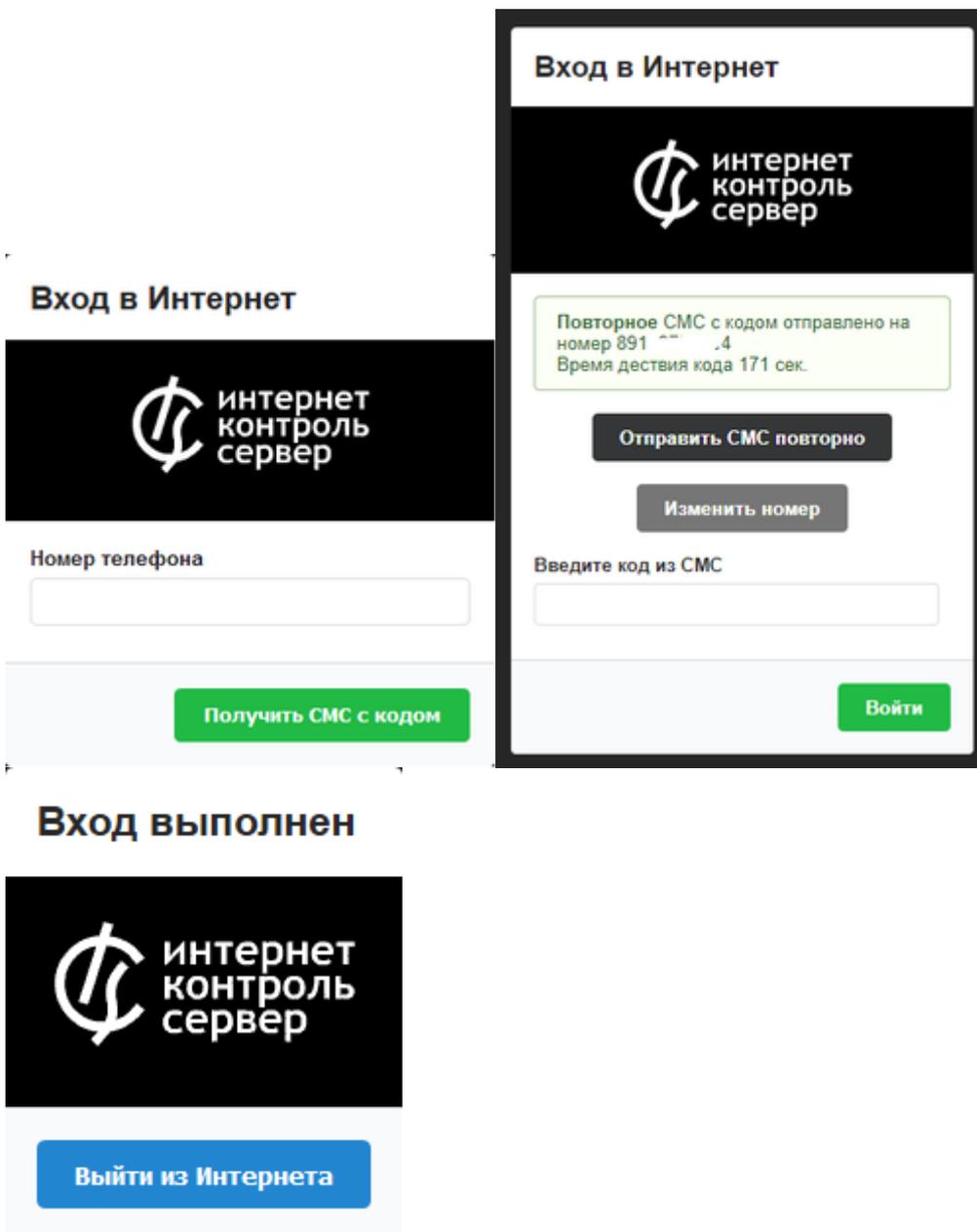
Last update: **2019/11/10 19:25**



Настройка SMS-авторизации

Принцип работы

- Пользователь подключается к точке WiFi
- Пользователь заходит в браузер, затем вводит свой номер телефона и нажимает кнопку Получить СМС с кодом
- На указанный номер телефона приходит СМС с кодом
- Полученный код пользователь вводит в форму авторизации и получает доступ к сети Интернет



Основные возможности

- Отправка смс по протоколу SMPP
- Возможность указания произвольного интервала времени действия кода в смс-сообщении
- Возможность указания произвольного текста в смс-сообщении с кодом
- Возможность вставки своего логотипа

Важно:выданный пользователю IP-адрес удаляется через 3 часа неактивности.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:sms_auth

Last update: **2019/11/10 19:25**



Синхронизация

Модуль «Синхронизация» расположен в Меню «Пользователи и статистика». Данный модуль предназначен для управления и настройки службы синхронизации «ИКС». Модуль имеет три вкладки: «Служба синхронизации пользователей», «Настройки» и «Журнал».

Служба

Муми-дол > Служба синхронизации пользователей Туге Янссон 60

Служба синхронизации пользователей Настройки Журнал

Служба синхронизации пользователей запущен
Позволяет синхронизировать импортированных из домена пользователей Выключить

Журнал ↓↑ ↻

no actions 23:29:43
done 23:29:43
no actions 23:29:53
done 23:29:53
no actions 23:30:04

На вкладке «Служба синхронизации пользователей» представлен статус службы (запущен/выключен/не настроен), кнопки «Включить» / «Выключить» и журнал событий за текущую дату.

Настройки

Служба синхронизации пользователей **Настройки** Журнал

Контроллер домена *

Домен * LDAP-группа

 Secure LDAP
Сертификат *

Вкладка «Настройки» синхронизируется с формой импорта из LDAP/AD. При заполнении настроек, обязательными полями являются: «Контроллер домена» - указывается IP-адрес, «Домен» - указывается имя домена, «Логин» и «Пароль». При корректном заполнении всех необходимых полей и нажатии кнопки «Сохранить», служба синхронизации будет запущена, в ином случае настройки не будут сохранены.

В случае необходимости установки шифрованного канала между LDAP-сервером и «ИКС» необходимо установить флаг «Secure LDAP» и выбрать сертификат из модуля сертификатов «ИКС». Стоит отметить, что данный сертификат должен быть установлен на LDAP-сервере. При создании сертификата на «ИКС» стоит выбрать в поле «Тип сертификата» - «Конечный сертификат», а в поле «Шаблон» - «Сервер».

Логин * Пароль *

Пропускать пустые группы при синхронизации

Частота обновлений (мс)

Журнал

Служба синхронизации пользователей Настройки **Журнал**

28.10.2019 - 03.11.2019 Сегодня **Неделя** Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

started 31.10.2019 23:28:45
locale loaded 31.10.2019 23:28:45
config loaded 31.10.2019 23:28:45
No users to sync 31.10.2019 23:28:45
config loaded

На вкладке «Журнал» отображается сводка всех системных сообщений модуля «Синхронизация» 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 журнала 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». Также данный журнал отображается в Меню - «Обслуживание» - «Журнал и уведомления» - вкладка «Системный журнал», для отображения журнала необходимо выбрать «Служба синхронизации пользователей».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:ldapsync>

Last update: **2019/11/10 19:25**



Первичная настройка системы

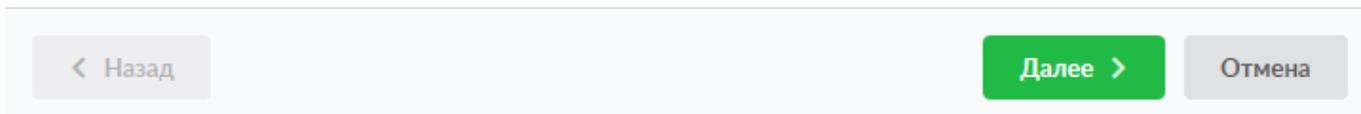
Мастер первоначальной настройки системы

После первого [входа в веб-интерфейс](#) необходимо настроить основные параметры и сетевые интерфейсы сервера. Сделать это можно с помощью мастера начальной настройки системы. Он запускается автоматически при первом входе в веб-интерфейс.

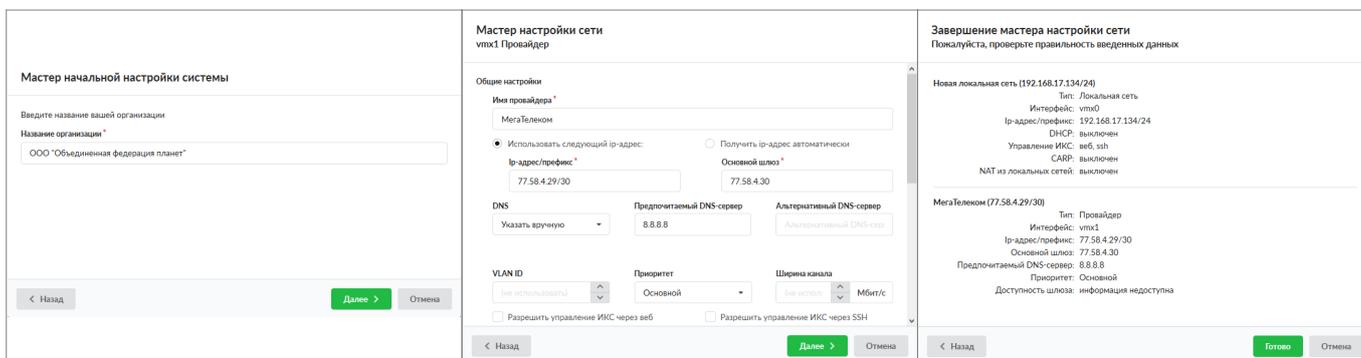
Мастер начальной настройки системы

Мастер начальной настройки системы

Помогает настроить ИКС для вашей организации



Мастер представляет собой пошаговую настройку системы. Он запросит ввести название организации, имя хоста и логин/пароль администратора.



После прохождения всех шагов завершите работу мастера нажатием кнопки «Готово».

Мастер настройки сети

При первом входе в веб-интерфейс модуль «Межсетевой экран» имеет статус «не настроен». Первичная настройка считается завершенной, когда модуль «Межсетевой экран» приобретет статус «запущен». Для этого необходимо, чтобы в модуле «Провайдеры и сети» был создан как минимум один сетевой интерфейс класса «Провайдер» и один класса «Локальная сеть». Для этой цели после прохождения мастера первоначальной настройки системы рекомендуется сразу запустить мастер настройки сети для конфигурации сетевых интерфейсов.

Типы сетевых интерфейсов

На первом шаге мастера, отображаются все сетевые интерфейсы типа Ethernet, обнаруженные в системе. Для каждого из них необходимо указать тип.

Мастер настройки сети

Пожалуйста, укажите, какие интерфейсы необходимо настроить

The screenshot shows a web-based configuration wizard for network interfaces. It contains two sections, one for interface 'vmx0' and one for 'vmx1'. Each section displays the interface name, its status (e.g., 'кабель подключен'), and its MAC and IP addresses. Below this information is a list of radio button options for selecting the interface type: 'Не использовать', 'Локальная сеть', 'DMZ сеть', 'Провайдер', 'Провайдер PPPoE', 'Провайдер PPTP поверх IP/DHCP', and 'Провайдер L2TP поверх IP/DHCP'. At the bottom of the wizard, there is a refresh button, a green 'Далее >' button, and a grey 'Отмена' button.

Возможные типы:

тип	описание
не использовать	интерфейс не будет использоваться

тип	описание
локальная сеть	внутренний интерфейс сервера. В этой сети будут находиться пользователи.
локальная сеть VLAN	работает аналогично обычной локальной сети, только при этом используется технология VLAN. Позволяет создать несколько виртуальных локальных сетей на одном физическом интерфейсе
провайдер	внешний интерфейс сервера со статически сконфигурированным ip-адресом.
провайдер PPPoE	внешний интерфейс сервера, подключающийся к провайдеру по протоколу PPPoE.
провайдер DHCP	внешний интерфейс сервера с динамическим ip-адресом, получаемым от DHCP-сервера провайдера.
провайдер VLAN	внешний интерфейс сервера со статически сконфигурированным ip-адресом и ID vlan-подсети, в которую он включен.
DMZ сеть	внутренний интерфейс сервера. 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 PPTP поверх IP	внешний интерфейс сервера, подключающийся к провайдеру по протоколу PPTP со статически сконфигурированным ip-адресом в «серой» сети провайдера.
Провайдер PPTP поверх DHCP	внешний интерфейс сервера, подключающийся к провайдеру по протоколу PPTP с динамическим ip-адресом «серой» сети провайдера, получаемым от DHCP-сервера провайдера.
DMZ сеть VLAN	внутренний интерфейс сервера. Аналогична DMZ сети, за исключением параметра VLAN ID

Важно: такие провайдеры, как 3G и WiFi требуется настраивать отдельно, поскольку они не выводятся в общем списке интерфейсов мастера.

В нашем примере, интерфейс le0 остаётся локальной сетью, а на интерфейсе le1 будет настроен простой провайдер.

Настройка локальной сети

На следующем этапе, мастер начальной настройки предложит ввести параметры локальной сети. При необходимости можно задать mac-адрес интерфейса, а также настроить интерфейс на раздачу адресов локальным хостам по протоколу DHCP, указав диапазон назначаемых адресов.

Мастер настройки сети

vpx0 Локальная сеть

Общие настройки

Название *

Ip-адрес/префикс *

VLAN ID

NAT из локальных сетей

Разрешить DHCP в этой сети

Диапазон ip-адресов *

Разрешить управление ИКС через веб

Разрешить управление ИКС через SSH

< Назад

Далее >

Отмена

Внимание! В ИКС вместо ввода маски сети в отдельном поле, необходимо вводить ip-адрес с префиксом сети в формате ip-адрес/префикс.

Таблица перевода маски сети в префиксы:

маска	префикс
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Кроме того, можно задавать диапазоны адресов в формате ip-адрес:маска. Например Введённый адрес ИКС в локальной сети можно было бы ввести как 192.168.17.123:255.255.255.0.

Настройка провайдера

На следующем этапе необходимо настроить провайдера. Для этого в соответствующих полях необходимо ввести адрес и префикс сети, адрес шлюза и адрес DNS сервера (одного или двух).

Мастер настройки сети vtx1 Провайдер

Общие настройки

Имя провайдера *

Использовать следующий ip-адрес: Получить ip-адрес автоматически

Ip-адрес/префикс * Основной шлюз *

DNS Предпочитаемый DNS-сервер Альтернативный DNS-сервер

VLAN ID Приоритет Ширина канала Мбит/с

Разрешить управление ИКС через веб Разрешить управление ИКС через SSH

Маску сети для провайдера необходимо вводить так же как и на предыдущем этапе: в виде адрес/префикс либо в виде адрес:маска.

В случае, когда провайдеров несколько, для каждого из них можно указать [приоритет](#).

Завершение работы мастера

На последней странице мастера настройки выводятся все введенные параметры.

Завершение мастера настройки сети

Пожалуйста, проверьте правильность введенных данных

Новая локальная сеть (192.168.17.134/24)

Тип: Локальная сеть
Интерфейс: vmx0
Ip-адрес/префикс: 192.168.17.134/24
DHCP: выключен
Управление ИКС: веб, ssh
CARP: выключен
NAT из локальных сетей: выключен

МегаТелеком (77.58.4.29/30)

Тип: Провайдер
Интерфейс: vmx1
Ip-адрес/префикс: 77.58.4.29/30
Основной шлюз: 77.58.4.30
Предпочитаемый DNS-сервер: 8.8.8.8
Приоритет: Основной
Доступность шлюза: информация недоступна

Назад Готово Отмена

Необходимо нажать кнопку «готово», мастер настройки сети применит новую конфигурацию и откроет модуль [сетевых интерфейсов](#).

Провайдеры и сети | Внешние устройства | Монитор провайдеров | Журнал

Добавить | Удалить | Выключить | Редактировать | **Мастер настройки сети** | Поиск... | ↻

 МегаТелеком (77.58.4.29/30) Провайдер	основной, шлюз не пингуется
 Новая локальная сеть (192.168.17.134/24) Локальная сеть	кабель подключен

Интерфейс: vmx0
Ip-адрес/префикс: 192.168.17.134/24
DHCP: выключен
Управление ИКС: веб, ssh
CARP: выключен
NAT из локальных сетей: выключен

Удалить | Редактировать | Выключить

Важно: если после прохождения Мастера настройки сети у вас пропал доступ к веб-интерфейсу, отключите через консоль восстановления межсетевой экран и проверьте, что ваша локальная сеть присутствует в поле «Доступ через веб» [настроек межсетевого экрана](#). В нем должны быть перечислены все сети, из которых осуществляется доступ к веб-интерфейсу. Если вы изменяли подсеть локального интерфейса, то при необходимости впишите ее.

Если вы не уверены, каким образом лучше интегрировать ИКС в вашу сеть, вы можете ознакомиться с несколькими [стандартными сценариями установки ИКС](#)

После настройки сети можно приступить к [созданию пользователей](#).

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:netmaster>

Last update: **2019/11/10 19:25**

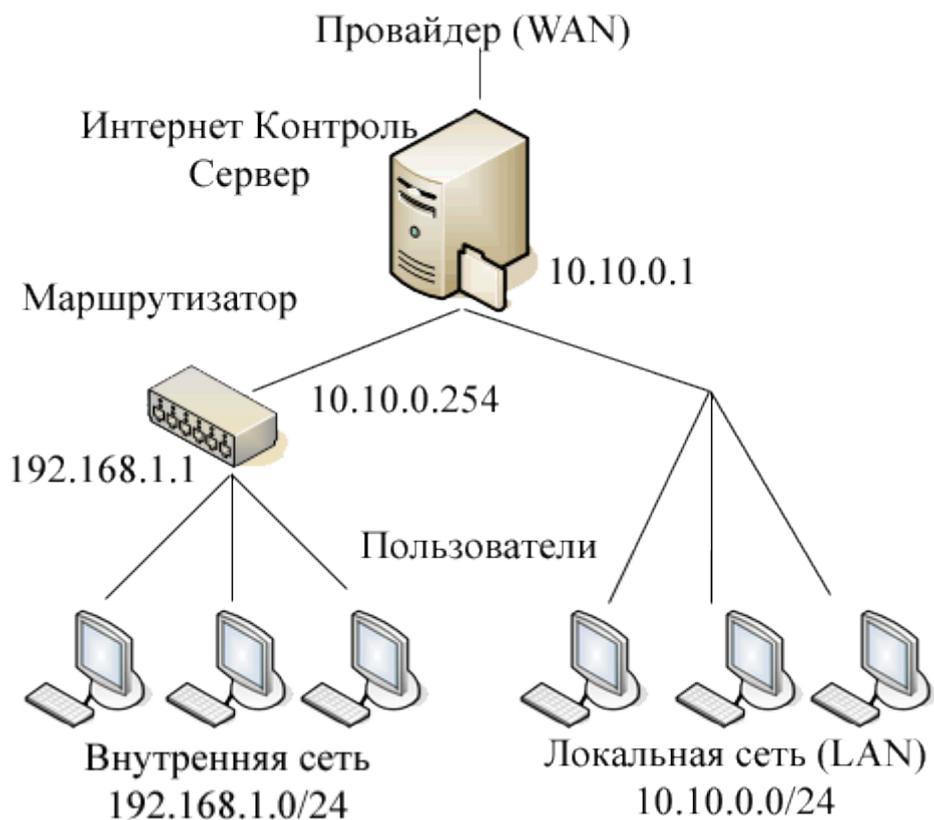


Провайдеры и сети

Общие положения

В модуле «Провайдеры и сети» содержится список всех внешних, внутренних и виртуальных сетей, подключенных к ИКС.

Для начала рассмотрим, что выступает в качестве объекта маршрутизации. Это:



1. WAN - сеть, которая в терминологии ИКС обозначается как "Провайдер",
2. LAN - сеть, directly-connected к ИКС,
3. Внутренняя сеть - сеть, которая не подключена к ИКС напрямую, а отделена маршрутизатором,
4. 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.

МегаТелеком (192.168.170.134/24)
Провайдер

выбран по умолчанию, основной, подключен

Интерфейс: vmtx1
 Мас-адрес: 00:50:56:8e:4d:28
 Ip-адрес/префикс: 192.168.170.134/24
 Основной шлюз: 192.168.170.254
 DNS: используются корневые DNS-сервера
 Приоритет: Основной
 Выбран по умолчанию с: 01.11.2019 14:54
 Доступность шлюза: 0.469 мс
 Управление ИКС: веб, ssh

выбрать по умолчанию

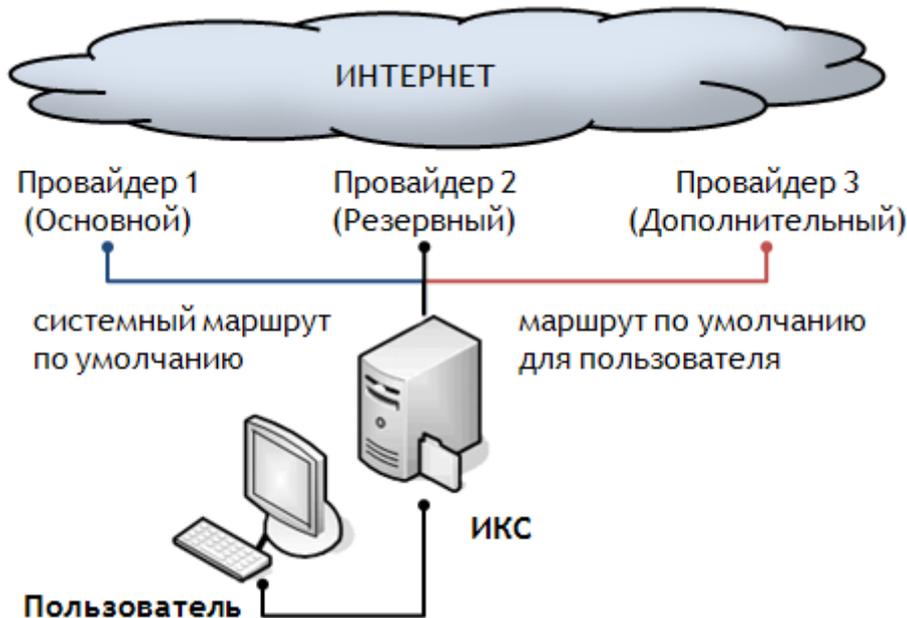
Провайдер - в терминологии ИКС это WAN-интерфейс, который обеспечивает работу сервиса NAT для пользователей ИКС.

При создании/редактировании провайдера, если установить флаг «**Сохранение UDP порта**», то порт исходящего UDP-трафика не будет подменяться «ИКС».

Приоритеты провайдеров

Каждому провайдеру при создании назначается один из трех возможных приоритетов:

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



Следующая схема представляет работу трех провайдеров ИКС. Основной Провайдер 1 является шлюзом по умолчанию для всех пользователей и сервисов. Провайдер 2 неактивен до тех пор, пока не пропадет связь с Провайдером 1. Провайдер 3 настроен как дополнительный. Для выделенного пользователя настроен статический маршрут через этого провайдера.

Вкладка «Внешние устройства» отвечает за добавление маршрутизаторов Cisco.

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

Параметры провайдера

 МегаТелеком (192.168.170.134/24)
Провайдер

выбран по умолчанию, основной, подключен
 выбрать по умолчанию

Редактировать Выключить ↕ ↻

Общее

Интерфейс: vmx1
Mac-адрес: 00:50:56:8e:4d:28
Ip-адрес/префикс: 192.168.170.134/24
Основной шлюз: 192.168.170.254
DNS: используются корневые DNS-сервера
Приоритет: Основной
Выбран по умолчанию с: 01.11.2019 14:54
Управление ИКС: веб, ssh

Статистика

За день: ▲148.81K ▲0
За неделю: ▲148.81K ▲0
За месяц: ▲148.81K ▲0

Наблюдение

Доступность шлюза: 0.381 мс

DynDNS

Сервер: Не использовать

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 отображается общее состояние провайдера и сведения о его DynDNS-сервере.

Состояние **Настройки** Правила События

Настройки мониторинга

- Проверять наличие линка на интерфейсе
- Проверять доступность шлюза
- Проверять доступность серверов

Добавить

Удалить

Настройки DynDNS

Сервер

Не использовать

Имя хоста

Логин

Пароль

- Получить адрес с сетевого интерфейса
- Получить адрес автоматически

Сохранить

Обновить

Каким образом 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. ИКС может определять доступность провайдера по следующим критериям:

1. Наличие сигнала в линии,
2. Доступность шлюза провайдера по умолчанию,
3. Доступность определенных внешних хостов;

Также, косвенным критерием для администратора может служить доступность провайдера через сервис DynDNS.

Во вкладке «Настройки» можно задать критерии мониторинга и определить параметры DynDNS.

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.

В закладке «Журнал» находится сводка всех системных сообщений от интерфейса провайдера. 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.

Данная вкладка наиболее актуальна для rrr-провайдеров (PPPoE, PPTP), сообщения от статических провайдеров появляются в журнале редко.

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.

Наконец, 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.

From:
<https://doc.a-real.ru/> - **Документация**

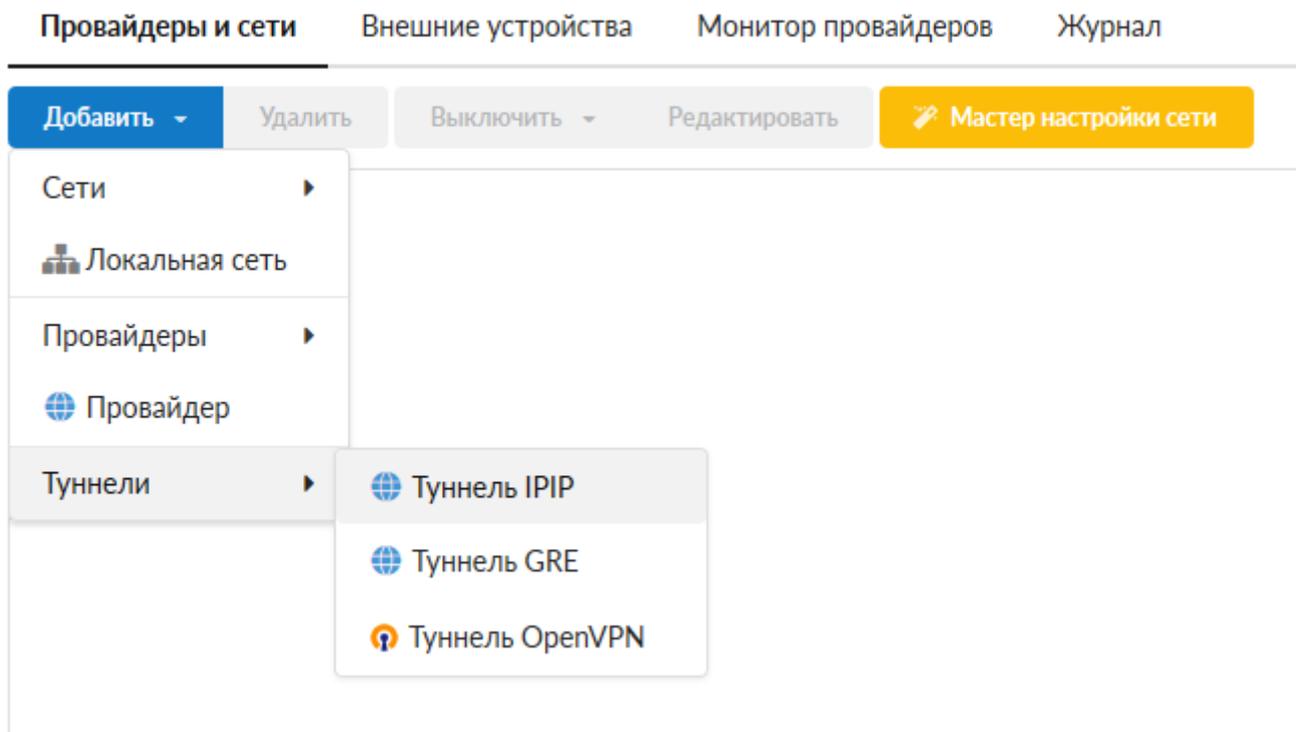
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:networks>

Last update: **2019/11/10 19:25**



Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру. Статические туннели используются для объединения нескольких локальных сетей в одну: например при объединении нескольких удалённых офисов в одну локальную сеть таким образом, чтобы пользователи одной сети могли обращаться к ресурсам других. Туннели настраиваются на пограничных маршрутизаторах этих сетей и весь промежуточный трафик передаётся через интернет инкапсулированным в IP или GRE-пакеты.

В ИКС вы можете настроить подключение между серверами статическим туннелем по IP/IP или GRE протоколу.



Обычно выбор типа туннеля зависит от промежуточных провайдеров, которые по каким-либо причинам они могут блокировать трафик GRE или IP/IP что приводит к невозможности использования какого-то одного типа туннеля. Принципиальной же разницы между этими типами туннелей нет.

<h3>Добавление туннеля IPIP</h3> <p>Общие настройки Настройки шифрования</p> <p>Название * Ламповый туннель</p> <p>Внешний интерфейс * Мощный провайдер (192.168.170.134/24) x</p> <p>Внешний ip-адрес удаленного сервера * 192.168.187.14</p> <p>Локальный ip-адрес туннеля * 10.0.0.1</p> <p>Удаленный ip-адрес туннеля * 10.0.0.2</p> <p>Локальные сети Локальные сети</p> <p>Удаленные сети Удаленные сети</p> <p>MTU Автоопределение</p> <p><input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей</p> <p><input type="checkbox"/> Использовать NAT</p> <p>Добавить Отмена</p>	<h3>Добавление туннеля GRE</h3> <p>Общие настройки Настройки шифрования</p> <p>Название * Классный туннель GRE</p> <p>Внешний интерфейс * Мощный провайдер (192.168.170.134/24) x</p> <p>Внешний ip-адрес удаленного сервера * 192.168.187.14</p> <p>Локальный ip-адрес туннеля * 10.0.0.1</p> <p>Удаленный ip-адрес туннеля * 10.0.0.2</p> <p>Локальные сети Локальные сети</p> <p>Удаленные сети Удаленные сети</p> <p>MTU Автоопределение</p> <p><input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей</p> <p><input type="checkbox"/> Использовать NAT</p> <p>Ключ GRE (не использовать)</p> <p>Добавить Отмена</p>
---	--

Настройки туннелей также не отличаются. Вам необходимо указать, на каком интерфейсе будет настроен данный туннель и прописать параметры маршрутизации: внешний адрес удаленного сервера, адрес локальной сети и адрес удаленной сети. Аналогичные настройки необходимо произвести на другом конце туннеля.

Важно: для того, чтобы туннель работал корректно, необходимо, чтобы в межсетевом экране ИКС был разрешен GRE-трафик, а также разрешены входящие соединения с ip-адреса удаленного сервера.

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.

Добавление туннеля IPsec

Общие настройки **Настройки шифрования**

Использовать шифрование

Ключ шифрования

Ключ шифрования

Настройки для фазы 1:

Режим работы

main

Настройки для фазы 2:

Протокол

ESP

Алгоритм шифрования

aes256

PFS

15 - modp3072

Алгоритм хеширования

sha2_384

Алгоритм аутентификации *

hmac_sha2_384 ✕

DH-группа

15 - modp3072

Алгоритм шифрования

aes256 ✕

Время жизни *

28800

сек.

Время жизни *

1200

сек.

Добавить

Отмена

Защита передачи данным по туннелям позволяет избежать многих проблем, связанных с утечкой информации и получения ложных данных. Вы можете защитить туннельный трафик, перейдя на вкладку «Шифрование» и установив флажок «Использовать шифрование». После этого вы можете произвести необходимые настройки параметров.

Внимание! Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.

Внимание! При использовании IPsec шифрования в туннелях IPsec и GRE трафик будет проходить через интерфейс **enc0**. Статистика на данном интерфейсе не собирается!

OpenVPN - свободная реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall, без необходимости изменения их настроек.

Добавление туннеля OpenVPN

Основные настройки

Шифрование и сертификаты

Название *

Лучший туннель OpenVPN

Адрес сервера *

10.100.0.0

Протокол

UDP

Порт сервера *

1194

Использовать NAT

Добавить

Отмена

Система туннелей OpenVPN построена таким образом, что одна из машин выбирается сервером, а все остальные - клиентами. На сервере прописывается адресация пространства внутри openVPN-сети (рекомендуется оставить значение по умолчанию) и размещаются SSL-сертификаты, а на клиентах указывается внешний ip-адрес сервера. Также, указывается порт обмена данными, что позволяет подключаться к серверу, который находится за межсетевым экраном или NAT, при помощи перенаправления портов .

Чтобы прописать необходимые сертификаты от сервера клиентам, сделайте следующее:

1. На сервере необходимо создать [OpenVPN-сеть](#)

 **Муми-OpenVPN (10.8.0.0/24)**
OpenVPN-сеть

Ip-адрес/Префикс: 10.8.0.0/24
Протокол: udp
Порт сервера: 1194

Корневой сертификат:  Корневой сертификат
Сертификат сервера:  Муми-OpenVpn

[Подробнее...](#) [Настройки авторизации](#) [Выгрузить сертификаты](#) [Удалить](#) [Редактировать](#) [Выключить](#)

2. Создать пользователя для подключения и открыть ему доступ в модуле OpenVPN

VPN-сервер Настройки **Пользователи** Текущие сеансы События Журнал

Добавить Удалить Выключить Редактировать

Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
Корневая группа			<input type="checkbox"/>	<input checked="" type="checkbox"/>
Семья			<input type="checkbox"/>	<input type="checkbox"/>
Долина			<input type="checkbox"/>	<input type="checkbox"/>
Друзья			<input type="checkbox"/>	<input type="checkbox"/>
Туде Янссон	root		<input type="checkbox"/>	<input type="checkbox"/>
Муми-туннель	tunnel		<input type="checkbox"/>	<input checked="" type="checkbox"/> Муми-OpenVPN (10.8.0.0/24)

3. Выгрузить сертификаты в индивидуальном модуле пользователя

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления **OpenVPN** Приложения Статистика

OpenVPN-доступ для пользователя включен в Муми-OpenVPN (10.8.0.0/24)

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей Удаленные сети

Передать клиентам маршруты до сетей Удаленные сети

Сертификат клиента

Муми-OpenVPN_Муми-туннель

Сохранить Обновить Выгрузить сертификаты

4. Распаковать скачанный архив с сертификатами для подключения и импортировать корневой и конечный сертификаты на клиентской стороне

Защита ООО "Организация" > Сертификаты Администратор 137

Добавить Удалить Просмотр сертификата Импортировать Экспорт

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Сертификаты					
Корневой сертификат	CA	зашифрован	21.11.2019	21.11.2020	test.ru
OpenVpnNetwork1_tunnel	Конечный сертификат	не зашифрован	21.11.2019	21.11.2020	tunnel
Autogenerated Asterisk_5dd662397b8cd069169904	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-asterisk
Autogenerated GUI_5dd6623855b1d390975404	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-gui
Autogenerated MailServer_5dd66238932e16.61893393	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-mail-server

5. После этого импортированные сертификаты можно будет выбрать на вкладке «Шифрование» при создании туннеля OpenVPN

Добавление туннеля OpenVPN

Основные настройки

Шифрование и сертификаты

Алгоритм шифрования

AES-256-CBC

Алгоритм хеширования

SHA256

Включить сжатие LZO

link-MTU *

1500

Корневой сертификат

Корневой сертификат

Сертификат клиента

OpenVpnNetwork1_tunnel

Ключ TLS авторизации

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
7dbb7d87c3b7e3b9745211888bcbb9ef
9524ae4cc6876bf37255ef390a339c48
```

Сохранить

Отмена

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:tunnels>

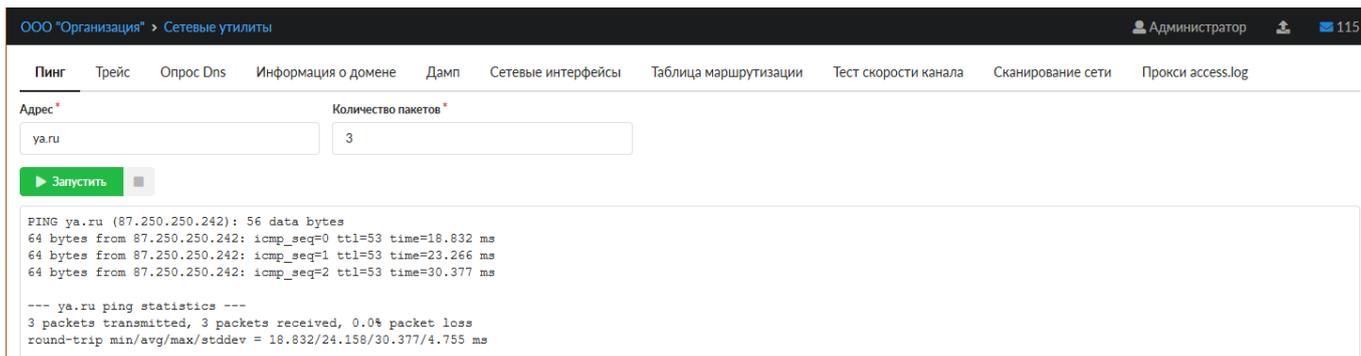
Last update: **2019/11/27 15:18**



Сетевые утилиты

В состав ИКС входят несколько сетевых утилит, которые помогают выполнять диагностику сети.

Пинг



Пинг (ping) — утилита для проверки соединений в сетях на основе TCP/IP. Она 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.

Также 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.

ООО "Организация" > Сетевые утилиты > Трейс

Пинг **Трейс** Опрос Dns Информация о домене Дамп Сетевые интерфейсы

Адрес * 8.8.8.8

▶ Запустить

```
tracert to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  192.168.170.254 (192.168.170.254)  4.290 ms  5.065 ms  1.200 ms
 2  ysul-ccr1036-3.yar.ru (213.187.127.100)  1.373 ms  1.702 ms  1.228 ms
 3  ysul-asbr-0-vlan922.yar.ru (213.187.127.101)  1.186 ms  2.344 ms  1.526 ms
 4  178.176.156.73 (178.176.156.73)  13.166 ms  4.911 ms  2.586 ms
 5  dns.google (8.8.8.8)  31.005 ms  28.545 ms  29.612 ms
```

Эта утилита позволяет определить проблемы с маршрутизацией трафика, а также в случае проблем при доставке данных до какого-то узла - определить, на каком именно участке сети возникли неполадки.

Нужно отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети. В силу 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.

Опрос DNS

ООО "Организация" > Сетевые утилиты > Опрос Dns

Пинг Трейс **Опрос Dns** Информация о домене Дамп Сетевые интерфейсы

Адрес *	Тип записи	DNS-сервер
<input type="text" value="ya.ru"/>	<input type="text" value="A"/>	<input type="text" value="(ИКС)"/>

```
; <<>> DiG 9.14.7 <<>> ya.ru a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50747
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9ca3f4b8da1c7d99c3ac4ef75dbc20b08f27625612a2c09f (good)
;; QUESTION SECTION:
;ya.ru.                IN      A

;; ANSWER SECTION:
YA.ru.                 472     IN      A       87.250.250.242

;; AUTHORITY SECTION:
YA.ru.                 345472 IN      NS      ns2.yandex.RU.
YA.ru.                 345472 IN      NS      ns1.yandex.RU.

;; ADDITIONAL SECTION:
ns1.YANDEX.ru.        345472 IN      A       213.180.193.1
ns2.YANDEX.ru.        345472 IN      A       93.158.134.1
ns1.YANDEX.ru.        345472 IN      AAAA    2a02:6b8::1
ns2.YANDEX.ru.        345472 IN      AAAA    2a02:6b8:0:1::1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 01 15:10:24 MSK 2019
;; MSG SIZE rcvd: 229
```

Опрос DNS (dig) - позволяет посылать различные запросы к днс-серверам и определять ошибки в их конфигурации.

При использовании необходимо ввести домен и выбрать тип записи, также можно указать конкретный dns сервер для опроса. Более подробно о типах записи смотрите в руководстве по использованию модуля DNS.

Информация о домене

Пинг Трейс Опрос Dns **Информация о домене** Дамп Сетевые интерф

Адрес *

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.tcinet.ru

domain:     RU

organisation: Coordination Center for TLD RU
address:    8 Marta street 1, bld 12
address:    Moscow 127083
address:    Russian Federation

contact:    administrative
name:       .RU domain Administrative group
organisation: Coordination Center for TLD RU
address:    8 Marta street 1, bld 12
address:    Moscow 127083
address:    Russian Federation
phone:      +7 495 730 29 71
fax-no:     +7 495 730 29 68
e-mail:     ru-adm@cctld.ru
```

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.

Дамп

Дамп (tcpdump) - отображает заголовки пакетов, проходящих через выбранный сетевой интерфейс. Позволяет диагностировать проблемы связанные с настройкой межсетевого экрана, маршрутизацией и работой сетевых сервисов.

Пинг Трейс Опрос Dns Информация о домене **Дамп** Сетевые интерфейсы Таблица маршрутизации

Интерфейс: МегаТелеком (vnx1) Протокол: (любой) Порт: (любой)

Хост: (любой)

Источник: (любой) Назначение: (любой)

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vnx1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:12:42.476443 IP 192.168.17.66.137 > 192.168.17.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
15:12:42.703997 ARP, Request who-has 192.168.17.227 tell 192.168.17.254, length 46
15:12:42.704171 ARP, Request who-has 192.168.170.165 tell 192.168.170.254, length 46
15:12:42.718844 IP 192.168.170.134 > 87.250.250.242: ICMP echo request, id 49737, seq 1307, length 64
15:12:42.718895 IP 192.168.170.134 > 192.168.170.254: ICMP echo request, id 18322, seq 52, length 64
15:12:42.719446 IP 192.168.170.254 > 192.168.170.134: ICMP echo reply, id 18322, seq 52, length 64
15:12:42.744182 IP 87.250.250.242 > 192.168.170.134: ICMP echo reply, id 49737, seq 1307, length 64
15:12:43.228728 IP 192.168.17.66.137 > 192.168.17.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
15:12:43.718771 ARP, Request who-has 192.168.17.227 tell 192.168.17.254, length 46
15:12:43.719055 ARP, Request who-has 192.168.170.165 tell 192.168.170.254, length 46
15:12:43.731709 IP 192.168.170.134 > 87.250.250.242: ICMP echo request, id 49737, seq 1308, length 64
15:12:43.731801 IP 192.168.170.134 > 192.168.170.254: ICMP echo request, id 18322, seq 53, length 64
15:12:43.732115 IP 192.168.170.254 > 192.168.170.134: ICMP echo reply, id 18322, seq 53, length 64
15:12:43.754165 IP 87.250.250.242 > 192.168.170.134: ICMP echo reply, id 49737, seq 1308, length 64
15:12:44.723555 ARP, Request who-has 192.168.170.165 tell 192.168.170.254, length 46
15:12:44.723795 ARP, Request who-has 192.168.17.227 tell 192.168.17.254, length 46
15:12:44.741768 IP 192.168.170.134 > 87.250.250.242: ICMP echo request, id 49737, seq 1309, length 64
15:12:44.741839 IP 192.168.170.134 > 192.168.170.254: ICMP echo request, id 18322, seq 54, length 64
15:12:44.742138 IP 192.168.170.254 > 192.168.170.134: ICMP echo reply, id 18322, seq 54, length 64
15:12:44.764874 IP 87.250.250.242 > 192.168.170.134: ICMP echo reply, id 49737, seq 1309, length 64
15:12:45.736474 ARP, Request who-has 192.168.17.227 tell 192.168.17.254, length 46
15:12:45.736652 ARP, Request who-has 192.168.170.165 tell 192.168.170.254, length 46
15:12:45.751653 IP 192.168.170.134 > 87.250.250.242: ICMP echo request, id 49737, seq 1310, length 64
15:12:45.751702 IP 192.168.170.134 > 192.168.170.254: ICMP echo request, id 18322, seq 55, length 64
15:12:45.752077 IP 192.168.170.254 > 192.168.170.134: ICMP echo reply, id 18322, seq 55, length 64
15:12:45.774779 IP 87.250.250.242 > 192.168.170.134: ICMP echo reply, id 49737, seq 1310, length 64
15:12:46.373733 ARP, Request who-has 192.168.17.254 tell 192.168.17.237, length 46
```

Для запуска утилиты необходимо выбрать сетевой интерфейс, на котором будет выполняться сбор данных.

Для фильтрации сообщений возможно выбрать протокол, указать порт, а также выбрать направление сетевого трафика для указываемого IP-адреса, «Хост» или «Источник/Назначение».

Сетевые интерфейсы

Пинг Трейс Опрос Dns Информация о домене Дамп **Сетевые интерфейсы** Таблица маршрутизации Тест

▶ Запустить

```
vmx0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
  ether 00:50:56:8e:40:c0
  hwaddr 00:50:56:8e:40:c0
  inet 192.168.17.134 netmask 0xffffffff broadcast 192.168.17.255
  nd6 options=29<PERFORMNUD, IPDISABLED, AUTO_LINKLOCAL>
  media: Ethernet autoselect
  status: active
vmx1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
  ether 00:50:56:8e:4d:28
  hwaddr 00:50:56:8e:4d:28
  inet 192.168.170.134 netmask 0xffffffff broadcast 192.168.170.255
  nd6 options=29<PERFORMNUD, IPDISABLED, AUTO_LINKLOCAL>
  media: Ethernet autoselect
  status: active
vmx2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
  ether 00:50:56:8e:95:f0
  hwaddr 00:50:56:8e:95:f0
  nd6 options=29<PERFORMNUD, IPDISABLED, AUTO_LINKLOCAL>
  media: Ethernet autoselect
  status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
  options=680003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
  inet6 ::1 prefixlen 128
  inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
  inet 127.0.0.1 netmask 0xff000000
  nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
  groups: lo
enc0: flags=41<UP,RUNNING> metric 0 mtu 1536
  nd6 options=29<PERFORMNUD, IPDISABLED, AUTO_LINKLOCAL>
  groups: enc
pflog0: flags=141<UP,RUNNING,PROMISC> metric 0 mtu 33160
  groups: pflog
lo1: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
  options=680000<LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
  inet 172.77.77.253 netmask 0xffffffff
  inet 172.77.77.1 netmask 0xffffffff
  nd6 options=29<PERFORMNUD, IPDISABLED, AUTO_LINKLOCAL>
  groups: lo
```

Утилита «Сетевые интерфейсы» позволяет получить сведения о состоянии всех интерфейсов ИКС. Она выводит результат команды `ifconfig`, позволяя узнать, какие ip-адреса назначены каждому интерфейсу, какие виртуальные интерфейсы созданы, а также проверить наличие сигнала в подключенном кабеле.

Таблица маршрутизации

▶ Запустить

```
Routing tables

Internet:
Destination      Gateway          Flags    Netif  Expire
default          192.168.170.254 UGS      vmx1
127.0.0.1        link#4          UH       lo0
172.77.77.1      link#7          UH       lo1
172.77.77.253    link#7          UH       lo1
192.168.17.0/24  link#1          U        vmx0
192.168.17.134   link#1          UHS      lo0
192.168.170.0/24 link#2          U        vmx1
192.168.170.134  link#2          UHS      lo0

Internet6:
Destination      Gateway          Flags    Netif  Expire
::/96            ::1             UGRS     lo0
::1              link#4          UH       lo0
::ffff:0.0.0.0/96 ::1             UGRS     lo0
fe80::/10        ::1             UGRS     lo0
fe80::%lo0/64    link#4          U        lo0
fe80::1%lo0      link#4          UHS      lo0
ff02::/16        ::1             UGRS     lo0
```

Данная утилита выводит текущую таблицу маршрутизации ИКС. С ее помощью вы можете увидеть все маршруты, созданные в системе.

Тест скорости канала

Эта утилита позволяет измерить пропускную способность канала. Для измерения необходимо выбрать сервер и запустить 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 нагруженность.

Сканирование сети

Пинг Трейс Опрос Dns Информация о домене Дамп Сетевые интерфейсы Таблица маршрутизации Тест скорости канала **Сканирование сети**

Действие Адрес* Порт

Сканирование портов 192.168.17.134

▶ Запустить

```

Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 15:15 MSK
Initiating System DNS resolution of 1 host. at 15:15
Completed System DNS resolution of 1 host. at 15:15, 0.03s elapsed
Initiating SYN Stealth Scan at 15:15
Scanning 192.168.17.134 [100 ports]
Discovered open port 22/tcp on 192.168.17.134
Discovered open port 53/tcp on 192.168.17.134
Discovered open port 3128/tcp on 192.168.17.134
Discovered open port 81/tcp on 192.168.17.134
Increasing send delay for 192.168.17.134 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Discovered open port 389/tcp on 192.168.17.134
Completed SYN Stealth Scan at 15:15, 14.73s elapsed (100 total ports)
Nmap scan report for 192.168.17.134
Host is up (0.000045s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
81/tcp    open  hosts2-ns
389/tcp   open  ldap
3128/tcp  open  squid-http

Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.88 seconds
Raw packets sent: 495 (21.780KB) | Rcvd: 555 (24.420KB)

```

С помощью сканирования сети вы можете тестировать безопасность локальной сети предприятия. Она позволяет проверить доступность локальных машин, а также определить открытые в сети порты. Кроме того, указав в качестве исследуемого хоста сам ИКС, вы можете дополнительно проверить безопасность системы на предмет доступных портов.

Сканирование сети может работать в трех режимах:

Режим	Действия
Доступность адресов	ИКС проверяет, в сети ли выбранные машины. В качестве аргумента может быть указан как отдельный хост, так и подсеть. В последнем случае ИКС проверит доступность всего указанного диапазона перебором.
Сканирование портов	ИКС проверяет, какие порты открыты для доступа на указанном хосте или всех машинах указанной подсети
Информация о версии	ИКС проверяет версию службы каждого открытого порта на указанном хосте или всех машинах указанной подсети

From: <https://doc.a-real.ru/> - **Документация**

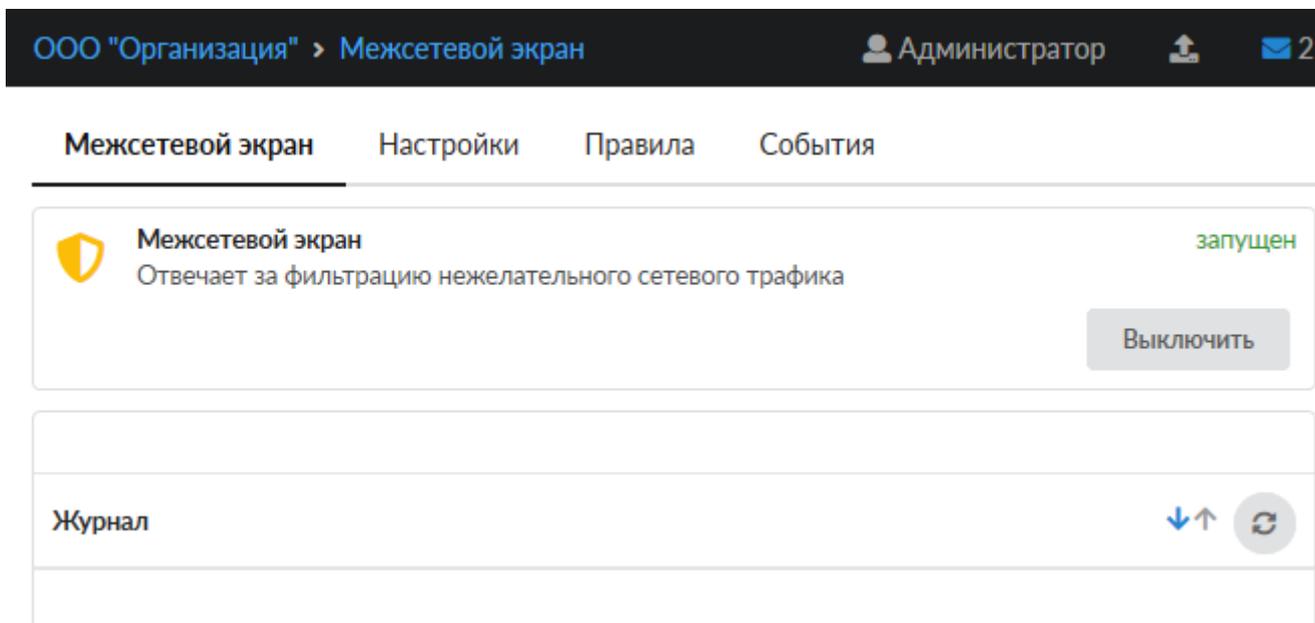
Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:netutil>

Last update: **2019/11/10 19:25**



Межсетевой экран

Стартовая страница модуля



Межсетевой экран — комплекс программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также, межсетевой экран ИКС отвечает за трансляцию сетевых адресов во внешнюю сеть (NAT) и перенаправление портов.

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние события системы.

Внимание! Выключение межсетевого экрана оставит работающими только правила NAT'а. Все правила, ограничивающие доступ извне, будут отключены, что может негативно сказаться на безопасности системы. Отключайте межсетевой экран только при крайней необходимости.

Также следует отметить, что после перезагрузки системы с выключенным межсетевым экраном список правил `pf`, в том числе и правила NAT'а будет полностью очищен, и пользователи потеряют доступ во внешнюю сеть по всем протоколам, кроме HTTP.

Настройки

Межсетевой экран

Настройки

Правила

События

Управление ИКС через веб

Управление ИКС через SSH

Максимальное количество активных соединений *

Режим работы межсетевого экрана

Вкладка «Настройки» позволяет определить уровень доступа к управлению ИКС без создания дополнительных правил межсетевого экрана. Вы можете прописать ip-адреса или подсети, с которых будет осуществляться доступ к веб-интерфейсу ИКС или к консоли восстановления по протоколу SSH.

Если вы хотите получать доступ к 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 ИКС может быть затруднена прохождением через NAT модуля pf. В таком случае измените очередность запуска на pf→ipfw.

Правила

Вкладка «Правила» является главным рабочим полем администратора по настройке межсетевого экрана. Она разделена на две части: список всех интерфейсов 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.

Межсетевой экран Настройки **Правила** События

Добавить Удалить Выключить Редактировать Поиск... ↻

- ✓ Разрешающее правило
- ⊘ Запрещающее правило
- 👤 Приоритет
- ➔ Маршрут
- Ограничение скорости

Разрешающие правила

- ✓ **Доступ по протоколу ICMP**
Разрешить ICMP трафик, входящий на ИКС через Внешние интерфейсы
- ✓ **Доступ к серверу через GRE тоннели**
Разрешить GRE трафик, входящий на ИКС через Внешние интерфейсы
- ✓ **Доступ к почтовому серверу**
Разрешить TCP трафик, входящий на ИКС на порт ✉ Порт SMTP (25), 📧 Порт IMAP (143), 📧 Порт POP3 (110) через Внешние интерфейсы
- ✓ **Доступ к VPN-серверу** служба не запущена
Разрешить TCP трафик, входящий на ИКС на порт ● rppp (1723) через Внешние интерфейсы
- ✓ **Доступ к L2TP-серверу** служба не запущена
Разрешить UDP трафик, входящий на ИКС на порт 1701 через Внешние интерфейсы
- ✓ **Доступ к OpenVPN-сетям** служба не запущена
Разрешить TCP/UDP трафик, входящий на ИКС на порт ● OpenVpn

Правила межсетевого экрана группируются по типу:

1. Разрешающие правила
2. Запрещающие правила
3. Приоритеты
4. Маршруты
5. 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), веб-сервер (порт 80), 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.

События

Межсетевой экран Настройки Правила **События**

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ↻

📄 Экспорт Удалить логи Все сообщения Поиск... 🔍

⬇ ⬆ ⬇

Запрещающее правило FTP было добавлено пользователем **Администратор**
11:34:42

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.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:firewall>

Last update: **2019/11/10 19:25**



Маршруты

Модуль «Маршруты» расположен в Меню «Сеть». Данный модуль предназначен для просмотра и редактирования маршрутов. При открытии модуля «Маршруты» будет отображен список маршрутов, созданных в ИКС, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать) активирующиеся при выборе объекта.

The screenshot shows the 'Маршруты' (Routes) page in the 'Муми-дол' (Mumi-dol) system. At the top, there is a navigation bar with 'Муми-дол > Маршруты' on the left and user information 'Туге Янссон' and a notification icon '22' on the right. Below the navigation bar is a toolbar with buttons: 'Добавить' (Add), 'Удалить' (Delete), 'Выключить' (Disable), and 'Редактировать' (Edit). A search bar with the placeholder 'Поиск...' and a refresh icon is also present. The main content area displays a list of routes:

- вай-фай через морру**
Направлять трафик, исходящий с ИКС от Вай-фай (192.168.242.242/24) на Муми-локалка (192.168.17.242/24), через шлюз 192.168.17.246
(Использовать NAT)
Buttons: Удалить, Редактировать
- красненький провод**
Направлять трафик, исходящий с ИКС на 192.168.88.0/24, через интерфейс ge1

Маршруты в межсетевом экране создаются аналогично пользовательским маршрутам, но имеют дополнительные опции: *источник*, *порт источника* и *интерфейс*, а также флаг «Использовать NAT».

Добавление правила маршрута

Описание

красненький провод

Направление

Исходящий с ИКС

Протокол

(любой)

Источник

(любой)

Порт источника

(любой)

Назначение

192.168.88.0/24 ✕

Порт назначения

(любой)

Интерфейс

(любой)

Доступные значения и объекты при заполнении полей можно посмотреть наведя на соответствующее поле курсор или выбрать из выпадающего списка, заведенные на «ИКС» значения и объекты. Правило «Маршрут» используется для маршрутизации трафика как между сегментами сети, так и для перенаправления трафика на различных провайдеров.

При установке флага «Не обрабатывать трафик межсетевым экраном», для данного правила, ко всему проходящему трафику через «ИКС» не будут применяться правила межсетевого экрана. Стоит отметить, если не устанавливать данный флаг и через «ИКС» проходит TCP трафик, то межсетевой экран при простое в 30 секунд разорвет данное соединение.

Через шлюз Через интерфейс Через провайдера

 re1

Не обрабатывать трафик межсетевым экраном

Использовать NAT

Время действия

При установке правила «Через шлюз» необходимо указать IP-адрес устройства, выполняющего функцию шлюза. Чаще всего данное правило используется если «ИКС» установлен на сервере имеющем один сетевой интерфейс.

При установке правила «Через интерфейс» создаст правило маршрута через один из сетевых интерфейсов «ИКС».

При установке правила «Через провайдера» сетевой трафик будет направлен через одного из заведенных провайдеров на «ИКС».

Маршруты, созданные в правилах межсетевого экрана, и маршруты, добавленные через одноименный модуль представляют один и тот же список маршрутов ИКС.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:routes>

Last update: **2019/11/10 19:25**



Перенаправление портов

Модуль «Перенаправление портов» расположен в Меню «Сеть». Данный модуль используется, чтобы снаружи организовать доступ к компьютеру, находящемуся в локальной сети: для подключения к windows-серверу по RDP, для подключения к локальному веб-серверу и т.д.

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.

Добавление перенаправления порта

Название *	Порт перенаправления *
<input type="text" value="Ssh23"/>	<input type="text" value="12312"/>
Протокол	
<input type="text" value="TCP"/>	
Источник	Порт источника
<input type="text" value="(любой)"/>	<input type="text"/>
Назначение	
<input type="text" value="85.89.20.117"/>	
Интерфейс	
<input type="text" value="(любой)"/>	

Важно: ip-адрес хоста, на который организовывается проброс порта, должен быть назначен какому-либо пользователю ИКС.

Также можно перенаправлять диапазоны портов, введя номера портов через дефис: например «10000-10100».

Перенаправить на:

Назначение *

Порт *

- Использовать NAT
- Разрешить подключаться из локальной сети
- Автоматически создавать разрешающее правило

Время действия

Также, если необходимо, чтобы машины локальной сети при обращении на перенаправленный порт попадали на хост назначения, можно включить опцию «разрешить подключаться из локальной сети». **Важно! При этом локальные соединения будут проходить через NAT и хост назначения увидит эти подключения как инициированные ИКС.**

Если для хоста, на который перенаправляется запрос, ИКС не является шлюзом по умолчанию, полезно включить для такого перенаправления флаг «Использовать NAT».

Для того, чтобы в межсетевом экране автоматически создавалось 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.

 **Ssh23**
Перенаправить трафик, идущий на 85.89.20.117 на порт 12312, на адрес 192.168.17.6 на порт 3389

Связано с разрешающими правилами:  Разрешающее правило для перенаправления портов Ssh23 1
 Разрешающее правило для перенаправления портов Ssh23 2

[Удалить](#) [Редактировать](#)

 TMD СМТД-?

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:fwd>

Last update: **2019/11/10 19:25**



Служба доменных имен (DNS)

Стартовая страница модуля

DNS-сервер Настройки Зоны Журнал

 **DNS-сервер** запущен
Служба доменных имен

Журнал ↓↑ ↻

sizing zone task pool based on 1 zones 15:37:12
none:104: 'max-cache-size 90%' - setting to 2724MB (out of 3027MB) 15:37:12
set up managed keys zone for view _default, file 'managed-keys.bind' 15:37:12
none:104: 'max-cache-size 90%' - setting to 2724MB (out of 3027MB) 15:37:12
configuring command channel from '/usr/local/etc/namedb/rndc.key' 15:37:12
couldn't add command channel 127.0.0.1#953: file not found 15:37:12
managed-keys-zone: loaded serial 0 15:37:12
all zones loaded 15:37:12
running 15:37:12

DNS (англ. Domain Name System — система доменных имён) — 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 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.

Настройки

Автоматически создавать разрешающее правило

Доступ к DNS-серверу

Разрешить трансфер зон из следующих сетей

Добавить Удалить

Автоматически создавать разрешающее правило

Использовать в качестве DNS-серверов

Добавить Удалить

При подключении к домену прописывать контроллер домена основным DNS

Основной внешний параметр DNS-сервера - список разрешений для трансфера зон. Сюда добавляются адреса других DNS-серверов, которые имеют право получать записи зон от ИКС.

Если у вас не создано ни одного провайдера, то в данной вкладке вы можете вписать DNS-сервера, которые будет использовать ИКС.

Также, вы можете определить, устанавливаются ли первичным DNS-сервером контроллер домена в том случае, если ИКС является его членом.

Зоны

DNS-сервер **Настройки** **Зоны** Журнал

Добавить Удалить Выключить Редактировать

Поиск...

Имя	Тип записи	Параметры	Адрес
DNS-зоны			
.new.zone.backlocal.in-addr.arpa.			
new.zone.local.			
new.zone.local.	NS (авто)		ns1.new.zone.local.
new.zone.secondarylocal.			

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 связанная часть дерева, зона внутри тоже представляет собой дерево.

Вкладка «Зоны» позволяет создавать DNS-зоны для работы различных служб ИКС, таких как веб-сервер, почтовый сервер и джаббер-сервер.

Различаются следующие типы DNS-зон:

- DNS-зона
- Вторичная DNS-зона
- Обратная DNS-зона
- Перенаправление DNS-зоны.(позволяет направлять запросы для данного домена на конкретный dns-сервер)

<p>Добавление DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p>Имя зоны * <input type="text" value="new.zone.local."/> DNS-сервер * <input type="text" value="ns1"/> <input type="text" value=".new.zone.local."/></p> <p>E-mail администратора * <input type="text" value="admin@host.ru"/></p> <p>TTL * <input type="text" value="38400"/> сек. Обновление <input type="text" value="10800"/> сек.</p> <p>Повторение попытки * <input type="text" value="3600"/> сек. Устаревание * <input type="text" value="604800"/> сек.</p> <p>Отрицательное TTL * <input type="text" value="3600"/> сек.</p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>	<p>Добавление DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p><input checked="" type="radio"/> Разрешить чтение из всех сетей <input type="radio"/> Разрешить чтение из указанных сетей</p> <p><input type="text"/></p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>
<p>Добавление вторичной DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p>Имя зоны * <input type="text" value="new.zone.local."/> IP-адрес первичного сервера <input type="text" value="192.168.1.1"/></p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>	<p>Добавление вторичной DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p><input checked="" type="radio"/> Разрешить чтение из всех сетей <input type="radio"/> Разрешить чтение из указанных сетей</p> <p><input type="text"/></p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>
<p>Добавление обратной DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p>Адрес зоны * <input type="text" value="new.zone.backlocal."/> in-addr.arpa. DNS-сервер * <input type="text" value="ns1"/></p> <p>E-mail администратора * <input type="text" value="admin@host.ru"/></p> <p>TTL * <input type="text" value="38400"/> сек. Обновление <input type="text" value="10800"/> сек.</p> <p>Повторение попытки * <input type="text" value="3600"/> сек. Устаревание * <input type="text" value="604800"/> сек.</p> <p>Отрицательное TTL * <input type="text" value="3600"/> сек.</p> <p><input checked="" type="checkbox"/> Автоматически создавать PTR-записи для A-записей</p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>	<p>Добавление обратной DNS-зоны</p> <p>Настройки <u>Доступ</u></p> <p><input checked="" type="radio"/> Разрешить чтение из всех сетей <input type="radio"/> Разрешить чтение из указанных сетей</p> <p><input type="text"/></p> <p><input type="button" value="Добавить"/> <input type="button" value="Отмена"/></p>

Журнал

DNS-сервер Настройки Зоны **Журнал**

01.11.2019 - 01.11.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

⬇ Экспорт Удалить логи Поиск... 🔍

network unreachable resolving '1.ru.pool.ntp.org/A/IN': 192.33.4.12#53 09:49:19
network unreachable resolving '1.ru.pool.ntp.org/A/IN': 192.203.230.10#53 09:49:19

В закладке «Журнал» находится сводка всех системных сообщений от DNS-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, сообщения о состоянии системы (включение/выключение) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

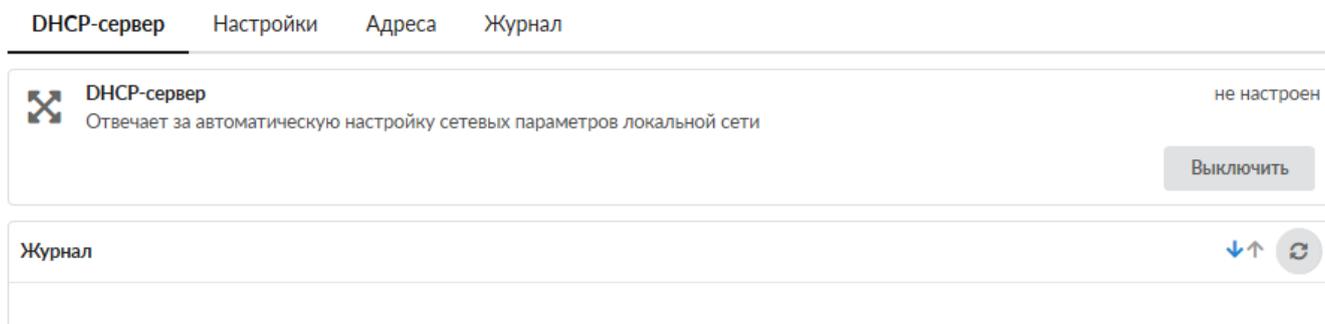
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:dns>

Last update: **2019/11/10 19:25**



DHCP

Модуль «DHCP» расположен в Меню «Сеть». Данный модуль предназначен для настроек протокола DHCP. Модуль «DHCP» имеет четыре вкладки: «DHCP-сервер», «Настройки», «Адреса», «Журнал».



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. <https://ru.wikipedia.org/wiki/DHCP>

DHCP-сервер

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале. Если ни на одной из локальных сетей не выбрана опция DHCP, модуль находится в состоянии «Не настроен».

Включение DHCP

Редактирование локальной сети

Общие настройки

CARP

Название *

Новая локальная сеть

Интерфейс *

vmx0 (00:50:56:8e:40:c0)

Ip-адрес/префикс *

192.168.17.134/24

VLAN ID

(не использовать)

NAT из локальных сетей

Разрешить DHCP в этой сети

Диапазон ip-адресов *

192.168.17.100-192.168.17.100

Разрешить управление ИКС через веб

Разрешить управление ИКС через SSH

Использование DHCP настраивается индивидуально для каждой локальной сети и выполняется в разделе «Провайдеры и сети».

Для того, чтобы разрешить работу DHCP в какой-либо локальной сети, необходимо отредактировать её, установить флаг «разрешить DHCP в этой сети» и задать в поле диапазон адресов, которые будут раздаваться DHCP-сервером (в виде 192.168.1.1-192.168.1.100 или 192.168.1.1/16).

Настройки

DHCP-сервер **Настройки** Адреса Журнал

Использовать ИКС как основной DNS-сервер и сервер времени
 Задать адреса серверов вручную:

Предпочитаемый DNS-сервер	Альтернативный DNS-сервер	Сервер времени
<input type="text" value="8.8.8.8"/>	<input type="text" value="10.5.1.2"/>	<input type="text" value="(ИКС)"/>

WINS-сервер **URL TFTP-сервера**

<input type="text" value="(не используется)"/>	<input type="text" value="tftp://192.168.1.5/public.dhcp"/>
--	---

Срок аренды ip-адреса

<input type="text" value="60"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	минут
---------------------------------	----------------------------------	----------------------------------	-------

ДНС-зона для авторегистрации адресов

<input type="text" value="(нет)"/>	▼
------------------------------------	---

Публиковать скрипт автоконфигурации по DHCP

Использовать скрипт автоконфигурации прокси ИКС
 Указать URL скрипта автоконфигурации вручную:

<input type="text" value="http://192.168.17.134:81/wpad.dat"/>
--

Данная вкладка содержит следующие настройки:

Выбор параметров DNS-серверов и сервера времени позволяет определить, будет ли для всех пользователей, получающих адреса автоматически в качестве DNS-сервера и сервера времени использоваться ИКС либо же сторонние сервера;

Поле **WINS-сервер** - позволяет указать выдаваемый клиентам WINS-сервер для разрешения Netbios-имен. https://ru.wikipedia.org/wiki/Windows_Internet_Name_Service

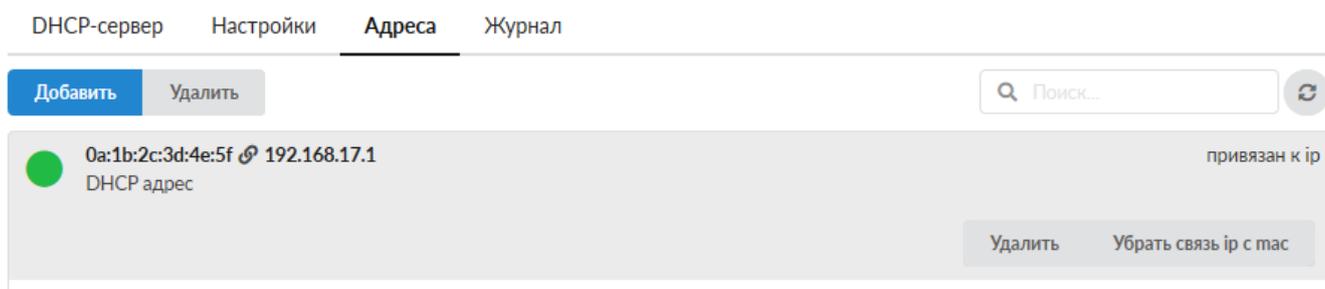
Поле **URL TFTP-сервера** - позволяет указать выдаваемый клиентам TFTP, с которого может быть произведена загрузка тонкого клиента.

Поле **Срок аренды ip-адреса (в минутах)** - позволяет задать период аренды адреса. По истечению данного периода, если клиент с данным адресом отсутствует в сети, запись о выдаче адреса очищается, и он может быть выдан новому клиенту (если не задано сопоставление IP и mac адресов).

Поле **ДНС-зона для авторегистрации адресов** - позволяет указать одну из предварительно созданных DNS-зон, в которой новые пользователи, получившие адреса по протоколу DHCP, будут регистрироваться как A-записи вида <имя_хоста>.<имя_зоны>.

Включение флага **Публиковать скрипт автоконфигурации по DHCP** позволяет сделать выбор, каким образом будут переданы пользователю автоматические настройки прокси-сервера - автоматически либо из указанного в следующем поле адреса, по которому находится файл с настройками.

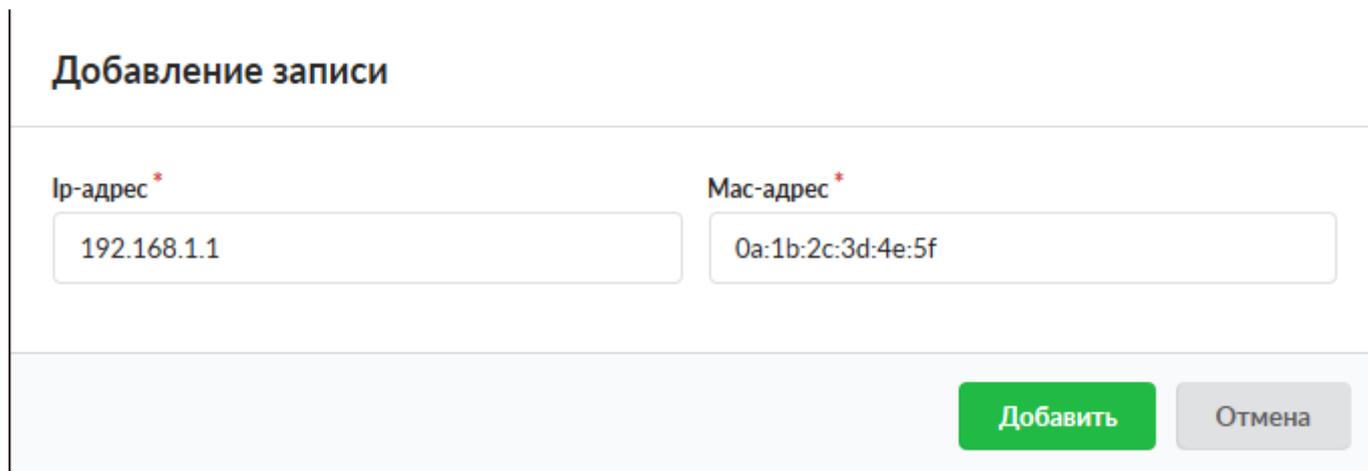
Адреса



Вкладка «Адреса» позволяет 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.

При нажатии кнопки «Добавить» будет открыто окно с полями **IP-адрес** и **MAC-адрес**, что позволит аналогичным образом добавить связь IP и MAC адресов.



Для IP-адресов, присвоенных пользователям, будут отображаться имена владельцев. Клик по имени пользователя переместит на его страницу.

DHCP-сервер использует общий список сопоставлений IP- и MAC-адресов с модулем ARP-таблица.

Журнал

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «DHCP» 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) - 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».

From:

<https://doc.a-real.ru/> - Документация

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:dhcp>

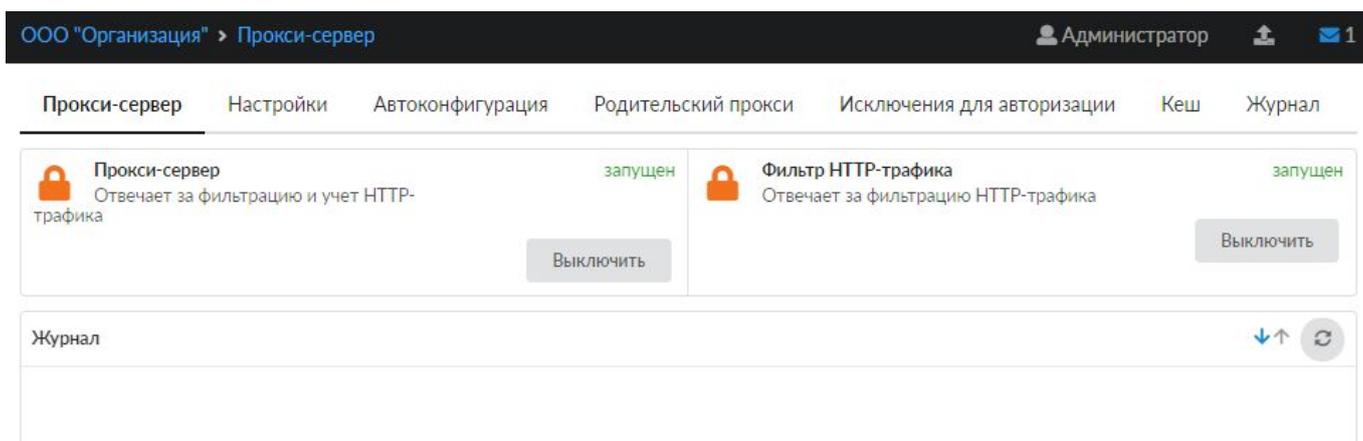
Last update: **2019/11/10 19:25**



Прокси

Стартовая страница модуля

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 изменён прокси-сервером в определённых целях.



Также, прокси-сервер позволяет анализировать проходящие через сервер HTTP-запросы клиентов, выполнять фильтрацию и учёт трафика по URL и mime-типам. Кроме этого, прокси-сервер реализует механизм доступа в интернет по логину/паролю.

Прокси-сервер выполняет кеширование объектов, полученных пользователями из интернета и за счёт 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

Прокси-сервер **Настройки** Автоконфигурация Родительский прокси Исключения для авторизации Кеш Журнал

Порт *
3128

Автоматически создавать разрешающее правило

Доступ к прокси

Тип авторизации: По логину/паролю ИКС
Порядок авторизации пользователей: По IP, затем по логину/паролю

Скрывать ip-адрес пользователя
 Использовать кеш

Размер кеша * 100 МБ
Ограничивать размер ответа (не ограничивать) МБ

Сообщение о запрете доступа
Доступ запрещен

Использовать прозрачный прокси

Порты * 80
Исключения для прозрачного прокси (нет)

Порты для HTTPS * 443
 перехватывать трафик из DMZ сетей
 перехватывать трафик между локальными сетями

Сертификат для HTTPS фильтрации

Расшифровывать трафик с подменой сертификата
 Фильтровать без подмены сертификата

Не фильтровать HTTPS для (нет)
Расшифровывать трафик с подменой сертификата для (нет)

Разрешенные порты * 80, 21, 443, 563, 70, 210, 1025-65535, 280, 488, !
Порты для метода CONNECT * 443, 563

Использовать socks5 сервер

Порт socks5 сервера *

Авторизация на socks5 сервере по логину/паролю

Автоматически создавать разрешающее правило

Использовать антивирус Clamav

Использовать антивирус Касперского

Использовать внешний ICAP-сервер

Сервис REQMOD URI

Разрешать доступ при недоступности сервиса

Сервис RESPMOD URI

Разрешать доступ при недоступности сервиса

Использовать DLP

Использовать контент-фильтр

Использовать SkyDNS

Использовать веб-фильтр Касперского

Использовать DNS

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, то 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 учёта 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.

Типы авторизации

Прокси-сервер ИКС поддерживает два способа авторизации: по ip-адресу пользователя, и по логину-паролю.

Авторизация по ip-адресу подходит для случаев, когда пользователь постоянно пользуется одним и тем же компьютером. Прокси определяет, какому пользователю принадлежит тот или иной трафик, исходя из ip-адреса его компьютера. Этот способ не подходит для терминальных серверов, так как в этом случае с одного ip-адреса работает несколько пользователей. Также этот способ не подходит для организаций, в которых пользователи постоянно перемещаются между рабочими местами. Кроме того, пользователь может сменить ip-адрес своего компьютера и, если не настроена привязка MAC-адреса к IP, ИКС примет его за кого-то другого.

Авторизация по логину/паролю решает проблему привязки пользователей к собственному компьютеру. В этом случае при первом обращении к любому интернет-ресурсу, браузер выдаст пользователю запрос логина/пароля для доступа в интернет. Если в вашей сети пользователи авторизуются в домене, вы можете установить тип авторизации «Через домен». В таком случае, если ИКС подключен к контроллеру домена и в из домена были импортированы пользователи, авторизация будет выполнена прозрачно, без запроса логина/пароля.

Недостаток этого способа авторизации заключается в том, что он не поддерживается прозрачным прокси, и во всех программах, обращающихся в интернет, необходимо прописывать адрес прокси-сервера.

Кроме того, следует помнить о том, что авторизация на прокси используется только для http-трафика пользователей. Доступ в интернет для программ, использующих протоколы, отличные от http, регулируется межсетевым экраном, который имеет только один способ авторизации: по ip-адресу. Другими словами, если пользователь использует только авторизацию по логину/паролю, он не сможет пользоваться почтой, jabber-клиентом, torrent-клиентом и другими программами, не поддерживающими работу через http-прокси.

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 «содержимое кеша». Следует отметить, что веб-интерфейс отображает не все содержимое кэша, а только некоторые элементы, такие как изображения.

Прозрачный прокси

В этом режиме 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».

Для того, чтобы настроить [HTTPS-фильтрацию](#), нужно заполнить поле «Сертификат для SSL-фильтрации» ранее созданным корневым сертификатом. Адреса, которые не нужно фильтровать подменным сертификатом, могут быть добавлены в исключения.

SOCKS5

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 соединиться с SOCKS прокси сервером. Такой прокси сервер контролирует права клиента для доступа к внешним ресурсам и передаёт запрос к серверу. SOCKS может использоваться и противоположным способом, разрешая внешним клиентам соединиться с серверами за межсетевым экраном (брандмауэром).

В отличие от HTTP прокси серверов, SOCKS передаёт 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

Интернет Контроль Сервер поддерживает сканирование трафика, проходящего через прокси-сервер антивирусом. В версии 4 поддерживается 3 антивирусных модуля: бесплатный ClamAV и платные модули DrWeb и Касперский. Для работы антивируса, необходимо приобрести лицензию и установить её в соответствующем модуле.

Для того, чтобы включить антивирусное сканирование веб-трафика каким-либо антивирусным модулем, необходимо включить соответствующую опцию в настройках прокси. Параметр «Максимальный объем для сканирования» определяет максимальный размер файла, единовременно проходящего обработку антивирусом. Файлы, размер которых превышает указанный, сканироваться не будут, что может повлиять на производительность.

Рекомендуется также включить проверку изображений, поскольку существуют вирусы, распространяющиеся через обычные изображения, однако сканирование изображений значительно увеличивает потребление системных ресурсов антивирусом, что при больших объемах графики способно сильно снизить быстродействие сервера.

Разрешённые порты

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

ICAP

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 ИКС сторонний ICAP-сервер, отметив соответствующий флажок в настройках и указав его адрес.

Три последних флажка подключают к работе прокси-сервера соответственно, модули [DLP](#) и [контент-фильтра](#) и [skydns](#)

Автоконфигурация 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 ИКС.

Прокси-сервер Настройки **Автоконфигурация** Родительский прокси Исключения для авторизации Кеш Журнал

Создать скрипт автоконфигурации прокси

HTTP HTTPS FTP

Опубликовать по адресу

Создать виртуальный хост на веб-сервере

Создать запись на DNS-сервере

Публиковать скрипт автоконфигурации по DHCP

Он включается установкой флажка в соответствующей вкладке. Вы можете отметить один или несколько протоколов из доступных (HTTP, HTTPS, FTP).

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 ИКС прокси-сервер будет являться его **родительским прокси**. Кроме того, в качестве родительского прокси может выступать любой узел сети.

Прокси-сервер Настройки Автоконфигурация **Родительский прокси** Исключения для авторизации Кеш Журнал

Использовать родительский прокси

Адрес * Порт *

10.0.0.1 3128

Использовать ICP

Порт ICP

3130

Использовать авторизацию

Логин * Пароль *

Работать без DNS-сервера

Чтобы 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 кэшей 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.

Исключения для авторизации

Прокси-сервер Настройки Автоконфигурация Родительский прокси **Исключения для авторизации** Кеш Журнал

Добавить Удалить

Источник ▲	Назначение	Описание	<input checked="" type="checkbox"/> Выкл.
(любой)	213.146.17.2 mumi.dol	Корпоративный сайт	<input checked="" type="checkbox"/>
192.168.17.43	.google.com / *.ai.\.ru/gi	Поддомены google.com и mail.ru для Хемуля	<input checked="" type="checkbox"/>

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. В основном окне отображаются кнопки «Добавить» и «Удалить», соответственно для добавления и удаления информации об исключениях для авторизации в прокси сервере. А также таблица, содержащая наборы исключений. При добавлении исключения доступны следующие поля:

- «Источник». Позволяет задать в качестве источника трафика IP-адрес или сеть, для которых не будет производиться аутентификация в прокси сервере. Это приведет к тому, что трафик идущий с указанных IP-адреса или сети не будет учитываться в статистике за определенными Пользователями. Но будет учитываться в общей статистике.
- «Назначение». В качестве назначения возможно указывать: IP-адрес; IP/mask; имя домена (например, ya.ru); поддомены исключая основной домен (например, ".google.com" - при обращении на drive.google.com авторизация не будет запрошена, но при обращении на google.com будет запрошена авторизация); регулярное выражение в формате - /regex/gi (например, /.*.ai.\.ru/gi - разрешит домен mail.ru и его поддомены). Правила для заполнения данного поля также распространяются на поля содержащие URL, при создании запрещающего, разрешающего правила или исключения прокси.
- «Описание». Позволяет задать произвольное описание для создаваемого правила.
- «Выкл.». Позволяет выключить созданное правило.

Содержимое кэша

Прокси-сервер Настройки Автоконфигурация Родительский прокси Исключения для авторизации **Кеш** Журнал

Очистить кеш Поиск...

URL	Объем	Последнее обращение
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 15:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 16:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 17:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 18:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 19:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	410	30.10.2019 20:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	414	30.10.2019 21:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	414	30.10.2019 22:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	414	30.10.2019 23:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	414	31.10.2019 00:56:52
http://testics.local:3128/squid-internal-periodic/store_digest	414	31.10.2019 01:56:52

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

Журнал

Прокси-сервер Настройки Автоконфигурация Родительский прокси Исключения для авторизации Кеш **Журнал**

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

↓ ↑

Squid Parent: squid-1 process 8929 exited with status 0
11:57:12

В закладке «Журнал» находится сводка всех системных сообщений от прокси-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, сообщения о состоянии системы (включение/выключение, обработка кэша) - 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.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:proxy>

Last update: **2019/11/22 12:29**



Настройка HTTPS-фильтрации

Для того, чтобы получить возможность фильтровать HTTPS-трафик пользователей, необходимо сделать следующее:

1. Добавить корневой сертификат (CA) со стандартными настройками в модуле [сертификаты](#).

Добавление сертификата

Общее Настройки Использование ключа Netscape расширение

Название *

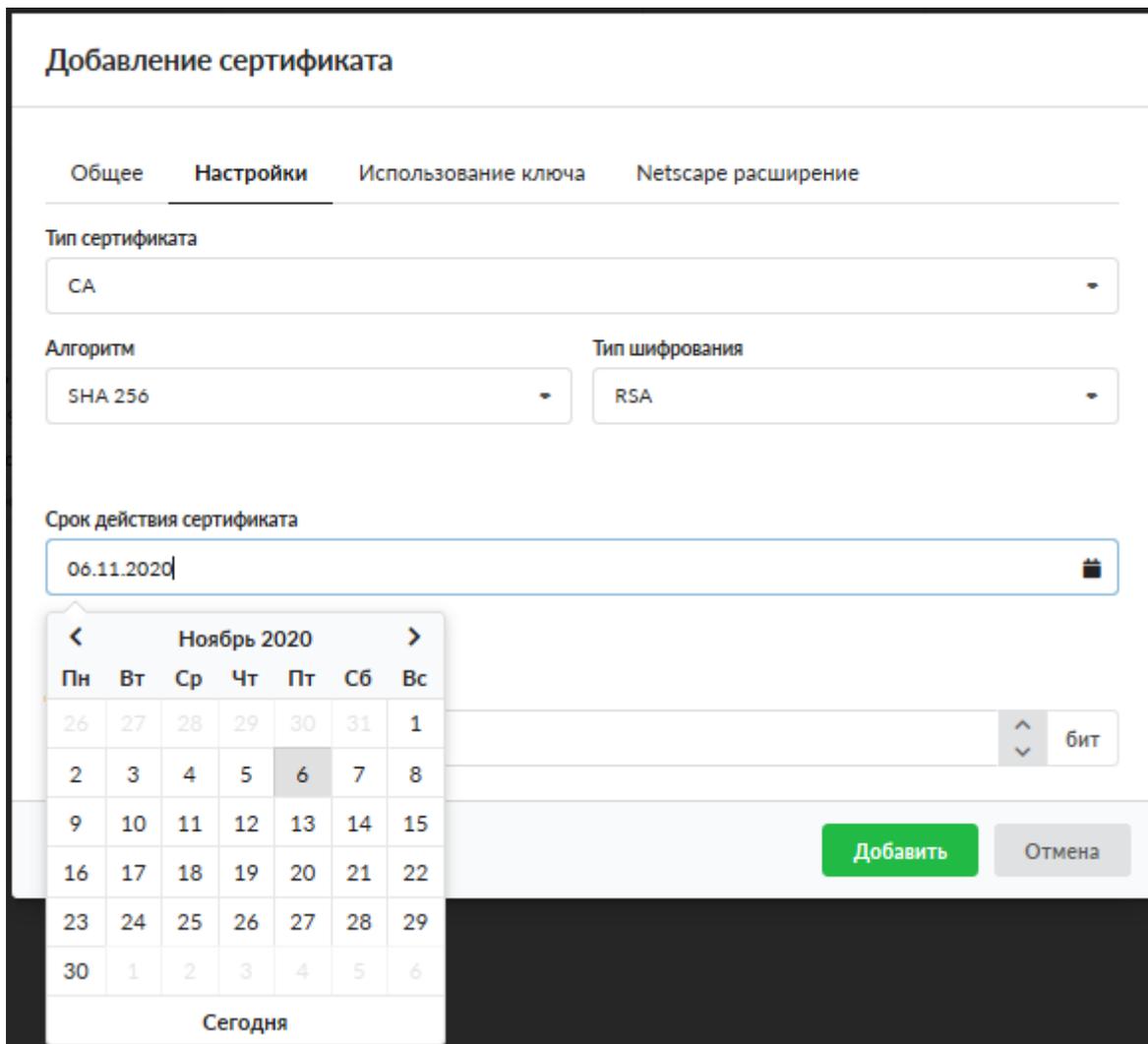
Код страны

Город Область

Организация E-mail

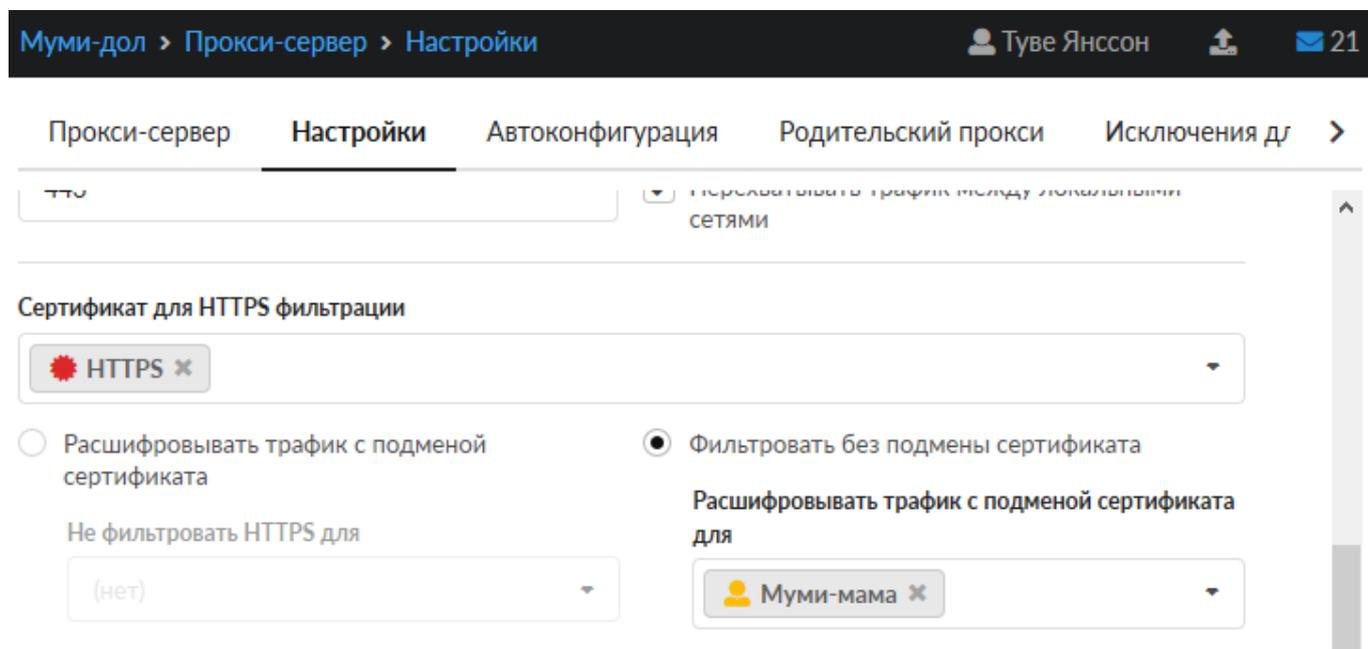
Имя или адрес хоста *

Для того, чтобы сертификат работал длительное время и не было необходимости менять его на конечных пользователях, установите дату окончания сертификата более чем 1 год (по умолчанию). Остальные параметры сертификата оставьте по умолчанию.



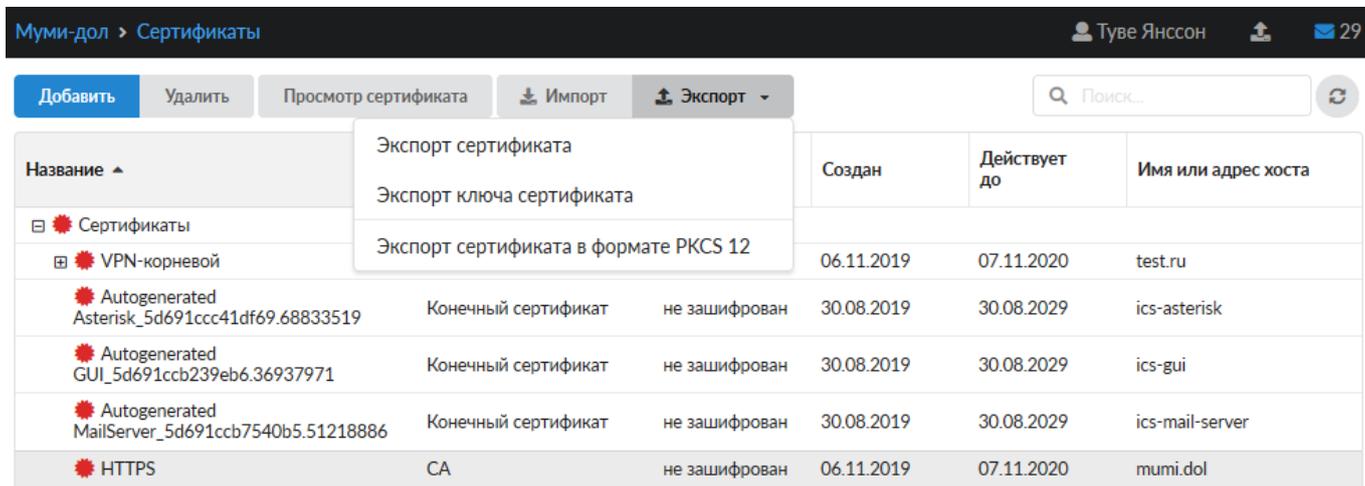
После нажатия кнопки «Добавить» система спросит, нужно ли шифрование ключа. Укажите «Не шифровать закрытый ключ».

2. Выбрать данный сертификат в поле «Сертификат для HTTPS-фильтрации» настроек модуля прокси.



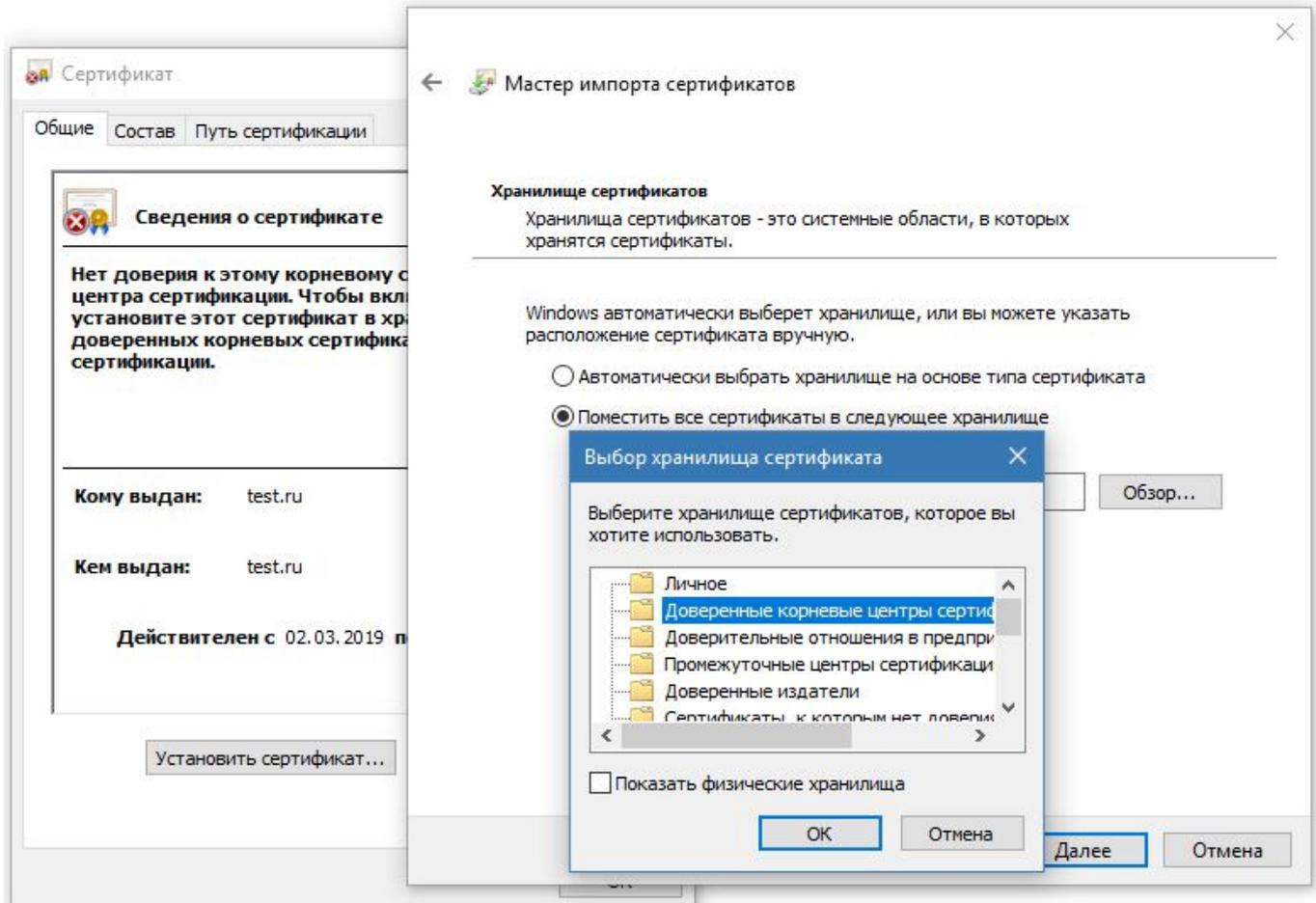
После этого необходимо выбрать один из двух режимов работы фильтрации:

Фильтровать весь HTTPS-трафик с расшифровкой. В этом режиме весь проходящий трафик будет расшифровываться посредством подмены сертификата. После этого правила фильтрации начнут работать, однако в связи с подменой сертификата при запросе браузер пользователя будет сообщать о некорректном сертификате. Чтобы исключить данную ошибку, необходимо сделать следующее:

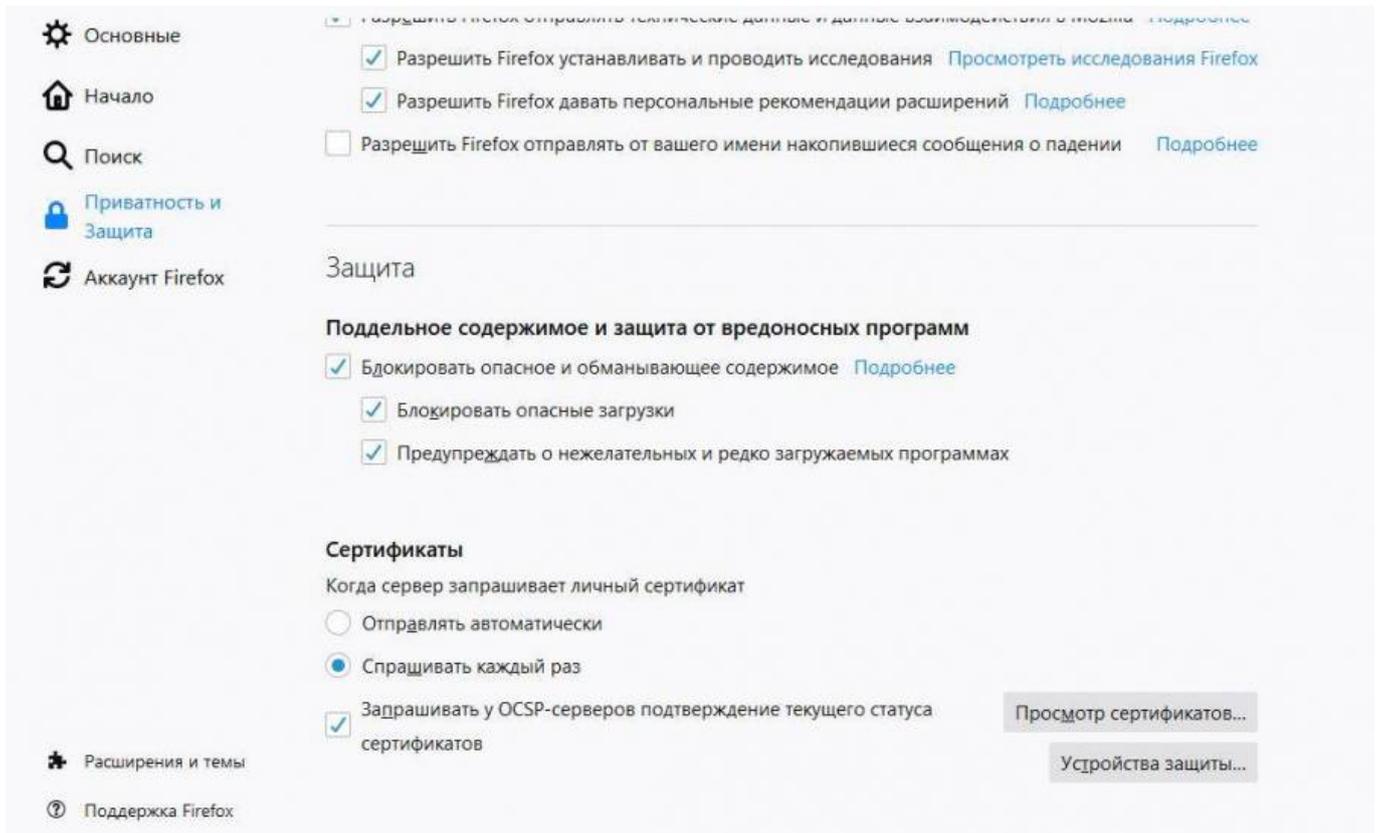


В модуле [сертификаты](#) экспортировать данный сертификат на машину конечного пользователя. Экспорт ключа сертификата не требуется.

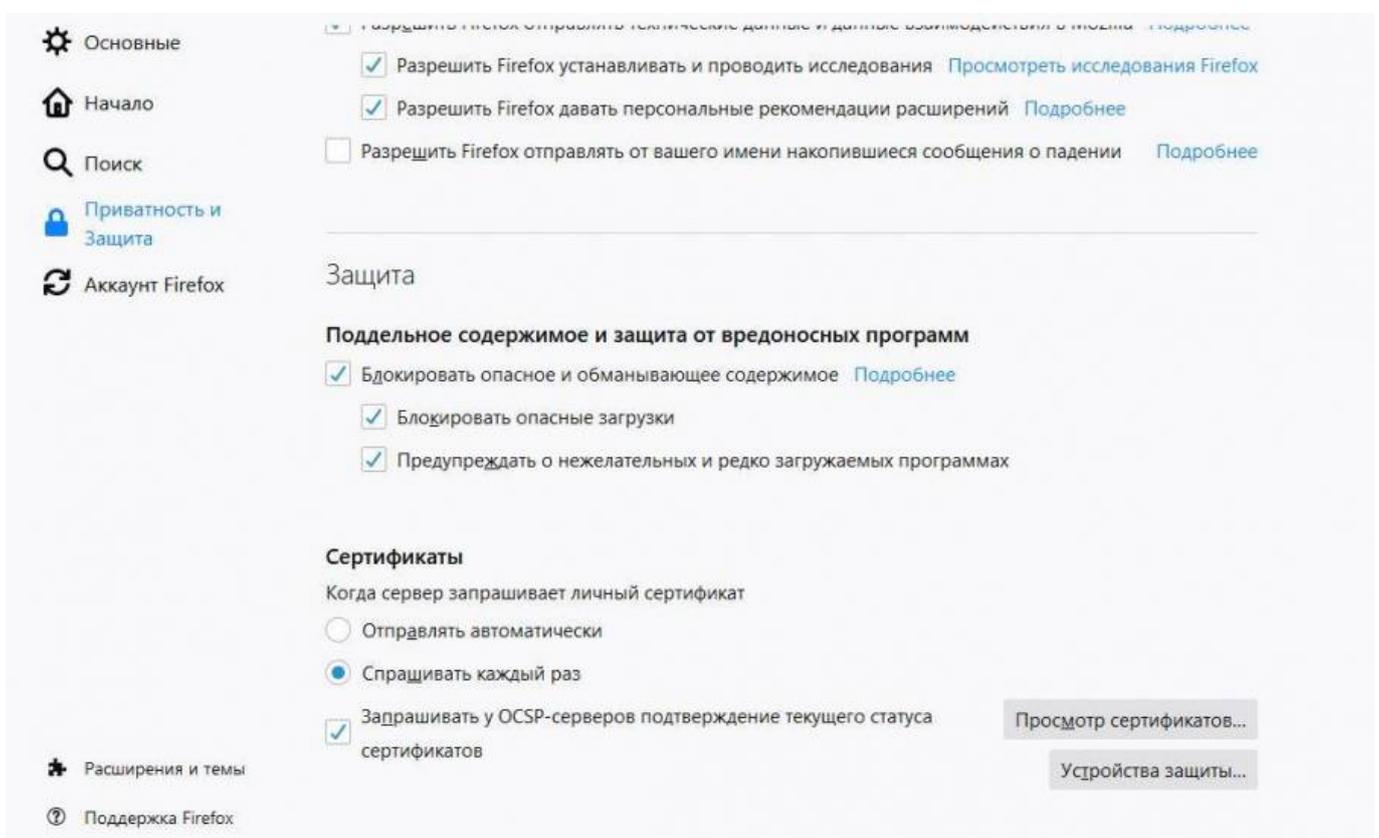
На каждом клиентском компьютере добавить сертификат в доверенные корневые центры сертификации. Это делается следующим образом (на примере Windows 7): дважды кликните на сертификат. Нажмите кнопку «Установить сертификат». Откроется мастер импорта сертификата. Когда мастер спросит выбор места хранения сертификата, выберите «поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и выберите «доверенные корневые центры сертификации».

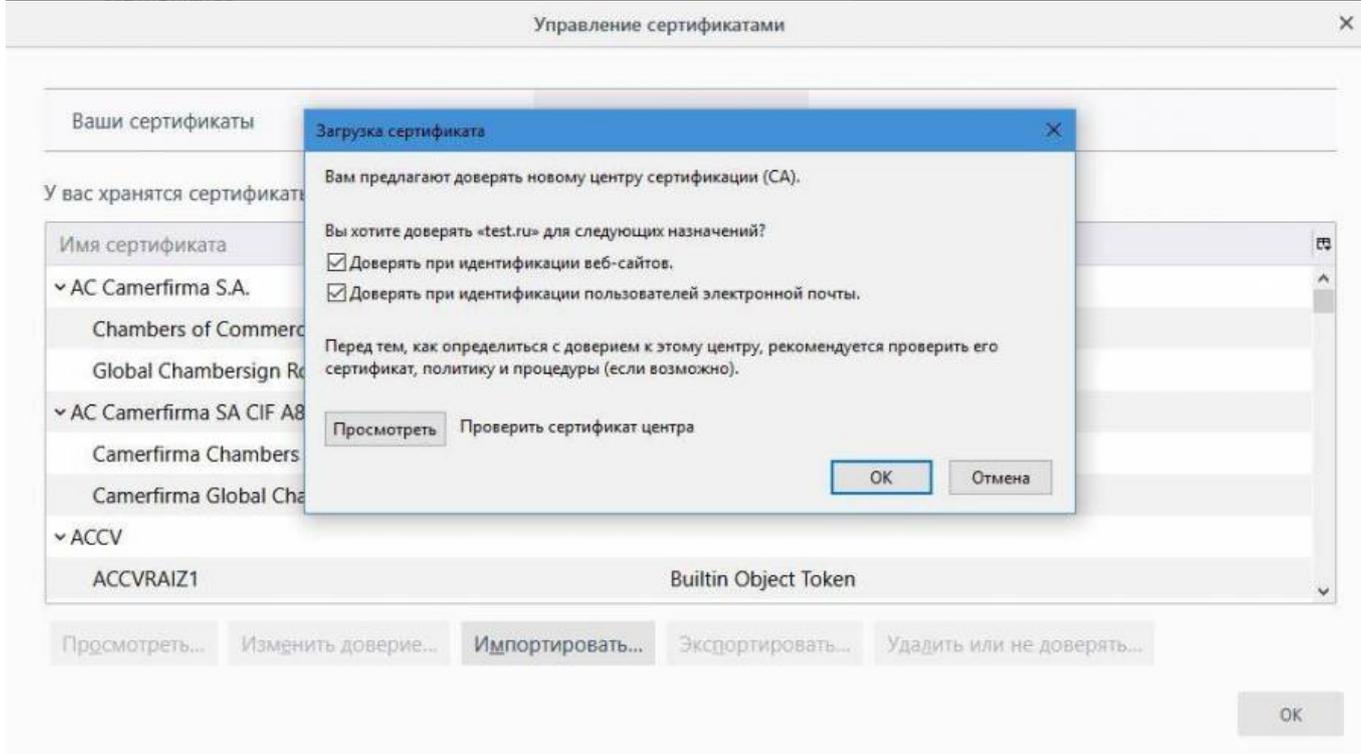
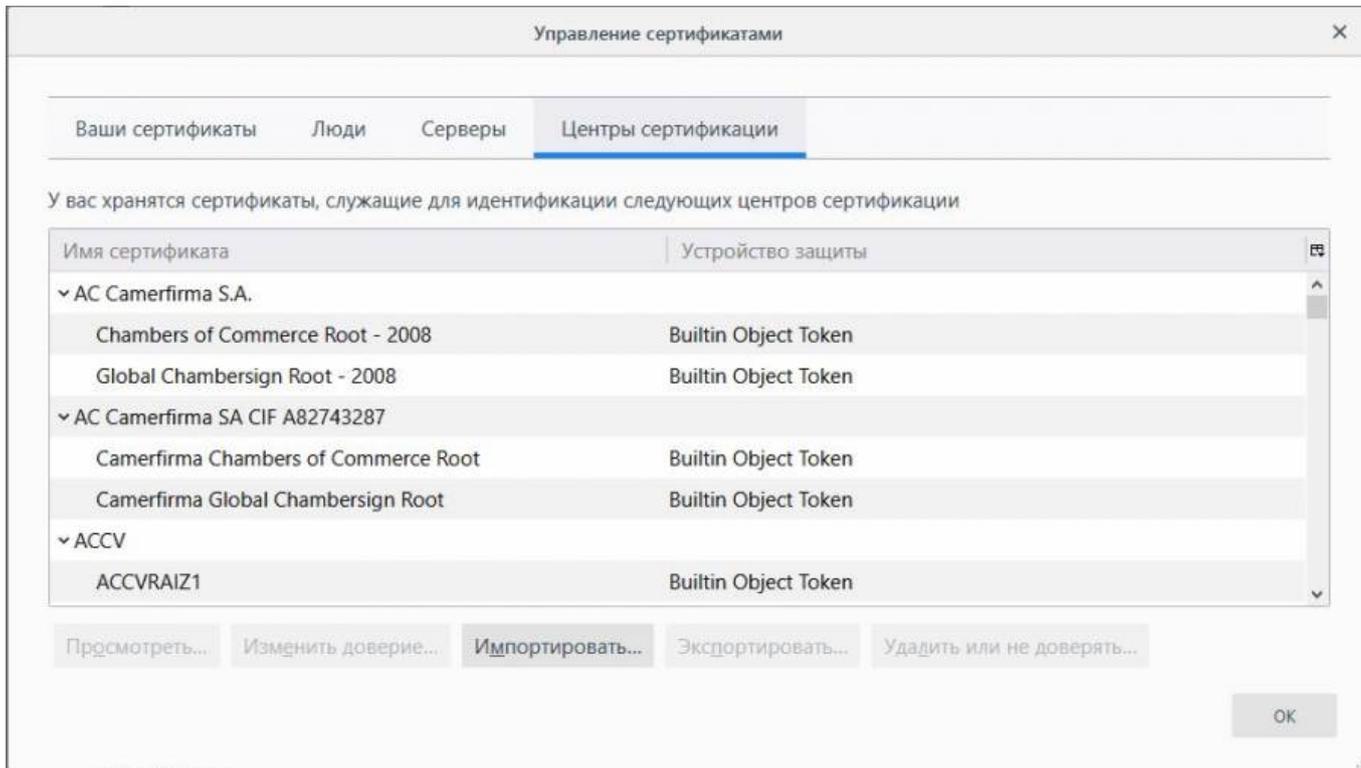


Таким образом, сертификат будет импортирован в глобальное хранилище системы. Он будет работать для тех браузеров, которые используют системные хранилища сертификатов, например, Internet Explorer, Chrome, Yandex. Если же браузер использует собственное хранилище, как, к примеру, Firefox, то импорт необходимо произвести непосредственно в настройках браузера. Это делается следующим образом (для Mozilla Firefox):



Зайдите в настройки браузера, перейдите в Дополнительные - Сертификаты - Просмотр сертификатов - WЦентры сертификации - Импортировать и укажите скачанный с ИКС сертификат.





Отметьте все флажки и импортируйте сертификат.

Для того, чтобы исключить выбранных пользователей или отдельные домены, применяется поле «Исключения». Соединения пользователей, указанных в этом поле не будут расшифровываться и, соответственно, импортировать сертификат для них нет необходимости. Аналогично, соединения на указанные домены также не будут расшифровываться. Добавлять домены может потребоваться для корректной работы безопасных сервисов в проверкой MitM-атак, таких как почтовые или банковские сервисы.

Фильтровать без подмены сертификата. В этом режиме установка сертификата в систему конечного пользователя не требуется. Однако, в данном режиме работы ИКС будет знать

только о домене назначения запроса, а не о полном URL.

Например, если вы хотите заблокировать весь домен yandex.ru, то для этого достаточно настроить фильтрацию в режиме работы без подмены сертификата. Если же вы хотите заблокировать домен yandex.ru, но при этом разрешить адрес yandex.ru/video, то вам потребуется настроить полную подмену сертификата для расшифровки URL назначения.

Также, в данном режиме работы есть возможность настроить отдельные домены либо же отдельных пользователей на полную расшифровку в поле «Фильтровать с расшифровкой». В этом случае импортировать сертификат нужно либо для тех пользователей, которые указаны в поле, либо для всех пользователей, которые будут обращаться к прописанному доменному имени (например vk.com).

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:https>

Last update: **2019/11/10 19:25**



VPN

Модуль «VPN» расположен в Меню «Сеть». Данный модуль предназначен для контроля пользователей, подключающихся по технологии VPN к ИКС. Модуль «VPN» имеет шесть вкладок: «VPN-сервер», «Настройки», «Пользователи», «Текущие сеансы», «События», «Журнал».

Стартовая страница модуля (VPN-сервер)

Ареал Ланк > VPN-сервер Администратор ↑ 15

VPN-сервер Настройки Пользователи Текущие сеансы События Журнал

Служба PPP-соединений запущен
Предоставляет удаленный доступ и обеспечивает подключение PPP-провайдеров

OpenVPN запущен
Отвечает за работу OpenVPN-соединений

Журнал ↓↑ ↻

11:36:37	[L2TP-2] LCP: Close event
11:36:37	[L2TP-2] LCP: state change Stopped --> Closed
11:36:37	[L2TP-2] LCP: Down event
11:36:37	[L2TP-2] LCP: state change Closed --> Initial

Вкладка «VPN-сервер». На данной вкладке отображается состояние служб «Служба PPP-соединений» и «OpenVPN» с возможностью «Выключить» (или «Включить» если служба выключена), а также последние сообщения в журнале за текущий день.

Ареал Ланк > VPN-сервер Администратор ↑ 11

VPN-сервер Настройки Пользователи Текущие сеансы События Журнал

Служба PPP-соединений запущен
Предоставляет удаленный доступ и обеспечивает подключение PPP-провайдеров

Журнал ↻

13:19:29	[PPTP-2] AUTH: ran out of backends
13:19:29	[PPTP-2] CHAP: Auth return status: failed
13:19:29	[PPTP-2] CHAP: Reply message: E=691 R=0 M>Login incorrect
13:19:29	[PPTP-2] CHAP: sending FAILURE #1 len: 31
13:19:29	[PPTP-2] LCP: authorization failed

Настройки

VPN-сервер **Настройки** Пользователи Текущие сеансы События Журнал

Разрешать одновременные подключения под одним пользователем

Автоматически создавать разрешающее правило Автоматически создавать разрешающее правило OpenVPN

Доступ к VPN-серверу

Доступ к L2TP-серверу

Доступ к OpenVPN-сетям

Время ожидания сессии * Время ожидания ответа от RADIUS *

121 ^ сек.

v

3 ^ сек.

v

Вкладка «Настройки» позволяет задать следующие настройки:

- Флаг «разрешать одновременные подключения под одним пользователем»
- Флаг «автоматически создавать разрешающее правило» для доступа к VPN-серверу из внешней сети
- Флаг «автоматически создавать разрешающее правило для IPsec» разрешающее IPsec-шифрование для VPN-подключений
- Поле «время ожидания сессии» позволяет определить время разрыва сессии в случае неактивности пользователя. Данное поле позволяет определить время в секундах, значение по умолчанию - 60 секунд.

Для флагов автоматического создания правил приводятся гиперссылки на соответствующие правила во вкладке «Сеть» → «Межсетевой экран» → «Правила»

Ареал Ланк > VPN-сервер > Настройки Администратор 11

VPN-сервер **Настройки** Пользователи Текущие сеансы События Журнал

Разрешать одновременные подключения под одним пользователем

Автоматически создавать разрешающее правило Автоматически создавать разрешающее правило для IPsec

[Доступ к VPN-серверу](#)

[Доступ к VPN-серверу](#)

[Разрешающее правило для IPsec-шифрования VPN-подключений](#)

[Разрешающее правило для IPsec-данных VPN-подключений](#)

Время ожидания сессии * сек.

60 ^ сек.

v

Пользователи

Вкладка «Пользователи» отображает список пользователей ИКС и позволяет определить, кому разрешены VPN-доступ и OpenVPN-доступ. По умолчанию разрешающие флаги сняты для всех пользователей, которым присвоены адреса из VPN-сети. Разрешить/запретить пользователю доступ, можно установив/сняв соответствующий флаг.

VPN-сервер Настройки **Пользователи** Текущие сеансы События Журнал

Добавить ▾ Удалить Выключить ▾ Редактировать

Имя	Логин ▲	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
[-] Корневая группа			<input type="checkbox"/>	<input type="checkbox"/>
[-] ИКС			<input type="checkbox"/>	<input type="checkbox"/>
[-] Серверная			<input type="checkbox"/>	<input type="checkbox"/>
[-] Манагеры			<input type="checkbox"/>	<input type="checkbox"/>
[-] CloudX			<input type="checkbox"/>	<input type="checkbox"/>
archer	archer	192.168.17.92	<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер впн (10.8.0.0/24)
bender	bender		<input type="checkbox"/>	<input type="checkbox"/>

Ареал Ланк > VPN-сервер > Пользователи Администратор 11

VPN-сервер Настройки **Пользователи** Текущие сеансы События Журнал

Добавить ▾ Удалить Выключить ▾ Редактировать

Имя ▲	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
[-] Корневая группа			<input type="checkbox"/>	<input type="checkbox"/>
[-] CloudX			<input type="checkbox"/>	<input type="checkbox"/>
[-] ИКС			<input type="checkbox"/>	<input type="checkbox"/>
HyperV ICS			<input type="checkbox"/>	<input type="checkbox"/>
morty			<input type="checkbox"/>	<input type="checkbox"/>
Артем Красотин	darkemon		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер впн
Беседин	besco		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Супер впн

В данной вкладке можно добавить нового пользователя, аналогично тому, как это делается во вкладке «Пользователи и статистика» → ["Пользователи"](#).

При выборе определенного пользователя активируются кнопки управления, позволяющие удалить, выключить и редактировать свойства выбранного пользователя. Их действия аналогичны соответствующим кнопками во вкладке «Пользователи и статистика» → ["Пользователи"](#).

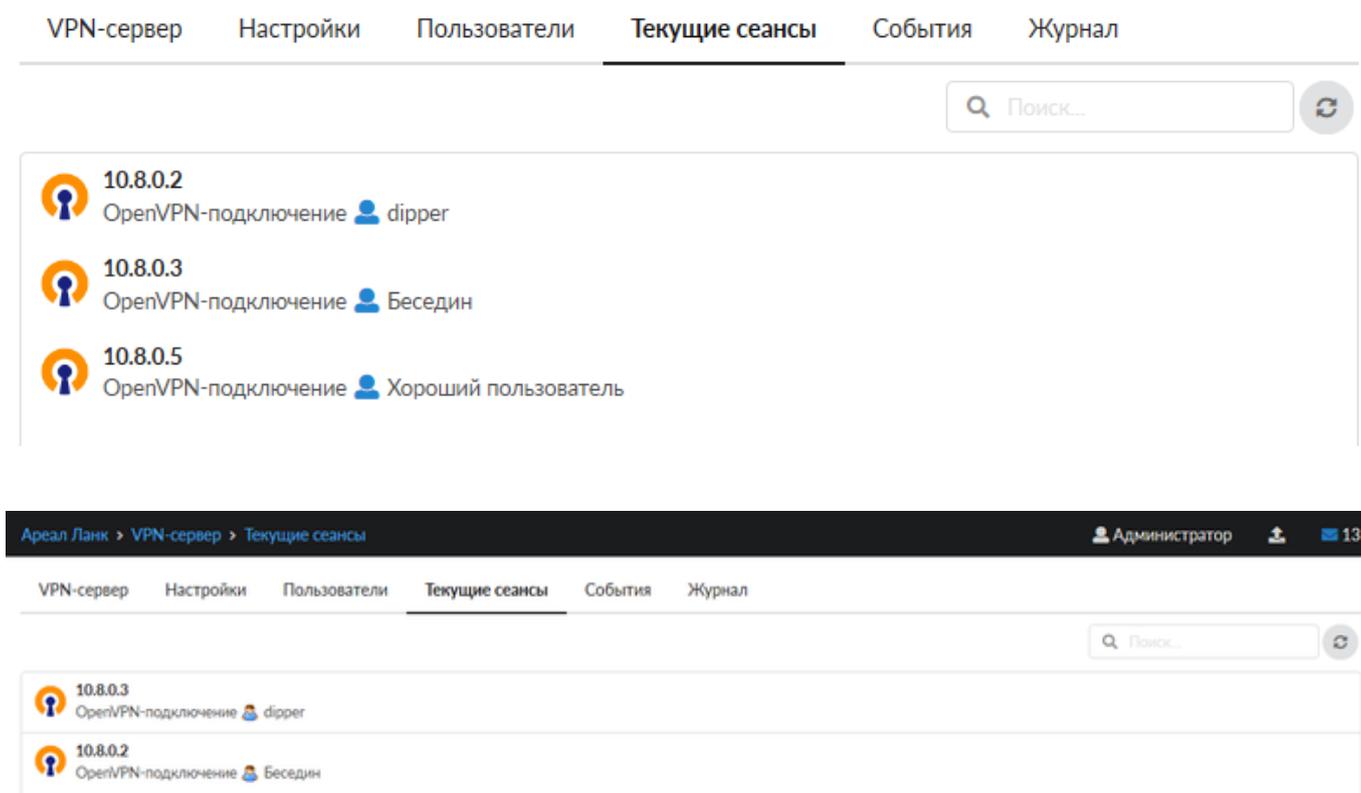
Для предоставления доступа к OpenVPN-сети необходимо напротив соответствующего Пользователя установить флаг в столбце «OpenVPN-доступ», при этом будет открыто новое диалоговое окно, в котором необходимо выбрать соответствующую OpenVPN-сеть. После произведенных манипуляций, у соответствующего Пользователя в индивидуальном модуле во вкладке «OpenVPN», станут доступны дополнительные настройки соединения в OpenVPN-сети. По мимо этого «ИКС» создаст автоматически конечный сертификат для соответствующего Пользователя, с именем имя сети>_<имя Пользователя>. Стоит отметить, что если будет изменен логин Пользователя добавленного в OpenVPN-сеть, то это может привести к нарушению работы «ИКС».

Важно, если Пользователь имеет кириллический логин, то для него не возможно создать сертификат, а значит он не будет подключен к OpenVPN-сети.

Текущие сеансы

В вкладке «Текущие сеансы» можно просмотреть кто из пользователей в настоящее время подключен, увидеть время подключения, а также при необходимости отключить пользователя.

В списке можно видеть [IP-адреса](#) VPN-соединений, тип VPN-соединения и имя пользователя, для которого это соединение создано.



При выборе пользователя отображаются:

- Время подключения - время когда было установлено данное соединение
- Длительность подключения
- IP-адрес и способ его выдачи
- IP-адрес и порт откуда осуществляется соединение
- Кнопка «Прервать соединение» для отключения пользователя

Ареал Ланк > VPN-сервер > Текущие сеансы Администратор 13

VPN-сервер Настройки Пользователи **Текущие сеансы** События Журнал

10.8.0.3
OpenVPN-подключение dipper

Время подключения: 28.05.2019 15:46
Длительность подключения: 2 дня 22 часа 47 минут 1 секунда
Ip-адрес: 10.8.0.3 (выдан динамически)
Удаленный адрес: 92.143.53:4067

[Прервать соединение](#)

10.8.0.2
OpenVPN-подключение Беседин

События

Во вкладке «События» отображается журнал события VPN-соединений. Во вкладке можно выбрать период за который будут отображаться события, тип событий (системные сообщения, сообщения сервисов, ошибки, остальные сообщения).

VPN-сервер Настройки Пользователи Текущие сеансы **События** Журнал

06.11.2019 - 06.11.2019 **Сегодня** Неделя Месяц Другой период ▾

[Экспорт](#) Удалить логи Все сообщения ▾

Пользователь Хороша девочка был подключен к VPN-сети по протоколу L2TP с адреса 37.145.167.157, выдан адрес 192.168.17.94 09:28:39
Пользователь Хорошая девочка был отключен от VPN-сети с адреса 37.145.167.157 Сессия: d41d8cd98f00b204e9800998ecf8427e 09:30:56

Кнопка «Экспорт» позволяет скачать данные журнала событий с виде файла txt.

Журнал событий представляет собой таблицу, состоящую из двух столбцов: «Время» - время наступления события «Сообщение» - описание сообщения

Ареал Ланк > VPN-сервер > События Администратор 13

VPN-сервер Настройки Пользователи Текущие сеансы **События** Журнал

31.05.2019 - 31.05.2019 **Сегодня** Неделя Месяц Другой период ▾

Экспорт Все сообщения ▾ Поиск...

Время	Сообщение
31.05.2019 09:1...	Пользователь Хороший мальчик был подключен к VPN-сети по протоколу PPTP с адреса 16.1.35.6, выдан адрес 192.168.1.10

Журнал

VPN-сервер Настройки Пользователи Текущие сеансы События **Журнал**

06.11.2019 - 06.11.2019 **Сегодня** Неделя Месяц Другой период ▾

Экспорт Удалить логи Поиск...

[PPTP-2] Accepting PPTP connection
00:41:51

[PPTP-2] Link: OPEN event
00:41:51

[PPTP-2] LCP: Open event
00:41:51

[PPTP-2] LCP: state change Initial --> Starting
00:41:51

В закладке «Журнал» находится сводка всех системных сообщений от VPN-сервера. Журнал разделен на страницы, кнопками «вперед» и «назад» осуществляется переход со страницы на страницу, ввод номера страницы в поле позволяет 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 можно искать в журнале нужные записи.

Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, нужно выбрать дату, используя календарь в левом верхнем углу модуля.

31.05.2019 - 31.05.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 Экспорт Удалить логи 

00:02:14	[PPTP-2] Accepting PPTP connection
00:02:14	[PPTP-2] Link: OPEN event
00:02:14	[PPTP-2] LCP: Open event
00:02:14	[PPTP-2] LCP: state change Initial --> Starting
00:02:14	[PPTP-2] LCP: LayerStart
00:02:14	[PPTP-2] PPTP: attaching to peer's outgoing call
00:02:14	[PPTP-2] Link: UP event
00:02:14	[PPTP-2] LCP: Up event
00:02:14	[PPTP-2] LCP: state change Starting --> Req-Sent
00:02:14	[PPTP-2] LCP: SendConfigReq #1
00:02:14	[PPTP-2] ACFCOMP
00:02:14	[PPTP-2] PROTOCOMP
00:02:14	[PPTP-2] MRU 1500
00:02:14	[PPTP-2] MAGICNUM 0xefc457f0
00:02:14	[PPTP-2] AUTHPROTO CHAP MSOFTv2
00:02:14	[PPTP-2] MP MRRU 2048
00:02:14	[PPTP-2] MP SHORTSEQ
00:02:14	[PPTP-2] ENDPOINTDISC [IP Address] ac 4d 4d fd

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:vpn>

Last update: **2019/11/10 19:25**



Настройка подключения OpenVPN.

Для подключения абонентов по протоколу OpenVPN, необходимо следующее:

- Создать корневой и конечный сертификаты в модуле Сертификаты. При создании конечного сертификата на вкладке «Использование ключа» в поле «Шаблон» следует выбрать значение «VPN-сервер».

Данные сертификата VPN-корневой

Общее

Название: VPN-корневой
Код страны: RU - Russian Federation
Имя или адрес хоста: test.ru

Настройки

Тип сертификата: CA
Алгоритм: SHA 256
Тип шифрования: RSA
Создан: 06.11.2019
Действует до: 07.11.2020
Длина ключа: 2048 бит

Использование ключа

Использование ключа: Certificate Sign
CRL Sign

Данные сертификата Openvpn-сервер

Общее

Название: Openvpn-сервер
Код страны: RU - Russian Federation
Имя или адрес хоста: test.ru

Настройки

Тип сертификата: Конечный сертификат
Алгоритм: SHA 256
Тип шифрования: RSA
Создан: 06.11.2019
Действует до: 07.11.2020
Длина ключа: 2048 бит

Использование ключа

Использование ключа: Digital Signature
Key Encipherment

Расширенное использование ключа: TLS Web Server Authentication
Netscape расширение: SSL Server

Ок **Отмена**

- Добавить OpenVPN-сеть в модуле Провайдеры и сети. Для того, чтобы пользователи могли подключаться к ресурсам локальных сетей ИКС, необходимо установить флаг «Передать клиенту маршрут по умолчанию» и выбрать из списка сети, которые нужно маршрутизировать.

Добавление OpenVPN-сети

Основные настройки Шифрование и сертификаты

Название * Ip-адрес/Префикс *

Супер VPN 10.8.0.0/24

Протокол Порт сервера *

UDP 1194

Использовать NAT

Разрешить трафик между клиентами

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

Мульти-локалка (192.168.17.242/24) ✕

Передать клиентам DNS сервера

Передать клиентам DNS сервера

Разрешить управление ИКК через веб

Разрешить управление ИКК через SSH

Добавить Отмена

- В качестве сертификатов указать предварительно сгенерированные сертификаты из п.1.

Добавление OpenVPN-сети

Основные настройки Шифрование и сертификаты

Алгоритм шифрования: AES-256-CBC Алгоритм хеширования: SHA256

Включить сжатие LZO

link-MTU *: 1500

Корневой сертификат *: VPN-корневой ✕ Сертификат сервера *: Openvpn-сервер ✕

Добавить Отмена

- Перейти в модуль VPN - Пользователи и отметить флажками пользователей, которым будет разрешено подключаться по протоколу OpenVPN, при этом будет предложено выбрать к какой из созданных сетей (если их несколько) будет подключаться пользователь. Важно: необходимо нажать кнопку «Сохранить», чтобы изменения вступили в силу.

Муми-дол > VPN-сервер > Пользователи Туде Янссон 19

VPN-сервер Настройки **Пользователи** Текущие сеансы События Журнал

Добавить Удалить Выключить Редактировать

Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ
Корневая группа			<input type="checkbox"/>	<input type="checkbox"/>
Муми-дол			<input type="checkbox"/>	<input type="checkbox"/>
Мумики			<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-мама	mumi3		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-папа	mumi2		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Муми-троль (месячная квота исчерпана)	mumi1		<input type="checkbox"/>	<input checked="" type="checkbox"/> Супер VPN (10.8.0.0/24)
Снорки			<input type="checkbox"/>	<input type="checkbox"/>

Сохранить Обновить

- Перейти в индивидуальный модуль пользователя, вкладка OpenVPN. Если необходимо настроить маршрутизацию из локальной сети ИКС до других ресурсов в локальной сети

пользователя, то необходимо прописать сеть, в которой находится данный пользователь.

- В модуле Провайдеры и сети необходимо выгрузить клиентские сертификаты для подключения пользователей

- Для подключения пользователя, ему необходимо установить на своем компьютере утилиту OpenVPN (<https://openvpn.net/>), после чего распаковать содержимое папки с именем пользователя из архива выгруженных сертификатов в папку <путь до установки>\config, запустить утилиту и выполнить подключение.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:openvpn_setup

Last update: **2019/11/10 19:25**



ARP-таблица

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.

Муми-дол > ARP-таблица Туге Янссон 45

ARP-таблица Журнал

Добавить Удалить Поиск...

IP-адрес	MAC-адрес	Привязка mac к ip
00:50:56:8e:59:43 192.168.170.246 Ip и mac адрес		
00:50:56:8e:ef:70 192.168.170.242 Ip и mac адрес		привязан к ip
74:d4:35:3b:0e:2f 192.168.17.43 Хемуль		
00:50:56:8e:d0:91 192.168.17.242 Ip и mac адрес		привязан к ip

В большинстве случаев в 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-адресом». Если компьютер пользователя уже есть в списке, и ему назначен желаемый IP - необходимо просто нажать кнопку «Связать IP с MAC». Аналогичную операцию можно сделать и в списке IP-адресов пользователя.

Добавление записи

Ip-адрес *	Mac-адрес *
<input type="text" value="192.168.1.1"/>	<input type="text" value="0a:1b:2c:3d:4e:5f"/>
<input checked="" type="checkbox"/> Связать ip с mac	
Комментарий	
<input type="text" value="Связываем ip-адрес и mac-адрес"/>	

Если IP адрес сопоставлен пользователю ИКС, то в строке с соответствующим IP будет показано его имя. По клику на имени пользователя, произойдет переход в на его страницу.

Сопоставления из ARP-таблицы также используется [DHCP-сервером](#). Именно по MAC-адресу DHCP-сервер определяет, какой IP адрес назначить сетевому устройству.

Примечание. Если в ARP-таблице Пользователю был определен, например, MAC-адрес 0a:1b:2c:3d:4e:5f и соответствующий ему IP-адрес 192.168.1.1. И через некоторое время IP-адрес был изменен на другой, например на 10.0.0.1, то в «ИКС» для данного Пользователя будет отображаться два IP-адреса связанных с одним 0a:1b:2c:3d:4e:5f, так как в системной таблице ARP будут существовать обе записи. Не корректная запись в ARP-таблице, будет удалена автоматически не позднее 1200 секунд.

Журнал

В закладке «Журнал» находится сводка всех системных сообщений от службы. 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) - 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».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:arp>

Last update: **2019/11/10 19:25**



Отказоустойчивость

Настройка CARP

CARP (от англ. Common Address Redundancy Protocol — протокол дубликации общего адреса) — сетевой протокол, основной задачей которого является использование одного IP-адреса несколькими хостами в пределах сегмента сети.

С помощью CARP сервера объединяются в виртуальную группу (VHID), которой назначается виртуальный IP-адрес (Virtual IP), которому протокол CARP выделяет виртуальный mac-адрес. Виртуальный IP-адрес должен использоваться в качестве шлюза по умолчанию на клиентских хостах в локальной сети. В пределах группы один из серверов становится «главным» (MASTER), а остальные обозначаются как «резервные» (BACKUP). Каждый сервер одновременно может принадлежать к нескольким виртуальным группам. В случае отказа сервера, выполняющего роль мастера, среди резервных серверов будет выбран новый мастер, который примет виртуальный IP-адрес и продолжит обслуживание клиентов. Дизайн CARP требует, чтобы члены одной виртуальной группы физически находились в одной подсети.

Для активации CARP в локальной сети нужно в свойствах локальной сети в модуле «Провайдеры и сети» установить флаг «Использовать CARP».

Добавление локальной сети

Общие настройки **CARP**

Использовать CARP

Virtual IP *

VHID

Пароль *

Advertisement base сек.

Advertisement skew 1/256 сек.

Virtual IP - IP-адрес виртуальной группы. Адрес должен быть уникальным и входить в ту же

сеть, что задана в настройках локальной сети.

VHID (Virtual Host ID) - идентификатор, используемый для объединения нескольких серверов в одну виртуальную группу (любое значение от 1 - 254). В пределах одного сервера на разных интерфейсах должны использоваться разные VHID, чтобы избежать конфликта виртуальных mac-адресов.

Виртуальный mac-адрес создается автоматически следующим образом: 00:00:5e:00:XX, где XX - VHID, записанный в шестнадцатеричной системе счисления (например, VHID=1, mac - 00:00:5e:00:01, VHID=254, mac - 00:00:5e:00:FE).

Пароль - используется для аутентификации сервера в виртуальной группе. На всех серверах в одной группе должен быть указан одинаковый пароль.

Advertisement base и Advertisement skew - параметры, используемые для определения, как часто сервер рассылает CARP-сообщения. Advertisement base измеряется в секундах и указывает основной интервал между анонсами CARP-сообщений. Advertisement skew измеряется в 1/256 секунды, это значение прибавляется к основному интервалу анонсов и используется, чтобы сделать рассылку CARP-сообщений чуть медленнее, чем на других серверах.

С помощью этих параметров можно указать, какой сервер будет мастером в виртуальной группе. Например: есть два сервера А (VHID 1) и В (VHID 1). Нам нужно, чтобы сервер А по умолчанию был мастером. Тогда выполняем следующие настройки:

```
сервер А: Advertisement base = 1 Advertisement skew = 100
сервер В: Advertisement base = 1 Advertisement skew = 200
```

Сервер А будет быстрее рассылать CARP-сообщения, поэтому первым станет мастером.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:cluster>

Last update: **2019/11/10 19:25**



Удалённое управление

Модуль «Удаленное управление» расположен в Меню «Сеть». Данный модуль позволяет из web-интерфейса главного «ИКС» заходить по защищённому каналу на web-интерфейсы подчиненных «ИКС». На основной вкладке модуля отображается: состояние модуля (не настроен / запущен / остановлен); кнопка «Включить» / «Выключить»; а также журнал с последними системными сообщениями от модуля.

Муми-дол > Удаленное управление Туве Янссон 59

Удаленное управление | Настройки | Узлы | Журнал

Удаленное управление запущен
Удаленное управление ИКС Выключить

Журнал ↓↑ ↻

- started
13:16:05
- connecting to 192.168.17.246:49494 ...
13:16:05
- ebus client [skyd-client] connected
13:16:05
- dial tcp 192.168.17.246:49494: connect: operation timed out
13:17:20
- dial tcp 192.168.17.246:49494: connect: operation timed out
13:18:40

Настройки

Удаленное управление **Настройки** Узлы Журнал

Использовать удаленное управление

Корневой сертификат * Сертификат *

VPN-корневой x remote-сервер x

Режим:

Сервер

Автоматически создавать разрешающее правило

Доступ для удаленного управления

Клиент

Если поле пустое, то будет сгенерирован новый ID

ID

node-5LWji2TX

IP сервера *

192.168.17.246

Флаг «Использовать удаленное управление» позволяет устанавливать использование удаленного управления и производить соответствующие настройки. Если установлен данный флаг, то предлагается выбрать режим работы «ИКС» - «Сервер» или «Клиент», а также установить корневой и конечный сертификаты из модуля «Сертификаты». Если выбрать режим «Сервер», то данный «ИКС» будет выступать в роли сервера, а остальные «ИКС» будут подключаться к нему. Также станет доступен флаг «Автоматически создавать разрешающее правило» для создания разрешающего правила в наборе правил межсетевого экрана. Если выбрать режим «Клиент», то данный «ИКС» будет выступать в роли клиента и им можно будет управлять с «ИКС», который выступает в роли сервера. По мимо этого станут доступными поля «ID» и «IP сервера» для заполнения. В поле «ID» указывается уникальный идентификатор клиента, генерируемый автоматически (но его можно изменить), в формате «node-*****», где '*' – это цифра или любой латинский символ (поле регистр зависимое). В поле «IP сервера» может указываться как IP-адрес, так и доменное имя сервера.

В общем случае, для функционирования удаленного управления, необходимо создать три сертификата на «ИКС» с ролью «Сервер»: Корневой Сертификат, Конечный Сертификат для Сервера, Конечный Сертификат для Клиента. Далее создание сертификатов рассматривается через модуль «Сертификаты» в «ИКС».

При создании Корневого Сертификата его тип должен быть «CA».

При создании Конечного Сертификата для Сервера в поле «Имя или адрес хоста» должно быть

указано или доменное имя системы или внешний IP-адрес «ИКС» с ролью «Сервер», тип сертификата должен быть «Конечный сертификат», в качестве шаблона рекомендуется выбрать «VPN-сервер».

При создании Конечного Сертификата для Клиента указывается тип сертификата «Конечный сертификат», а в качестве шаблона рекомендуется выбрать «VPN-клиент».

Соответственно на «ИКС» с ролью «Сервер» размещаются сертификаты: Корневой Сертификат и Конечный Сертификат для Сервера. А на «ИКС» с ролью «Клиент» сертификаты: Корневой Сертификат и Конечный Сертификат для Клиента (рекомендуется экспорт сертификатов производить в формате PKCS 12). В связи с особенностью реализации TLS, существует два режима взаимодействия между клиентом и сервером:

1. Частично защищенный. Если на «ИКС» с ролью «Клиент» в Удалённом управлении во вкладке «Настройки» в поле «IP сервера» указать IP-адрес, то защита канала будет односторонней. Т.е. «ИКС» с ролью «Клиент» не будет проверять сертификат «ИКС» с ролью «Сервера», при этом «Сервер» будет проверять «Клиентский» сертификат. Данная особенность открывает доступ к атаке Man-In-The-Middle (MITM), в которой злоумышленник может подменить сертификат «Сервера» и перехватывать трафик.
2. Полная защита. Для обеспечения полной защиты необходимо:
 - При создании Конечного Сертификата для Сервера в поле «Имя или адрес хоста» указать ИМЯ_ХОСТА.
 - На «ИКС» с ролью «Клиент» создать DNS-зону для ИМЯ_ХОСТА, которая будет ссылаться на IP-адрес «Сервера».
 - На «ИКС» с ролью «Клиент» в Удаленном управлении во вкладке «Настройки» в поле «IP сервера» указать ИМЯ_ХОСТА. При таком взаимодействии «Клиента» с «Сервером», обе стороны проверяют передаваемые сертификаты, а атака MITM не возможна.

Узлы

Удаленное управление	Настройки	Узлы	Журнал
----------------------	-----------	-------------	--------

Редактировать	Удалить				
---------------	---------	--	--	--	--

Имя ▾	ID	IP-адрес	Статус	Описание
-------	----	----------	--------	----------

В «ИКС» с ролью «Сервер» на данной вкладке содержится перечень всех «ИКС» с ролью «Клиент», которые были подключены к удаленному управлению. Перечень представлен в виде таблицы со столбцами:

- Имя. По умолчанию устанавливается из столбца ID. Является изменяемым полем. - ID. Содержит уникальный идентификатор, заданный на «ИКС» с ролью «Клиент». - IP-адрес. Содержит IP-адрес «ИКС» с ролью «Клиент». - Статус. Содержит значение подключен/ не

подключен. - Описание. По умолчанию пустое поле, предназначено для занесения пометок от системного Администратора.

Кнопка «Редактировать» - позволяет редактировать доступные значения в столбцах таблицы. Кнопка «Удалить» удаляет информацию о подключенном «ИКС» к удаленному управлению. Для перехода в GUI удаленного «ИКС» необходимо дважды кликнуть по его записи в таблице.

Журнал

Удаленное управление Настройки Узлы **Журнал**

06.11.2019 - 06.11.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

started 13:16:05
connecting to 192.168.17.246:49494 ... 13:16:05
ebus client [skyd-client] connected 13:16:05

В закладке «Журнал» отображается сводка 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:remote_control

Last update: **2019/11/10 19:25**



Антивирус ClamAV

Модуль «Антивирус ClamAV» расположен в Меню «Защита». Данный модуль предназначен для защиты от проникновения вредоносных программ в локальную сеть. Модуль «Антивирус ClamAV» имеет три вкладки: «Антивирус ClamAV», «Настройки», «Журнал».

Антивирус ClamAV

Антивирус ClamAV Настройки Журнал

 **Антивирус ClamAV**
Блокирует вирусы запущен

Количество сигнатур: 4566249(main), 1964249(daily), 94(byte)
Версия баз: 58(main), 25618(daily), 331(byte)
Версия: 0.101.4
Последнее обновление: 30.10.2019 11:54:22

Обновить сейчас Выключить

 **Антивирусный прокси-сервер**
Проверяет HTTP-трафик на наличие вирусов запущен

Выключить

Журнал ↓↑ ↻

daily.cvd updated (version: 25618, sigs: 1964249, f-level: 63, builder: raynman)
17:27:26

Can't query daily.25618.105.1.0.6810DA54.ping.clamav.net
17:27:27

Downloading bytecode.cvd [100%]
17:27:27

bytecode.cvd updated (version: 331, sigs: 94, f-level: 63, builder: anvillag)
17:27:28

Can't query bytecode.331.105.1.0.6810DA54.ping.clamav.net
17:27:28

Database updated (6530592 signatures) from db.ru.clamav.net (IP: 104.16.218.84)
17:27:33

Clamd successfully notified about the update.
17:27:57

Вкладка «Антивирус ClamAV». На данной вкладке отображается состояние служб «Антивирус ClamAV» и «Антивирусный прокси-сервер» с возможностью «Выключить» (или «Включить» если служба выключена). Служба «Антивирус ClamAV» отвечает за работоспособность предустановленного антивируса ClamAV, который проверяет почтовые письма, если установлен [соответствующий флаг](#), а также трафик HTTP и HTTPS, при условии запущенной службы «Антивирусный прокси-сервер» и [установленного флага](#) в настройках прокси-сервера. Соответственно служба «Антивирусный прокси-сервер» отвечает за передачу HTTP/HTTPS пакетов антивирусу ClamAV, при условии установленного флага в настройках прокси-сервера. В виджете службы «Антивирус ClamAV», также отображается: количество имеющихся сигнатур, текущие версии базы и антивируса ClamAV, время последнего обновления баз, кнопка «Обновить сейчас». Также последние события журнала за текущую дату.

Настройки

Антивирус ClamAV **Настройки** Журнал

- Использовать в прокси Проверять почту
- Обновлять вирусные базы при выключенном антивирусе

Проверять наличие обновлений вирусных баз

Каждые 3 часа ▼

День недели

- Пн
- Вт
- Ср
- Чт
- Пт
- Сб
- Вс

Время

00:00 📅

Следующая проверка 30.10.2019, 18:00:00

Сохранить Обновить

Вкладка «Настройки». Данная вкладка предназначена для настройки работы антивируса ClamAV. Флаги «Использовать в прокси» и «Использовать в почте» соответствуют соответствующим флагам в настройках модулей «Прокси» и «Почта». Данные флаги включают антивирус ClamAV для фильтрации трафика, проходящего через прокси-сервер и вложения в почтовых письмах. Поле «Проверять наличие обновлений вирусных баз» позволяет задать частоту проверок обновлений баз антивируса. По умолчанию этот процесс будет запускаться каждый час, при условии установленного хотя бы одного флага на данной вкладке. При выборе периода «Каждый день» или «Раз в неделю», возможно указать «Время начала проверки». Флаг «Обновлять вирусные базы при выключенном антивирусе» позволит запускать проверку обновления баз при выключенной службе «Антивирус ClamAV».

Журнал

Антивирус ClamAV Настройки **Журнал**

30.10.2019 - 30.10.2019 Сегодня Неделя Месяц Другой период ▼ ↻

📄 Экспорт Удалить логи

Поиск... 🔍

↓ ↑
daily.cvd updated (version: 25618, sigs: 1964249, f-level: 63, builder: raynman) <small>17:27:26</small>
Can't query daily.25618.105.1.0.6810DA54.ping.clamav.net <small>17:27:27</small>
Downloading bytecode.cvd [100%] <small>17:27:27</small>
bytecode.cvd updated (version: 331, sigs: 94, f-level: 63, builder: anvilleg) <small>17:27:28</small>
Can't query bytecode.331.105.1.0.6810DA54.ping.clamav.net <small>17:27:28</small>
Database updated (6530592 signatures) from db.ru.clamav.net (IP: 104.16.218.84) <small>17:27:35</small>
Clamd successfully notified about the update. <small>17:27:37</small>

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «Антивирус

ClamAV» 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) - 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».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:clamav>

Last update: **2019/11/10 19:25**



Антиспам Касперского

Модуль «Антиспам Касперского» расположен в Меню «Защита» и в Меню «Почта». Антиспам проверяет на спам входящие и исходящие почтовые сообщения и сортирует их в соответствии с установленными параметрами. Модуль «Антиспам Касперского» имеет три вкладки: «Антиспам Касперского», «Настройки», «Журнал».

Антиспам Касперского

The screenshot shows the Kaspersky Anti-Spam interface. At the top, there is a navigation bar with 'ИКС > Почта > Антиспам Касперского' on the left and 'Администратор' with a user icon and '17' on the right. Below the navigation bar are three tabs: 'Антиспам Касперского', 'Настройки', and 'Журнал'. The 'Антиспам Касперского' tab is active, displaying the service status as 'запущен' (running). It shows the version '6.0.0.281', the license expiration date '19.04.2020', and the last database update '09.09.2019 14:29:00'. A 'Выключить' (Turn off) button is visible. Below this is the 'Журнал' (Log) section, which contains a list of events: 'started' at 15:37:58, 'start initialization ...' at 15:37:58, 'databases not found' at 15:38:01, 'trying to update databases' at 15:38:01, 'update success' at 15:40:03, and 'auto databases update every 300 seconds' at 15:40:31. There are navigation icons for the log, including arrows and a refresh icon.

На первой вкладке модуля отображается состояние службы, кнопка «Выключить» (или «Включить» если служба выключена), Служба «Антиспам Касперского» отвечает за работоспособность предустановленного Антиспам Касперского, который проверяет почтовые письма. В виджете службы «Антиспам Касперского», также отображается: текущие версии базы и антиспама Касперского, дата истечения лицензии и последние события журнала за текущую дату.

Важно: по умолчанию служба находится в состоянии «не настроен». Чтобы активировать ее, отметьте в настройках почты флажок «Использовать Антиспам Касперского». Конечно, при этом у вас должен быть приобретен лицензионный ключ.

Настройки

ИКС > Почта > Антиспам Касперского > Настройки Администратор 1

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

Проверять почту

- Перенаправлять спам в папку СПАМ

Проверять наличие обновлений баз антивируса

Каждые 5 минут (рекомендуется)

Время ожидания ответа *

6000

- Предоставлять статистическую информацию в Kaspersky Lab
- Проверять репутацию IP
- Использовать облачные технологии детектирования спама (UDS, SURBL, репутация URL)

Если эта опция отключена, то запросы к облачным сервисам Kaspersky Lab не производятся. Эта опция отключает использование списков SURBL (списки по умолчанию и пользовательские списки).

Размер кэша для облачных сервисов Kaspersky Lab (КБ) *

30720

Сохранить Обновить

Менеджер лицензий позволяет загружать и просматривать сведения о файле лицензии программы.

Флаг **«Проверять почту»** активирует проверку почтовых сообщений на спам.

Флаг **«Перенаправлять спам в папку СПАМ»** включает автоматическое перенаправление писем, содержащих спам, в соответствующую папку. Без этого флага письмам будет только добавляться в тему слово «СПАМ».

Проверять наличие обновлений баз данных антиспама задает период обновления баз антивируса.

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

- Сканировать сообщения на спам
 - Применять лингвистический анализ к сообщению
 - Использовать метод детектирования спама DMARC (комбинация SPF и DKIM)
 - Использовать технологию детектирования спама на основе DNS
 - Использовать списки SURBL и DNSBL

Если определены пользовательские списки DNSBL и SURBL, то они используются вместо списков по умолчанию

Список адресов сервиса SURBL

Список адресов сервиса DNSBL

- Использовать технологию детектирования спама Анти-Фишинг
- Использовать сервис Enforced Anti-Spam Updates (EASUS)
- Использовать технологию детектирования спама Распознавание Изображений
- Анализировать сообщения на ненормативную лексику
- Анализировать сообщения с кодировкой восточных языков
- Анализировать сообщения с кодировкой на кириллице

Указанные опции позволяют определить параметры проверки писем на спам.

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

Белый список IP адресов

Добавить Удалить

Белый список фраз

Добавить Удалить

Белый список E-mail адресов

Добавить Удалить

Чёрный список IP адресов

Добавить Удалить

Чёрный список фраз

Добавить Удалить

Чёрный список E-mail адресов

Добавить Удалить

Сохранить Обновить

Так же на этой вкладке можно настроить вручную **белые** и **чёрные** списки почтовых доменов, ip-адресов и ключевых фраз, содержащихся в сообщении.

Журнал

09.09.2019 - 09.09.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 **Экспорт** Удалить логи 

started 15:37:58
start initialization ... 15:37:58
databases not found 15:38:01
trying to update databases 15:38:01
update success 15:40:03
auto databases update every 300 seconds 15:40:31
initialization success 15:40:31
EbusClient: connected

« < Стр 1 из 1 > » Показаны записи 1 - 8 из 8

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, сообщения о состоянии системы (включение/выключение) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**»

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:kastiel>

Last update: **2019/11/10 19:25**



Антивирус Касперского

Модуль «Антивирус Касперского» расположен в Меню «Защита». Данный модуль предназначен для защиты от проникновения вредоносных программ в локальную сеть. Модуль «Антивирус Касперского» имеет четыре вкладки: «Антивирус Касперского», «Настройки», «События», «Журнал».

Антивирус Касперского

The screenshot shows the Kaspersky Antivirus control panel. At the top, there is a navigation bar with the text "ИКС > Антивирус Касперского" and a user profile "Администратор" with a notification icon showing "8". Below the navigation bar are four tabs: "Антивирус Касперского", "Настройки", "События", and "Журнал". The "Антивирус Касперского" tab is active, displaying the service status as "запущен" (running). The service description is "Блокирует вирусы, проверяет почту и HTTP-трафик на наличие вирусов". Below this, the version is "8.5.1.83", the license expires on "23.11.2020", and the database version is "05092019 0746". A "Выключить" (Turn off) button is visible. The "Журнал" (Log) tab is also visible, showing a list of events with timestamps and descriptions, such as "run service", "started", "KavService: start initialization", "EbusClient: connected", "reload", and "KavService: initialization success".

На первой вкладке модуля отображается состояние службы «Антивирус Касперского» с возможностью «Выключить» (или «Включить» если служба выключена). Служба «Антивирус Касперского» отвечает за работоспособность предустановленного Антивируса Касперского, который проверяет почтовые письма, если установлен [соответствующий флаг](#), а также трафик HTTP и HTTPS, [установленного флага](#) в настройках прокси-сервера. В виджете службы «Антивирус Касперского», также отображается: текущие версии базы и антивируса Касперского, дата истечения лицензии и последние события журнала за текущую дату.

Важно: по умолчанию служба находится в состоянии «не настроен». Чтобы активировать ее, отметьте в настройках прокси-сервера флажок «Использовать антивирус Касперского». Конечно, при этом у вас должен быть приобретен лицензионный ключ.

Настройки

ИКС > Антивирус Касперского > Настройки Администратор 11

Антивирус Касперского **Настройки** События Журнал

Менеджер лицензий Установлено лицензий: 1

Использовать в прокси Проверять почту

Расширенное журналирование событий

Внимание! Расширенное журналирование значительно нагружает систему.

Обновлять базы при выключенном антивирусе

Проверять наличие обновлений баз антивируса

Раз в неделю

День недели Время

Пн Вт Ср Чт Пт Сб Вс 03:00

Следующее обновление баз: 09.09.2019, 03:00:00

Сохранить Обновить

Данная вкладка предназначена для настройки работы антивируса Касперского.

Менеджер лицензий позволяет загружать и просматривать сведения о файле лицензии антивируса.

Флаги **«Использовать в прокси»** и **«Проверять почту»** соответствуют соответствующим флагам в настройках модулей **«Прокси»** и **«Почта»**. Данные флаги включают антивирус Касперского для фильтрации трафика, проходящего через прокси-сервер и вложения в почтовых письмах. При включении данных флагов можно указать флаг **«Расширенное журналирование событий»**, он позволяет увидеть в **Журнале** больше информации о работе модуля. **(Внимание!** Эта опция может значительно нагружать систему)

Флаг **«Обновлять базы при выключенном антивирусе»** позволяет запускать проверку обновления баз при выключенной службе «Антивирус Касперского». Если нагрузка на систему значительная, то антивирус может обновляться только во время отключения для понижения нагрузки.

Поле **«Проверять наличие обновлений баз антивируса»** позволяет задать частоту проверок обновлений баз антивируса. По умолчанию этот процесс будет запускаться каждый час, при условии установленного хотя бы одного флага на данной вкладке. При выборе периода **«Каждый день»** можно указать время начала проверки, а при выборе **«Раз в неделю»** можно указать день недели, в который необходимо производить проверку, и так же время начала

проверки.

События

ИКС > Антивирус Касперского > События Администратор   6

Антивирус Касперского Настройки **События** Журнал

05.09.2019 - 05.09.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 Экспорт Удалить логи 

Объект письма от sebastian.golda@footballacademy.pl для man@a-real.ru защищён паролем
04:24:49

« < Стр 1 из 1 > » Показаны записи 1 - 1 из 1

Данная вкладка содержит список всех блокировок Антивируса Касперского. В каждой строке блокировки указано время и причина блокировки.

Журнал

ИКС > Антивирус Касперского > Журнал Администратор 8

Антивирус Касперского Настройки События **Журнал**

05.09.2019 - 05.09.2019 **Сегодня** Неделя Месяц Другой период ▾

Экспорт Удалить логи

run service 09:08:19
started 09:08:20
KavService: start initialization 09:08:20
EbusClient: connected 09:08:20
reload 09:08:52
KavService: initialization success 09:12:48
databases loaded succesfully 11:50:48
run service

« » Стр 1 из 1 > >> Показаны записи 1 - 13 из 13

На данной вкладке находится сводка всех системных сообщений от службы 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, сообщения о состоянии системы (включение/выключение) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**»

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:kav>

Last update: **2019/11/10 19:25**



Веб-фильтр Касперского

Модуль «Веб-фильтр Касперского» расположен в Меню «Защита».

Веб-Фильтр Касперского проверяет веб-сайты до их открытия и блокирует фишинговые сайты, а также сайты, распространяющие вредоносный код. Для проверки Веб-Фильтр обращается к облачному сервису Kaspersky Security Network. По результатам проверки Веб-Фильтр загружает веб-сайт, который признан безопасным, и блокирует веб-сайт, который признан вредоносным.

Модуль «Веб-фильтр Касперского» имеет три вкладки: «Веб-фильтр Касперского», «Настройки», «Журнал».

Веб-фильтр Касперского

ИКС > Веб-фильтр Касперского Администратор 10

Веб-фильтр Касперского Настройки Журнал

Веб-фильтр Касперского запущен
Выполняет сканирование и категоризацию web-адресов

Версия: 1.0.1.129
Лицензия истекает: 29.02.2020

Журнал

run service 13:37:18
run service 13:38:32

На первой вкладке модуля отображается состояние службы «Веб-фильтр Касперского» с возможностью «Выключить» (или «Включить» если служба выключена). Служба «Веб-фильтр Касперского» отвечает за работоспособность предустановленного Веб-фильтра Касперского, который определяет, к какой категории принадлежит открываемый сайт, если [установлен соответствующий флаг](#) в настройках прокси-сервера. В виджете службы «Веб-фильтр Касперского», также отображается: текущая версия веб-фильтра Касперского, дата истечения лицензии и последние события журнала за текущую дату.

Важно: по умолчанию служба находится в состоянии «не настроен». Чтобы активировать ее, отметьте в настройках прокси-сервера флажок «Использовать веб-фильтр Касперского». Конечно, при этом у вас должен быть приобретен лицензионный ключ.

Настройки

ИКС > Веб-фильтр Касперского > Настройки

Администратор 10

Веб-фильтр Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

Использовать в прокси

Размер кэша * 15000 Кб

Время ожидания ответа * 5 сек.

Сохранить Обновить

На данной вкладке можно определить **размер кэша** прокси, который будет использоваться для обработки данных, а также **время ожидания ответа** от облачного сервиса.

Флаг **«Использовать прокси»** необходимо установить после активации лицензии для того, чтобы осуществлялась проверка проходящего через прокси-сервер ИКС веб-трафика. Этот флаг аналогичен флагу **«Использовать веб-фильтр Касперского»** в [настройках прокси](#).

В этой же вкладке находится **Менеджер лицензий**. Для того, чтобы веб-фильтр начал работать, необходима приобретенная действующая лицензия.

Журнал

ИКС > Веб-фильтр Касперского > Журнал Администратор   10

Веб-фильтр Касперского Настройки **Журнал**

09.09.2019 - 09.09.2019 **Сегодня** Неделя Месяц Другой период ▾ 

↑ Экспорт Удалить логи 



run service 13:37:18
run service 13:38:32

«<<» < Стр 1 из 1 > >> Показаны записи 1 - 2 из 2

На данной вкладке находится сводка всех системных сообщений от службы веб-фильтра. 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) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:avp_web

Last update: **2019/11/10 19:25**



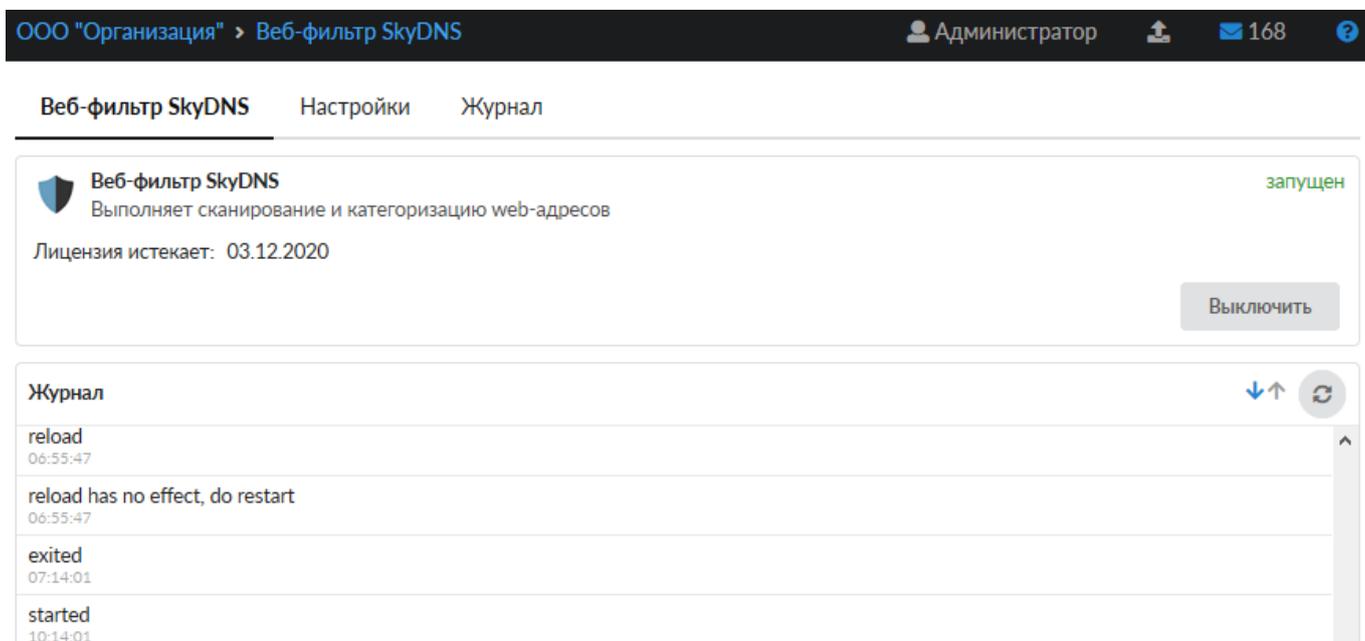
Веб-фильтр SkyDNS

Модуль «Веб-фильтр SkyDNS» расположен в Меню «Защита».

Кроме стандартных категорий трафика, в ИКС присутствует интегрированная синхронизация с сервисом фильтрации контента SkyDNS. Эти категории могут применяться таким же образом, как и все остальные. Их главное отличие - автоматическое обновление с сервера SkyDNS. Веб-фильтр SkyDNS проверяет веб-сайты до их открытия и блокирует фишинговые сайты, а также сайты, распространяющие вредоносный код.

Модуль «Веб-фильтр SkyDNS» имеет три вкладки: «Веб-фильтр SkyDNS», «Настройки», «Журнал».

Веб-фильтр SkyDNS



На первой вкладке модуля отображается состояние службы «Веб-фильтр SkyDNS» с возможностью «Выключить» (или «Включить» если служба выключена). Служба «Веб-фильтр SkyDNS» отвечает за работоспособность предустановленного Веб-фильтра SkyDNS, который определяет, к какой категории принадлежит открываемый сайт, если [установлен соответствующий флаг](#) в настройках прокси-сервера. В виджете службы «Веб-фильтр SkyDNS», также отображается дата истечения лицензии и последние события журнала за текущую дату.

Настройки

Использовать в прокси

Размер кэша *

 Мб

Время ожидания ответа *

 сек.

На данной вкладке можно определить **размер кэша** прокси, который будет использоваться для обработки данных, а также **время ожидания ответа** от облачного сервиса.

Флаг **«Использовать прокси»** отвечает за проверку проходящего через прокси-сервер ИКС веб-трафика. Этот флаг аналогичен флагу **«Использовать SkyDNS»** в [настройках прокси](#).

Журнал

03.12.2019 - 03.12.2019

Сегодня

Неделя

Месяц

Другой период ▾



Экспорт

Поиск...



started 06:55:30
ebus client [skydns] connected 06:55:30
[heartbeat]: started 06:55:30
[worker: 4]: started 06:55:30
[worker: 11]: started

На данной вкладке находится сводка всех системных сообщений от службы веб-фильтра. 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) - 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»**, или удалить логи за определенный период времени с помощью кнопки **«Удалить логи»**.

Лицензия

Для коммерческих организаций:

Для того, чтобы использовать модуль категорий трафика SkyDNS, Вам необходимо:

1. Заключить договор и оплатить модуль категории трафика SkyDNS;
2. Отправить на эл.почту hello@a-real.ru письмо с темой «Активация», содержащее название и ИНН организации, серийный номер (меню «О программе» - 32 символа).
3. Переактивировать программу.

Для учебных заведений:

Модуль категорий трафика SkyDNS включен в лицензию **«Контент-фильтр ИКС + категории трафика»**. Первый год после приобретения лицензии SkyDNS доступны по умолчанию, далее требуется приобретение **модуля «Техподдержка»**. Категоризация трафика осуществляется только при наличии действующей лицензии.

From:

<https://doc.a-real.ru/> - Документация

Permanent link:

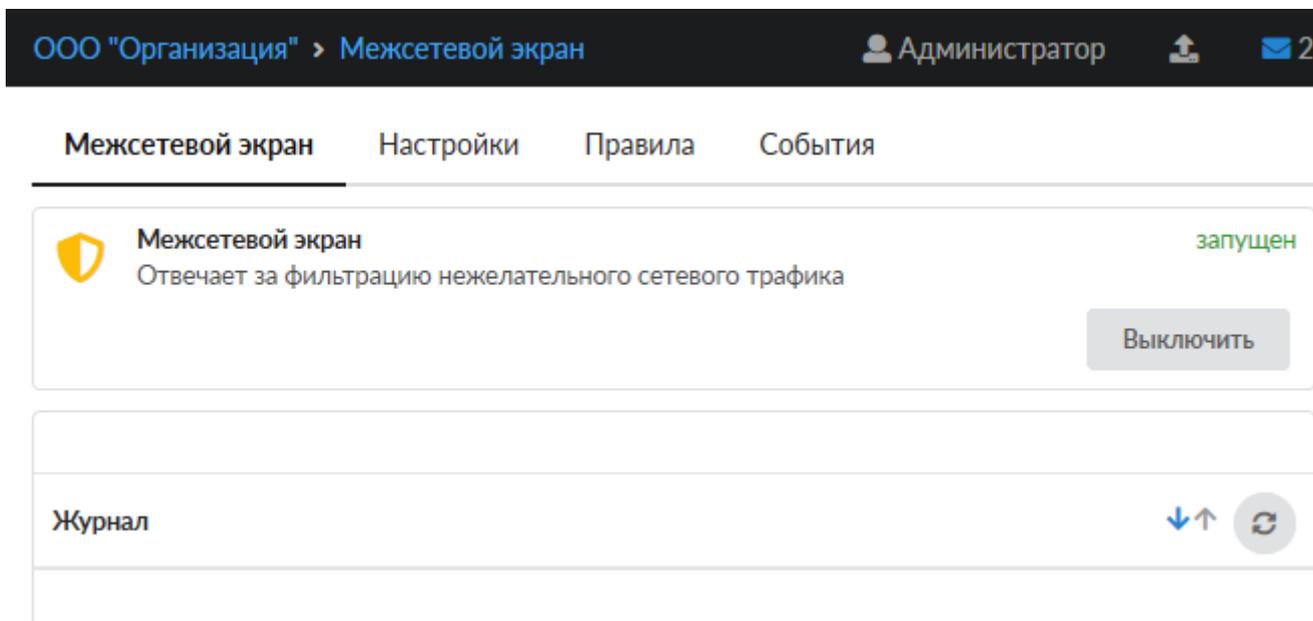
<https://doc.a-real.ru/doku.php?id=ics70:skydns>

Last update: **2019/12/03 15:55**



Межсетевой экран

Стартовая страница модуля



Межсетевой экран — комплекс программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также, межсетевой экран ИКС отвечает за трансляцию сетевых адресов во внешнюю сеть (NAT) и перенаправление портов.

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние события системы.

Внимание! Выключение межсетевого экрана оставит работающими только правила NAT'а. Все правила, ограничивающие доступ извне, будут отключены, что может негативно сказаться на безопасности системы. Отключайте межсетевой экран только при крайней необходимости.

Также следует отметить, что после перезагрузки системы с выключенным межсетевым экраном список правил `pf`, в том числе и правила NAT'а будет полностью очищен, и пользователи потеряют доступ во внешнюю сеть по всем протоколам, кроме HTTP.

Настройки

Управление ИКС через веб

Новая локальная сеть (192.168.17.190/24) x

Управление ИКС через SSH

Новая локальная сеть (192.168.17.190/24) x

Максимальное количество активных соединений *

10000 ^ v

Режим работы межсетевого экрана

ipfw -> pf v

Вкладка «Настройки» позволяет определить уровень доступа к управлению ИКС без создания дополнительных правил межсетевого экрана. Вы можете прописать ip-адреса или подсети, с которых будет осуществляться доступ к веб-интерфейсу ИКС или к консоли восстановления по протоколу SSH.

Если вы хотите получать доступ к 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 ИКС может быть затруднена прохождением через NAT модуля pf. В таком случае измените очередность запуска на pf→ipfw.

Правила

Вкладка «Правила» является главным рабочим полем администратора по настройке межсетевого экрана. Она разделена на две части: список всех интерфейсов 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.

Межсетевой экран Настройки **Правила** События

Добавить Удалить Выключить Редактировать Поиск... ↻

- ✓ Разрешающее правило
- ⊘ Запрещающее правило
- 👤 Приоритет
- ➔ Маршрут
- Ограничение скорости

Разрешающие правила

- ✓ **Доступ по протоколу ICMP**
Разрешить ICMP трафик, входящий на ИКС через Внешние интерфейсы
- ✓ **Доступ к серверу через GRE тоннели**
Разрешить GRE трафик, входящий на ИКС через Внешние интерфейсы
- ✓ **Доступ к почтовому серверу**
Разрешить TCP трафик, входящий на ИКС на порт Порт SMTP (25), Порт IMAP (143), Порт POP3 (110) через Внешние интерфейсы
- ✓ **Доступ к VPN-серверу** служба не запущена
Разрешить TCP трафик, входящий на ИКС на порт rprt (1723) через Внешние интерфейсы
- ✓ **Доступ к L2TP-серверу** служба не запущена
Разрешить UDP трафик, входящий на ИКС на порт 1701 через Внешние интерфейсы
- ✓ **Доступ к OpenVPN-сетям** служба не запущена
Разрешить TCP/UDP трафик, входящий на ИКС на порт OpenVpn

Правила межсетевого экрана группируются по типу:

1. Разрешающие правила
2. Запрещающие правила
3. Приоритеты
4. Маршруты
5. 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), веб-сервер (порт 80), 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.

События

Межсетевой экран Настройки Правила **События**

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ↻

Экспорт Удалить логи Все сообщения Поиск... 🔍

⬇ ⬆ ⬇ ⬆

Запрещающее правило FTP было добавлено пользователем **Администратор**
11:34:42

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.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:firewall>

Last update: **2019/11/10 19:25**



Web Application Firewall

Модуль «Web Application Firewall» (WAF) расположен в Меню «Защита». Данный модуль отслеживает и блокирует весь HTTP/HTTPS трафик входящий и исходящий от установленных Web-приложений на «ИКС» или в локальной сети. Путём анализа HTTP/HTTPS трафика WAF может предотвращать атаки, основанные на недостатках защиты Web-приложений, таких как: SQL инъекции, межсайтовый скриптинг (XSS), включение файлов, не правильная настройка безопасности.

The screenshot shows the 'Web Application Firewall' interface. At the top, there is a navigation bar with 'ИКС > Web Application Firewall', a user profile 'Администратор', and a notification icon with '17'. Below this is a date filter '13.09.2019 - 13.09.2019' and tabs for 'Сегодня', 'Неделя', 'Месяц', and 'Другой период'. There are buttons for 'Экспорт' and 'Удалить логи', and a search bar. The main area displays a list of log entries, each showing an IP address, timestamp, and request details. At the bottom, there is a pagination control showing 'Стр 1 из 1' and a note 'Показаны записи 1 - 84 из 84'.

192.168.17.8 - - [13/Sep/2019:12:36:57 +0300] "GET /styles.css?ver=7.0.0 HTTP/2.0" 200 129812 "https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"
192.168.17.8 - - [13/Sep/2019:12:36:57 +0300] "GET /jquery-3.1.1.min.js?ver=7.0.0 HTTP/2.0" 200 30120 "https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"
192.168.17.8 - - [13/Sep/2019:12:36:57 +0300] "GET /script.min.js?ver=7.0.0 HTTP/2.0" 200 732 "https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"
192.168.17.8 - - [13/Sep/2019:12:36:57 +0300] "GET /sockjs-1.1.5.min.js?ver=7.0.0 HTTP/2.0" 200 17900 "https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"
192.168.17.8 - - [13/Sep/2019:12:36:58 +0300] "GET /script.js?ver=7.0.0 HTTP/2.0" 200 71304 "https://192.168.17.246:81/" "Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0"

В самом модуле отображается сводка 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) - 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**».

Для включения/выключения фильтрации трафика необходимо установить/снять соответствующий флажок при добавлении или редактировании «**Виртуального хоста**»/«**Виртуального хоста с перенаправлением**», расположенных в Меню «**Файловый сервер**» - «**Веб**» - вкладка «**Веб-ресурсы**». Стоит отметить, что **Веб-сервер** должен быть настроен и запущен.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:waf>

Last update: **2019/11/10 19:25**



Application Firewall

Модуль «Application Firewall» расположен в Меню «Защита». Данный модуль предназначен для отслеживания и блокирования трафика пользователей на основании категорий библиотеки nDPI, а также соединений пользователей, подключившихся к ИКС через утилиту xauth.

Application Firewall Настройки Заблокированные соединения Журнал

L7 Application Firewall запущен
Отвечает за блокировку приложений пользователей

[Выключить](#)

Журнал ↓↑ ↻

started 10:36:36
locale loaded 10:36:36
config loaded 10:36:36
UDP xauthd server listening on 0.0.0.0:1984 10:36:36

Настройки

Application Firewall **Настройки** Заблокированные соединения Журнал

Доступные сети

🏠 Локальные сети ✕

[Сохранить](#) [Обновить](#)

Вкладка настройки содержит список сетей, в которых будет производиться сканирование соединений пользователей. По умолчанию выбраны Локальные сети.

Заблокированные соединения

Отображает список заблокированных соединений пользователей, если им назначены [правила](#)

Application Firewall или заблокированы процессы xauth.

Application Firewall Настройки **Заблокированные соединения** Журнал

🔍 Поиск...

BITTORRENT
192.168.17.22 -> 81.5.112.115
192.168.17.22 -> 195.211.101.124
192.168.17.22 -> 176.97.197.230
192.168.17.22 -> 121.152.204.216
192.168.17.22 -> 67.8.190.9
192.168.17.22 -> 59.127.107.227
192.168.17.22 -> 223.206.239.80
192.168.17.22 -> 37.187.105.66
192.168.17.22 -> 194.67.223.33

Журнал

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

Application Firewall Настройки Заблокированные соединения **Журнал**

17.09.2019 - 17.09.2019 Сегодня Неделя Месяц Другой период ▾ ↻

📄 Экспорт Удалить логи 🔍 Поиск...

started 10:36:36
locale loaded 10:36:36
config loaded 10:36:36
UDP xauthd server listening on 0.0.0.0:1984 10:36:36

« < Стр 1 из 1 > » Показаны записи 1 - 4 из 4

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».

Важно. Кнопка «Удалить логи» удаляет все логи, которые ведутся модулем «Application Firewall».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:appfirewall>

Last update: **2019/11/10 19:25**



Детектор атак Suricata

Модуль «Детектор атак» расположен в Меню «Защита». Данный модуль предназначен для запуска, настройки и конфигурирования используемого в «ИКС» open source IPS/IDS системы – Suricata. Данная система была разработана Open Information Security Foundation в 2009 году. Intrusion Prevention System (IPS, система предотвращения вторжений) — это система сетевой безопасности, обнаруживающая вторжения или нарушения безопасности. IPS отслеживает сетевой трафик в реальном времени и применяет различные меры – сброс соединения, логирование выявленных сигнатур или пропускает его. Также IPS может выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами. Система Suricata поддерживает многозадачность, как следствие обладает высокой производительностью, позволяющая обрабатывать трафик до 10Gbit на обычном оборудовании, и многое другое, в том числе полная поддержка формата правил Snort.

При открытии модуля в основном окне отобразятся вкладки «Детектор атак Suricata», «Настройки», «Правила», «Настройки обновлений» и «Журнал», при этом вкладка «Детектор атак Suricata» будет активна.

Детектор атак

Муми-дол > Детектор атак Suricata Тыве Янссон 45

Детектор атак Suricata Настройки Правила Настройки обновлений Журнал

Детектор атак Suricata запущен
Система обнаружения вторжений Выключить

Журнал

- [101477] <Notice> -- all 2 packet processing threads, 2 management threads initialized, engine started. 10:48:53
- [101477] <Notice> -- Signal Received. Stopping engine. 10:52:28
- [101477] <Error> -- [ERRCODE: SC_ERR_INVALID_SIGNATURE(39)] - Complete IP space negated. Rule address range is NIL. Probably have a !any or an address range that supplies a NULL address range 10:52:36

Вкладка «Детектор атак Suricata». На данной вкладке отображается состояние службы «Детектор атак Suricata» с возможностью «Выключить» (или «Включить» если служба выключена), а также последние события журнала за текущую дату.

Настройки

Детектор атак Suricata **Настройки** Правила Настройки обновлений Журнал

Интерфейсы

Внешние интерфейсы ✕

Внутренние сети

Локальные сети ✕

Внешние сети

Внешние диапазоны адресов ✕

DNS-сервера

Локальные сети ✕

SMTP-сервера

Локальные сети ✕

HTTP-сервера

Локальные сети ✕

SQL-сервера

Локальные сети ✕

TELNET-сервера

Локальные сети ✕

SSH-сервера

Локальные сети ✕

Контроллеры домена

Контроллеры домена

Вкладка «Настройки». Данная вкладка предназначена для настройки работы детектора атак. Для корректного применения базы сигнатур модуля, необходимо указать расположение объектов (сетей, серверов и портов), подверженных проверке. Здесь можно указать внутренние и внешние сети, диапазоны адресов различных серверов, а также используемые порты. Всем этим переменным присвоены значения по умолчанию, с которыми детектор атак может корректно запуститься. Для изменения конфигурации по умолчанию необходимо открыть выпадающий список в соответствующей ячейки и выбрать необходимые значения из известных «ИКС» портов или диапазона адресов, заданных Пользователем «ИКС». Либо в соответствующей ячейки в ручную указать необходимое значение. Для ячеек «сети» и «сервера» допустимыми являются следующие значения: доменное имя (host.ru); ip-адрес (192.168.1.1); ip-адрес/префикс (192.168.1.1/24); ip-адрес:маска (192.168.1.1:255.255.255.0); диапазон ip-адресов (192.168.1.1 - 192.168.1.254); пользователь; группа; локальная, внутренняя, VPN, OpenVPN, WiFi сети; и другие объекты, которыми оперирует «ИКС».

HTTP-порты

● http (80) × 311 × 591 ×

593 × 901 × 1220 × 1414 ×

1830 × 2301 × 2381 × 2809 ×

3128 × 3702 × 5250 × 7001 ×

7777 × 7779 × 8000 × 8008 ×

8028 × 8080 × 8088 × 8118 ×

8123 × 8180 × 8181 × 8243 ×

8280 × 8888 × 9090 × 9091 ×

9443 × 9999 × 11371 ×

SHELLCODE-порты

!80 ×

ORACLE-порты

1024 ×

SSH-порты

● ssh (22) ×

Для ячеек «порты» допустимыми являются следующие значения: номер порта (25, 110), диапазон портов (1000-2000), объекты порт заведенные на «ИКС». Для ячейки «SHELLCODE-порты» также допустимо исключение портов, например, !80. По умолчанию, анализируется трафик на внешних интерфейсах. Для анализа трафика локальной сети необходимо добавить в поле «Внешние сети» объект «Локальные сети».

Правила

Детектор атак Suricata

Настройки

Правила

Настройки обновлений

Журнал

Просмотр правил

Поиск...

Правила ▲	Количество правил	Применить
<input checked="" type="checkbox"/> Правила Emerging Threats		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Правила Positive Technologies Open Ruleset (Attack Detection)		<input checked="" type="checkbox"/>
pt-rules.rules	358	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Правила с snort.org		<input type="checkbox"/>
app-detect.rules (не загружено)		
attack-responses.rules (не загружено)		
backdoor.rules (не загружено)		
bad-traffic.rules (не загружено)		

Вкладка «Правила». В данной вкладке отображаются возможные базы модуля детектора атак. Существует три базы правил: правила с сайта snort.org, прекомпилированные правила с сайта snort.org и правила Emerging Threats. Каждая база содержит в себе набор скачиваемых файлов, в каждом файле содержится набор правил, объединенных по цели защиты. Для работы набора правил из базы, необходимо чтобы данная база была скачена (см. описание вкладки «настройка обновлений»), если база не скачена, то напротив каждого файла будет надпись «не загружено». Если база была загружена, то возможно выбрать применение всей базы целиком, отметив флажок в столбце «применить». Если необходимо применить определенный файл или наоборот не применять его, то необходимо отметить флажком в столбце «применить» соответствующий файл. Напротив каждого файла показано какое количество правил тот содержит. В правом верхнем углу располагается поиск по названию или по количеству правил в файле. Для просмотра правил и выбора действия необходимо кликнуть по имени файла, будет открыто новое окно с таблицей. Таблица имеет следующие поля: id правила – номер правила; приоритет – значение угрозы; предупреждение – описание производимой атаки; классификация – к какому классу относится атака; действие – определяет, что необходимо сделать при обнаружении данной атаки (alert – запишет в собственный лог обнаружение и пропустит, drop – уничтожит пакет, allow – пропустит, reject – уничтожит пакет и уведомит отправителя о данном событии); включение/выключение соответствующего правила.

Настройки обновлений

Детектор атак Suricata	Настройки	Правила	Настройки обновлений	Журнал
------------------------	-----------	---------	-----------------------------	--------

Oinkcode

Подписчик на обновления правил с snort.org

Устанавливать правила Emerging Threats

Positive Technologies Open Ruleset (AttackDetection)

Ежедневно проверять обновления правил

Правила обновлены 06.11.2019 10:48

Вкладка «Настройки обновлений». Данная вкладка предназначена для настройки процесса обновлений правил модуля. Существует 2 компании, которые активно занимаются разработкой правил для систем предотвращения вторжений – Sourcefire и Emerging Threats. Для того чтобы скачать базы «Правила с сайта snort.org» и «Прекомпилированные правила с сайта snort.org», необходимо: * Зарегистрироваться на сайте Snort.org (при необходимости стать подписчиком на обновления правил), * Получить Oinkcode для скачивания правил, находится в личном кабинете на сайте snort.org, * Ввести код в поле «Код для Oinkmaster», * Отметить следующий за этим полем флажок в том случае, если вы действительно стали подписчиком на обновления

правил, * Сохранить. Правила можно скачать при условии наличия одного лишь кода. Обратите внимание на отличие прав подписчика от обычного зарегистрированного пользователя. После удачного скачивания правил от данного разработчика, они будут отображаться во вкладке «Правила» без пометки (не загружено). Для того чтобы скачать базу «Правила Emerging Threats» достаточно поставить флажок «Устанавливать правила Emerging Threats» и сохранить изменения. Ещё один параметр, который возможно настроить в данной вкладке - это возможность ежедневно проверять обновления правил, которые были загружены. По умолчанию, флажок установлен, при необходимости его можно изменить. После того, как всё настроено, можно нажимать кнопку «Обновить сейчас».

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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:suricata>

Last update: **2019/11/10 19:25**

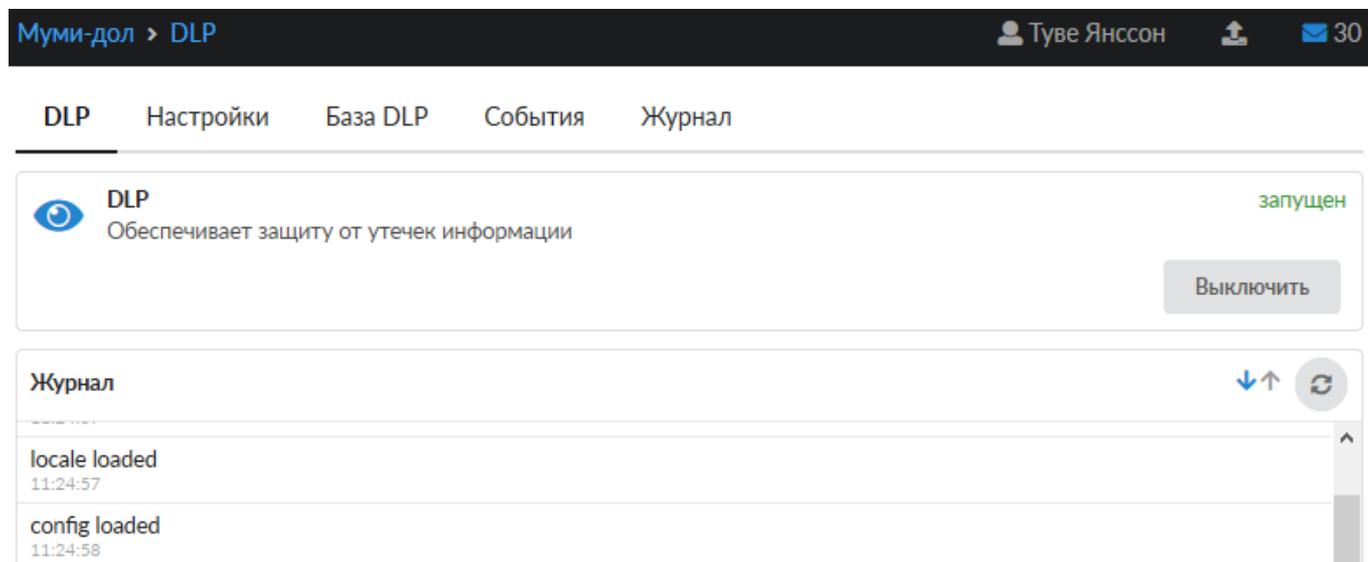


DLP

DLP (Data Leak Prevention) — технология предотвращения утечек конфиденциальной информации из внутренней сети. DLP-система базируется на анализе потоков данных, проходящих через шлюз сети. При обнаружении конфиденциальной информации срабатывает защита, и передача блокируется.

Модуль «DLP» расположен в Меню «Защита». Данный модуль предназначен для блокировки передачи конфиденциальной информации. Модуль «DLP» имеет пять вкладок: «DLP», «Настройки», «База DLP», «События» и «Журнал».

Общие сведения



Вкладка «DLP». На данной вкладке отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки

DLP **Настройки** База DLP События Журнал

Использовать DLP для прокси
 Использовать DLP для почты

Использовать для проверки:

Контрольные суммы файлов
 Шаблоны
 Ключевые слова
 Отпечатки текстовых файлов

80 ^ %
v

Вкладка «Настройки». Данная вкладка предназначена для настройки работы модуля «DLP».

Флаги **Использовать DLP для прокси** и **Использовать DLP для почты** соответствуют аналогичным флагам в разделах настроек модулей «Прокси» и «Почта», при их установке модуль DLP проверяет отпечатки в почтовых сообщениях ИКС и в HTTP-трафике.

Флаги **Контрольные суммы файлов**, **Шаблоны**, **Ключевые слова**, **Отпечатки текстовых файлов** позволяют определить, по каким критериям определять конфиденциальность информации, а также порог срабатывания для последнего.

Учитывать размер файла

1 ^ Мб
v

Использовать внешний DLP сервер

Сервер Порт

(не использовать) 1344

Сохранить Обновить

Флаг **Учитывать размер файла** определяет максимальный размер обрабатываемого файла, что позволит снизить нагрузку модуля на систему.

Флаг **Использовать внешний DLP сервер** дает возможность указать внешний сервер проверки.

База DLP

DLP Настройки **База DLP** События Журнал

Добавить Удалить Выключить Редактировать Поиск... 🔍 ↻

 Ключ сертификата для муми-сети Отпечаток файла
 Приветствие Отпечаток файла
 Запрещено к передаче Группа слов DLP Королевский рубин, Одинокие горы, Шляпа волшебника барометр, ботаник, грот, пещера

Удалить Редактировать Выключить

Вкладка «База DLP». Данная вкладка предназначена для управления списком файловых отпечатков и групп слов, согласно которому будет происходить проверка.

Отпечаток файла

Объект «Отпечаток файла» предназначен для защиты от передачи конкретного файла. Для добавления отпечатка файла необходимо нажать «Добавить» - «Отпечаток файла», откроется диалоговое окно, в котором будет предложено выбрать файл и дать описание отпечатку (по умолчанию, поле будет заполнено именем выбранного файла).

Добавление отпечатка файла

Название *

Файл *

Добавить Отмена

После добавления отпечатка он будет загружен в асинхронном режиме, а в списке базы DLP отобразятся проценты загрузки.

Общее Шаблоны **Ключевые слова**

Добавить Удалить  Импорт 4 записи 

грот
барометр
ботаник
пещера

Вкладка «Ключевые слова». Эта вкладка предназначена для добавления отдельных слов.

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 «Импорт».

События

DLP Настройки База DLP **События** Журнал

08.11.2019 - 08.11.2019 **Сегодня** Неделя Месяц Другой период ▾ 

 Экспорт Поиск... 

Запрещена отправка письма от mama@mumi.dol для daddy@mumi.dol 11:58:09
Запрещена передача файла "goose2.png" от 192.168.17.43 Файл: "goose2.png" URI: https://drive.google.com Совпадение по: отпечатку  Galactic guardian goose (контрольная сумма) 12:25:17

Вкладка «События». Данная вкладка содержит список всех блокировок DLP. В каждой строке блокировки указан пользователь либо ip-адрес, для которого был заблокирован ресурс, а также причина блокировки (название отпечатка или группа слов).

Журнал

DLP Настройки База DLP События **Журнал**

08.11.2019 - 08.11.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

started 11:24:57
locale loaded 11:24:57
config loaded 11:24:58
mail transparent proxy started at port 3333 11:24:58
DLP db is loaded 11:24:58

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «DLP» 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) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:dlp>

Last update: **2019/11/10 19:25**



Контент-фильтр

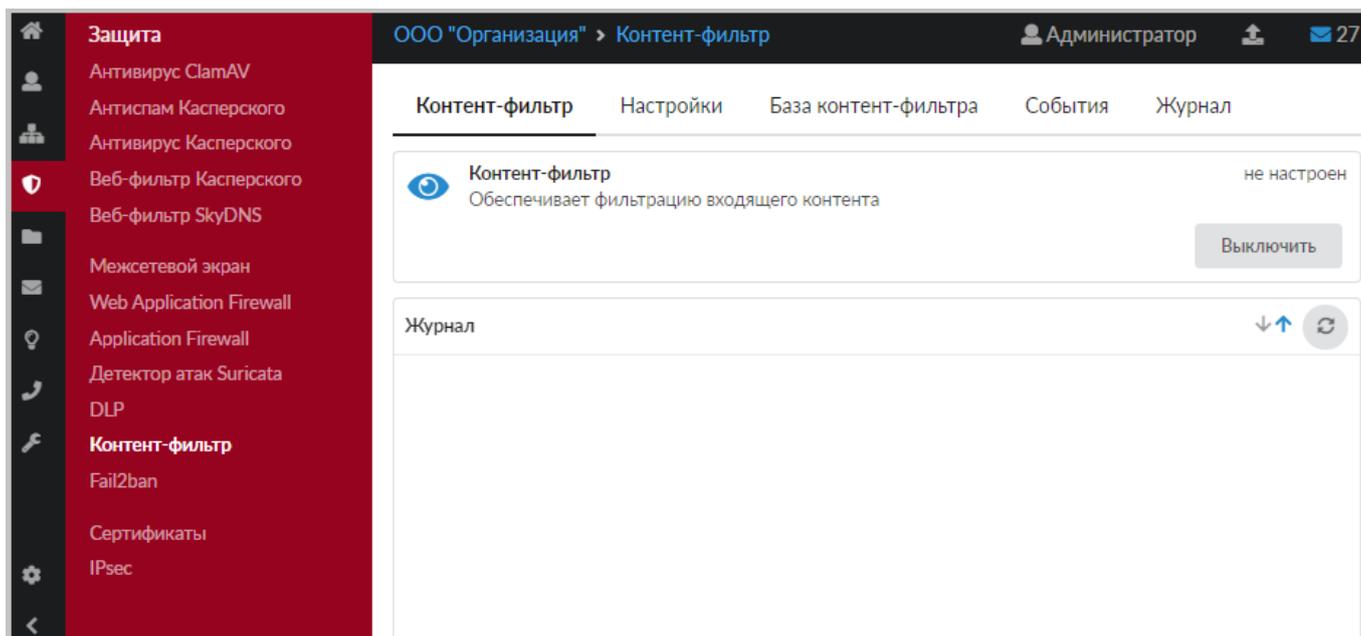
Модуль «Контент-фильтр» расположен в Меню «Защита». Модуль предназначен для настройки и блокировки интернет-страниц, содержащих в себе заданные ключевые слова или регулярные выражения. Модуль «Контент-фильтр» имеет вкладки:

- «Контент-фильтр»;
- «Настройки»;
- «База Контент-фильтра»;
- «События»;
- «Журнал».

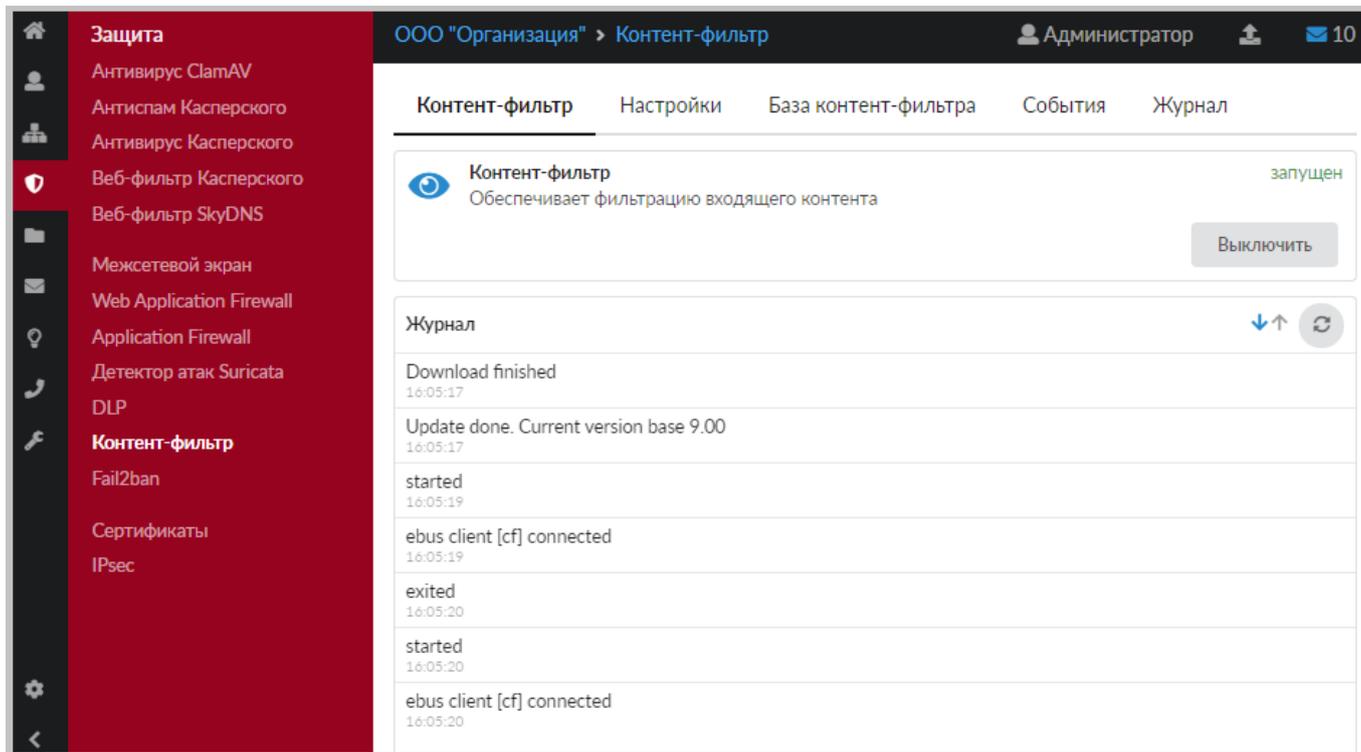
Для применения контентной фильтрации трафика, необходимо в Меню - «Наборы правил» добавить в один/несколько наборов [«Правило контентной фильтрации»](#). В данном случае, правило/правила примененные к Пользователю/группе Пользователей будут использовать контентную фильтрацию трафика. Или в индивидуальном модуле Пользователя/Группы Пользователей на вкладке [«Правила и ограничения»](#) добавить «Правило контентной фильтрации». Стоит отметить, что для корректного функционирования контентной фильтрации необходимо [расшифровывать трафик](#) полностью.

Контент-фильтр

Вкладка «Контент-фильтр». Отображает состояние модуля контент-фильтра запущен/остановлен/не настроен, также отображает журнал модуля за текущую дату, имеет кнопку включения/выключения.



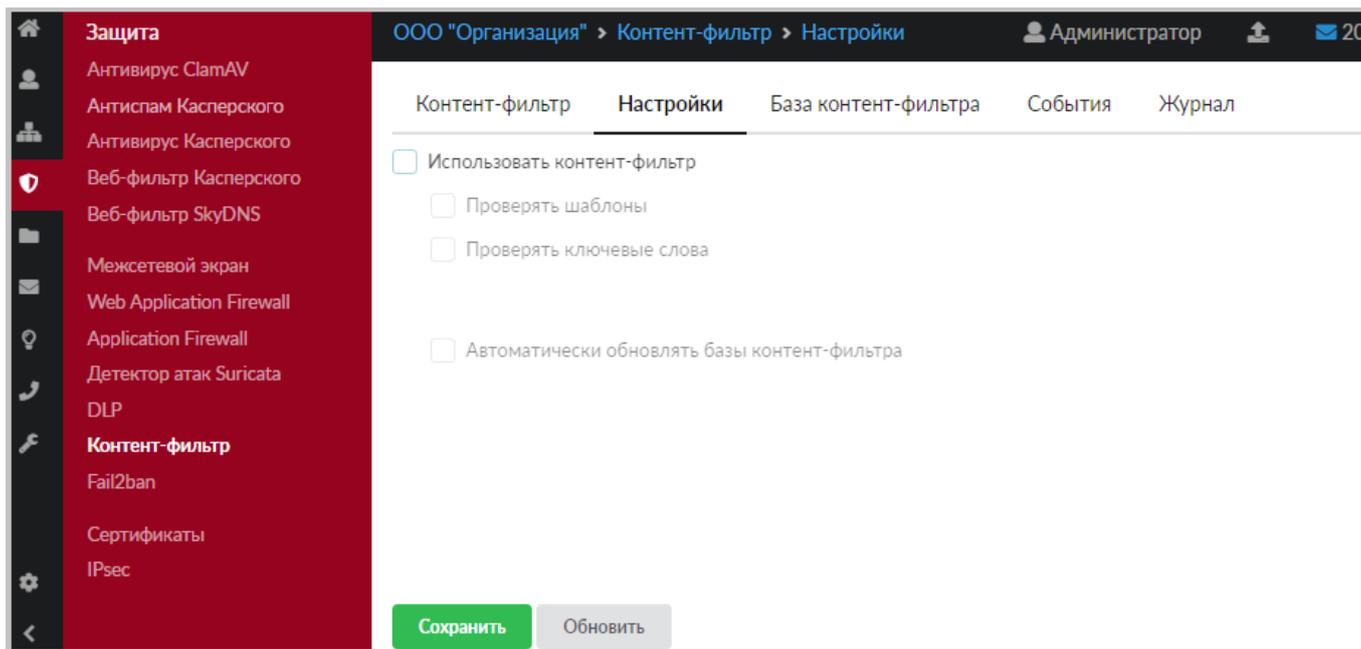
После регистрации «ИКС» (Меню «Обслуживание» - [«О программе»](#)) и настройки Контент-фильтра, окно «Контент-фильтр» будет выглядеть так:



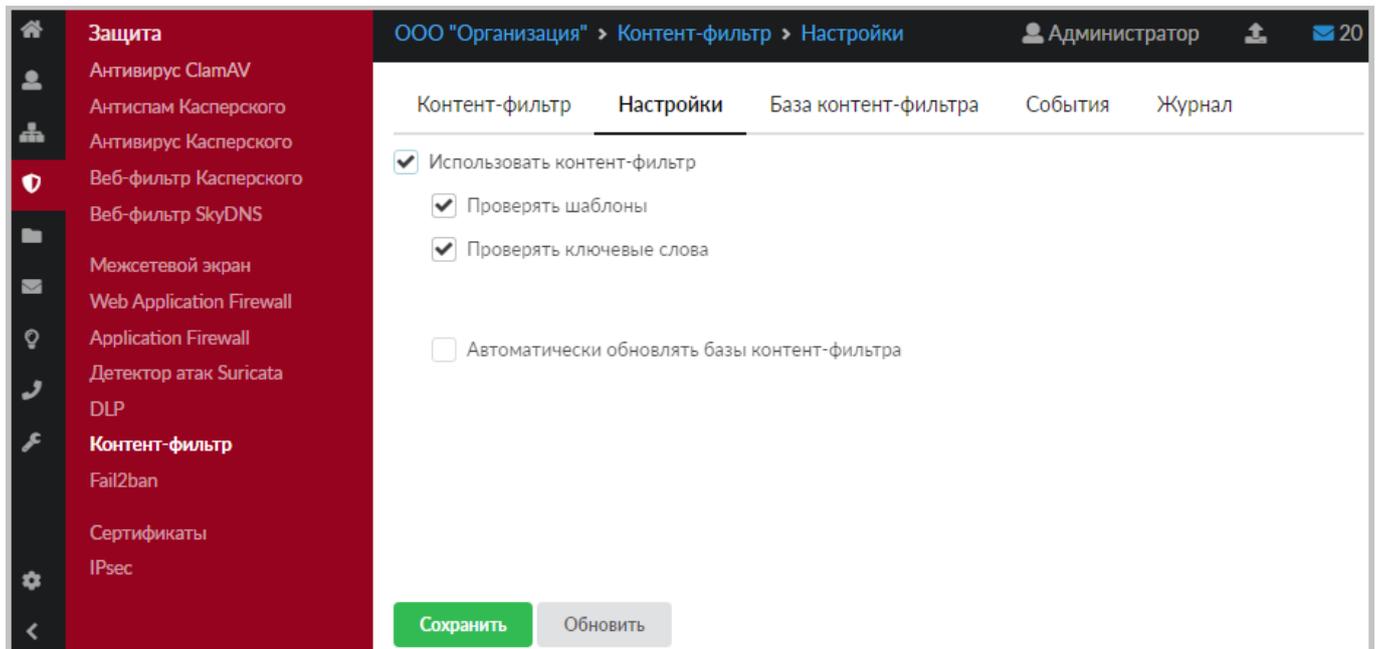
Состояние работы модуля изменится на «запущен», в журнале появятся записи логов.

Настройки

Вкладка «Настройки» содержит флаги управления состоянием модуля, обновлением его баз и вариантами фильтрации. Сразу после установки «ИКС» флаги вкладки «Настройки» не выставлены:



Включение флага «Использовать контент-фильтр» автоматически включает флаги «Проверять шаблоны» и «Проверять ключевые слова». Флаг «Автоматически обновлять контент-фильтр» выставляется отдельно при необходимости.



Важно. После установки «ИКС» списки баз модуля «Контент-фильтр» - пустые. Если флаг «Автоматически обновлять контент-фильтр» не включен, то для фильтрации необходимо создать и заполнить списки баз вручную.

Рекомендуется устанавливать флаг «Автоматически обновлять контент-фильтр» для использования уже готовых баз. Модуль подключится к облачному сервису и загрузит последнюю версию списков. В дальнейшем, при установленном флажке, списки будут обновляться раз в сутки.

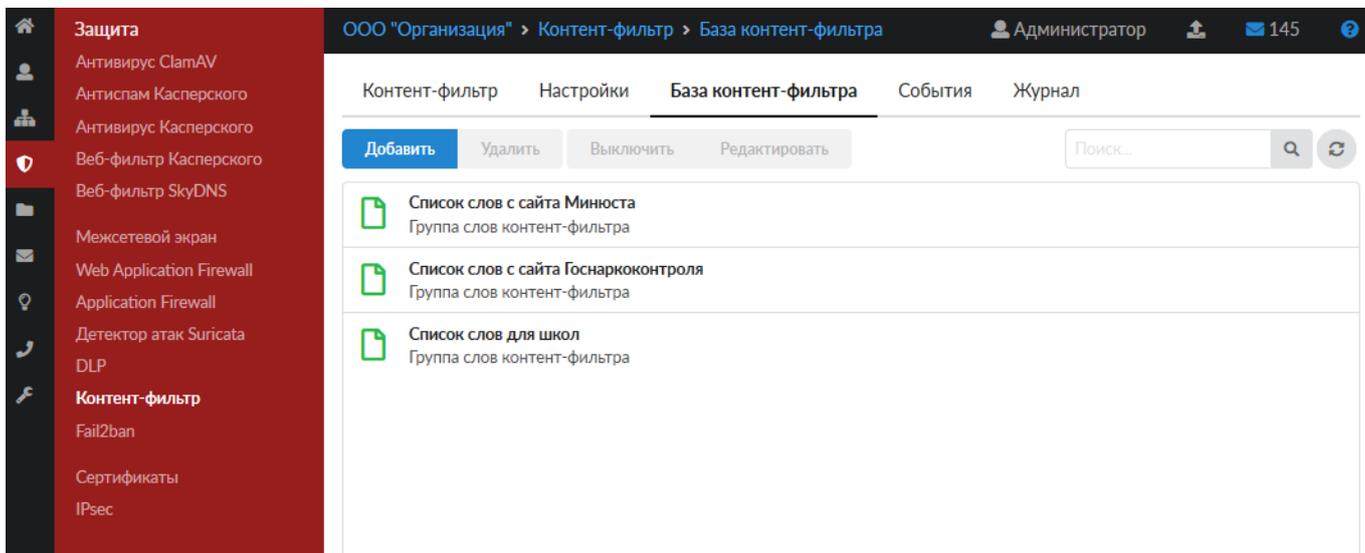
Важно. Чтобы настройки вступили в силу необходимо нажать кнопку «Сохранить». Далее необходимо проверить, что базы обновились - на вкладке «База Контент-фильтра». Нужно выбрать один из списков слов. Если обновление прошло удачно, то под названием выбранного списка появится несколько ключевых слов и шаблонных выражений из этого списка.

База Контент-фильтра

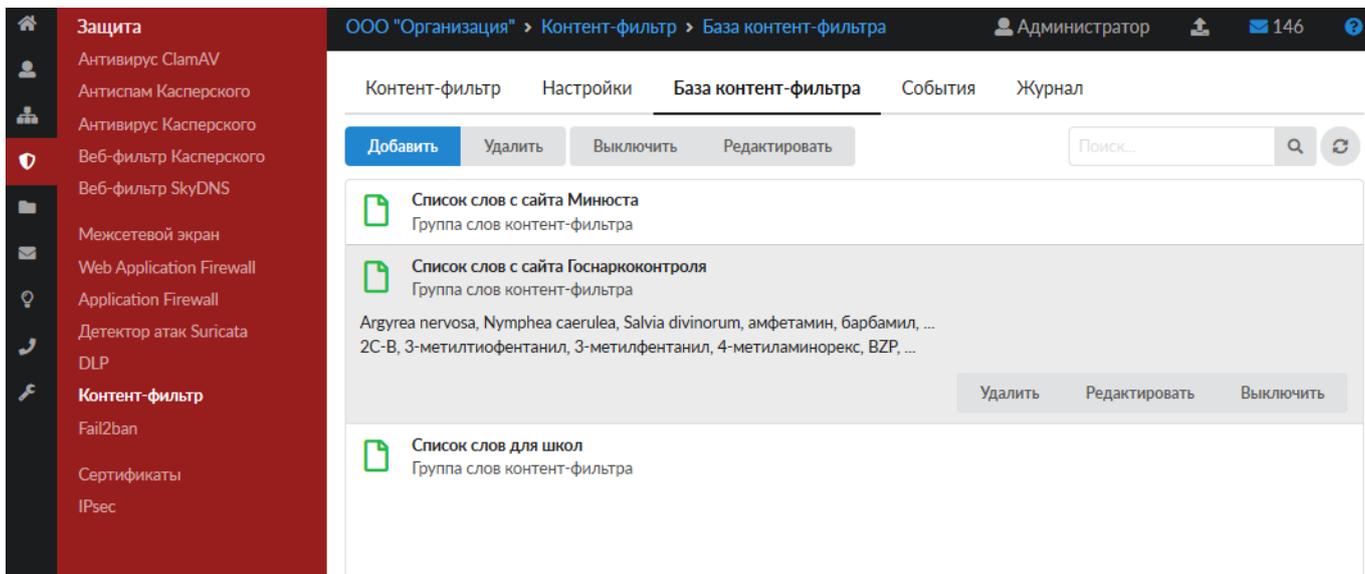
Вкладка «База Контент-фильтра» позволяет:

- управлять базами «Контент-фильтра»;
- редактировать списки шаблонов и слов баз;
- включать/выключать отдельную базу в работу модуля;
- удалять базы;
- искать шаблоны и слова в базах.

Важно: по-умолчанию, модуль «Контент-фильтр» содержит ПУСТЫЕ списки слов, запрещенных Минюстом и Госнаркоконтролем, а также специальный список для школ. Они не содержат записей. Для получения данных записей необходимо иметь активный модуль «Техподдержка» (в первый год действует по умолчанию у всех клиентов, далее требуется его ежегодное приобретение).



Каждая база содержит две вкладки - шаблоны и ключевые слова. Их просмотр и редактирование доступно в диалоговом окне «Редактирование группы слов контент-фильтра» при нажатии кнопки «Редактировать» в окне вкладки или в блоке базы при её выделении.



Вкладка «Ключевые слова» - позволяет задать любой длины строку, содержащую любые символы. Контент-фильтр сработает на данную строку, если перед и после указанной строки идет любой символ, кроме буквенного. Например, задано - «ет Са», контент-фильтр не сработает на «Привет Саша», но сработает на «Прив-ет Са».

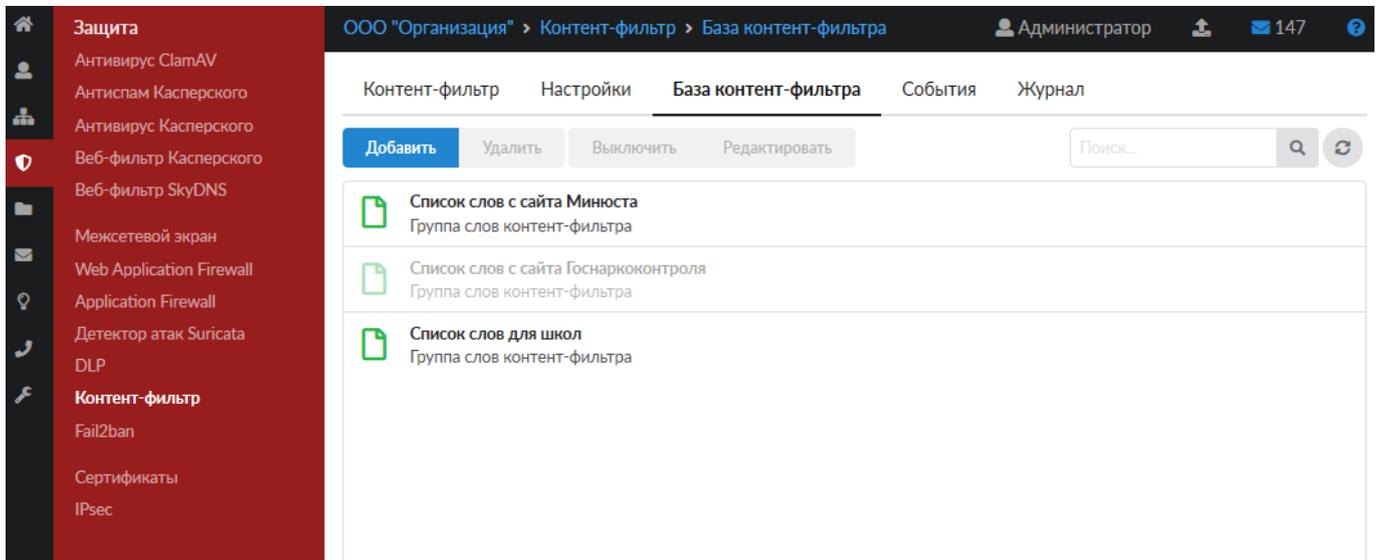
Вкладка «Шаблоны» - позволяет задать регулярные выражения. Например:

- **Привет** - Контент-фильтр будет искать не изменяемое регулярное выражение - «Привет»
- **/\bрус.*\b/** - Контент-фильтр сработает на слова: русич, русский, русофоб, рус.яз

При добавлении регулярного выражения в шаблоны, необходимо придерживаться конструкции - **/регулярное выражение/**. Само регулярное выражение задается по общепринятым нормам. Кратко почитать о регулярных выражениях возможно тут <https://tproger.ru/articles/regexp-for-beginners/>. Стоит отметить, что буква «ё» воспринимается как буква «е».

Важно. Модуль «Контент-фильтр» производит фильтрацию контента по списку шаблонов и списку ключевых слов, которые состоят из общих списков соответствующих шаблонов и слов каждой из включенных баз. Фильтрация по шаблонам и словам выключенной базы производится не будет.

Выключенная база в окне вкладки «База Контент-фильтра» выглядит неактивной - затенена.



Редактирование группы слов контент-фильтра

Диалоговое окно «Редактирование группы слов контент-фильтра» позволяет добавлять и удалять шаблоны и ключевые слова.

Редактирование группы слов контент-фильтра

Шаблоны Ключевые слова

Добавить Удалить  Импорт  Экспорт 2890 записей 

1488
21sextury
50921688334548
7pgb1h44vg08
abrek
abshabashennyi
abstiag
abstiaga
abstiak
adiveda
adult

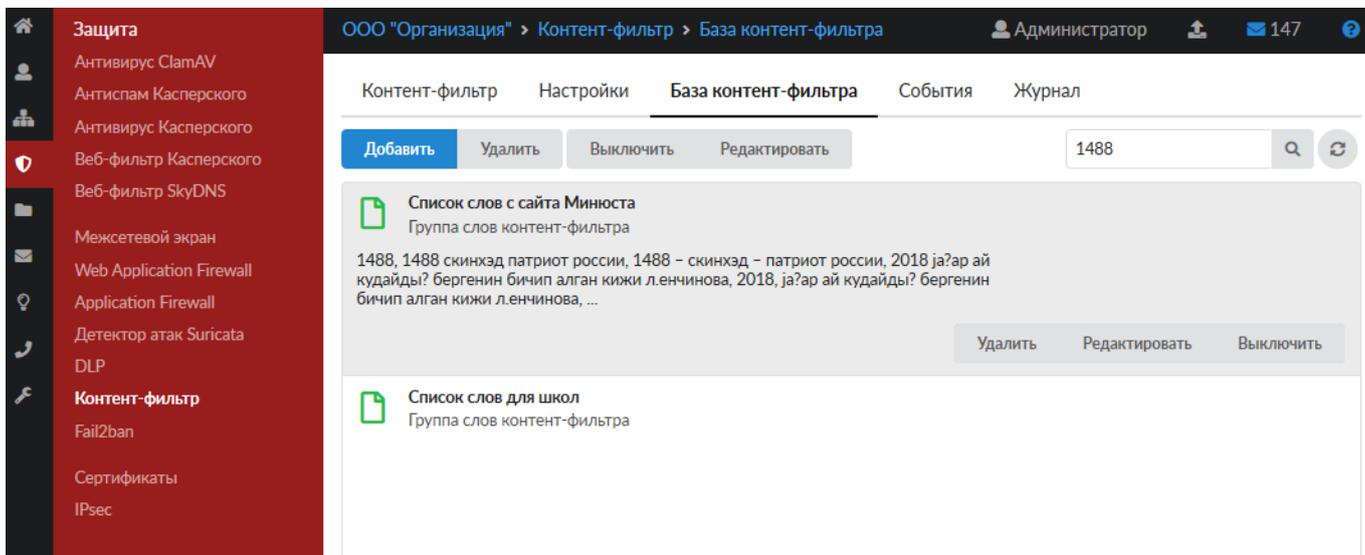
Сохранить Отмена

Для экспорта списка «Шаблоны» или «Ключевые слова» необходимо выбрать соответствующую вкладку и нажать кнопку «Экспорт». Список будет загружен браузером с именем файла - <Имя базы>-<тип списка>.txt, например - «Список слов с сайта Госнаркоконтроля-regexp.txt».

Добавить свой список шаблонов или ключевых слов можно по кнопке «Импорт». Файл должен содержать список шаблонов или слов (каждое с новой строки) в формате *.txt.

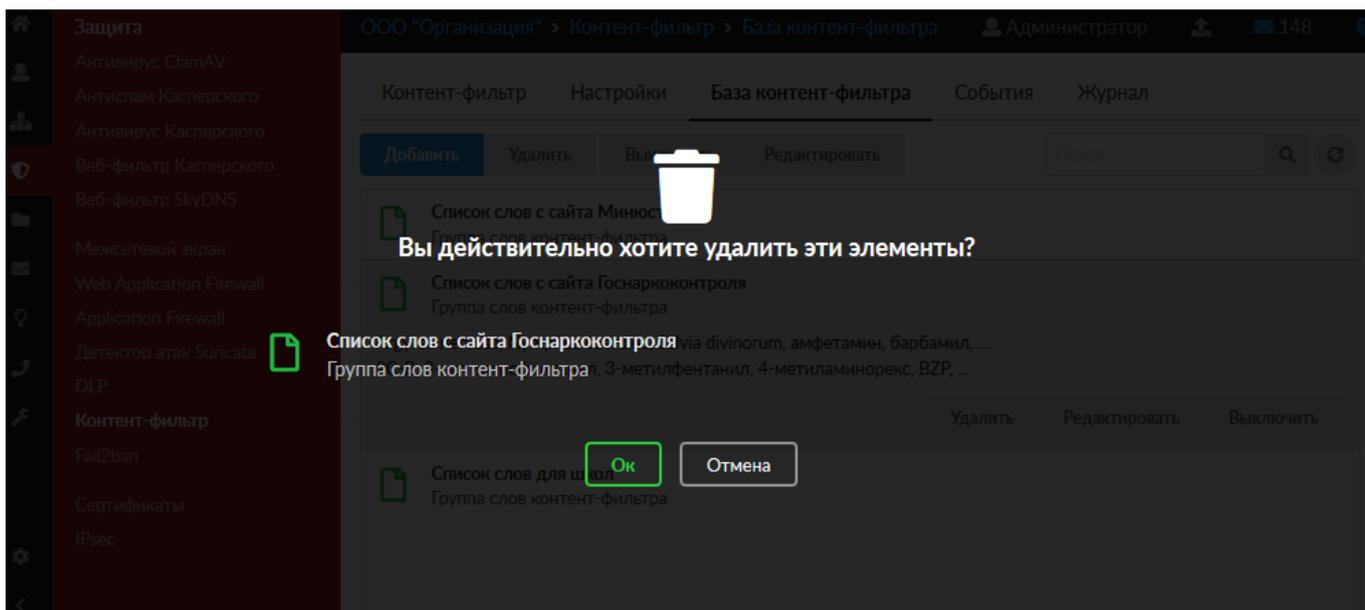
Поиск шаблонов и слов в базах

Поиск шаблонов и ключевых слов в списках баз модуля «Контент-фильтр» происходит с использованием поискового поля. При наборе слов шаблона происходит динамический поиск по базам, в результате в окне вкладки «База Контент-фильтра» в списке баз остаются только базы, содержащие искомое выражение.



Удаление списка из Базы контент-фильтра

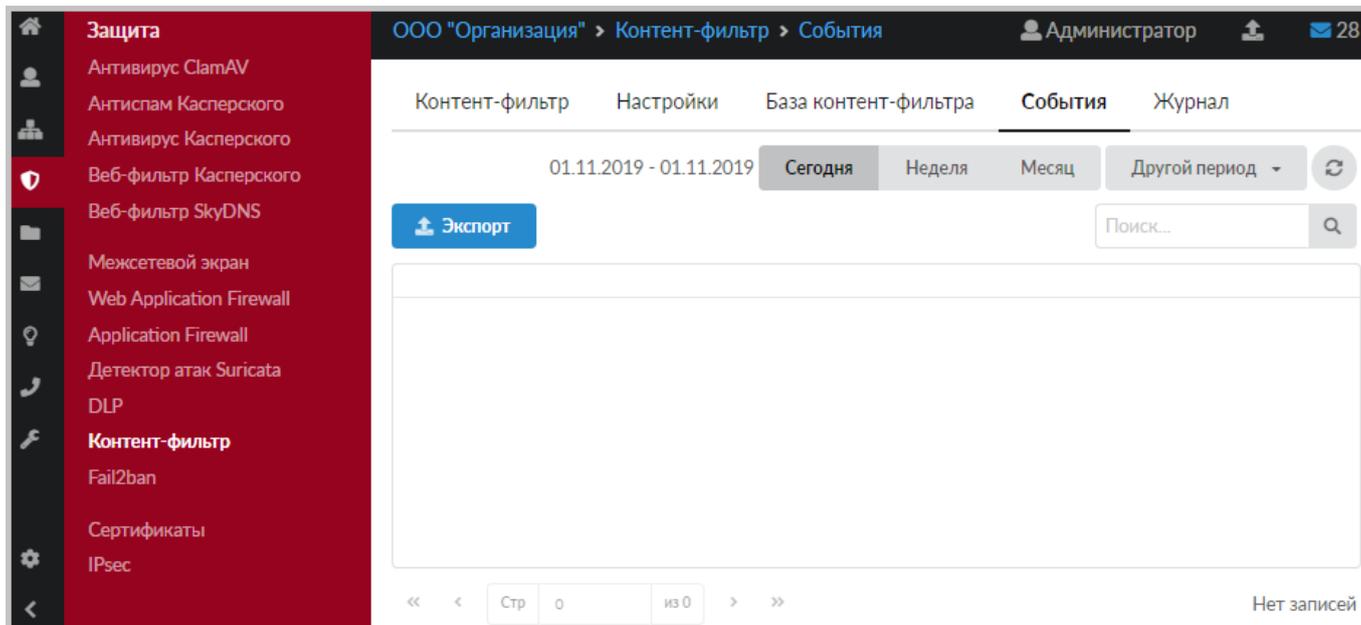
Удаление неиспользуемого списка из базы контент-фильтра происходит по кнопке «Удалить» при его выделении:



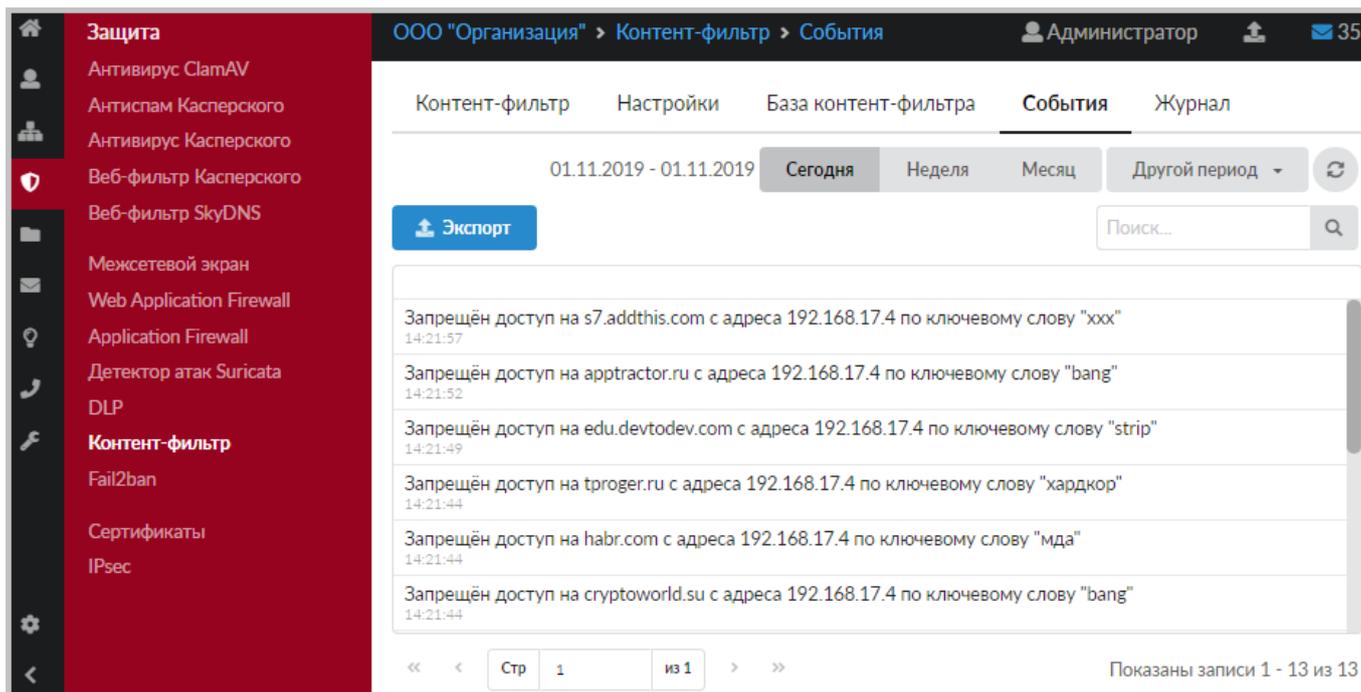
Важно. При удалении списков Базы по-умолчанию (Минюст, Госнаркоконтроль и SkyDNS), вернуть их обратно НЕЛЬЗЯ. Прежде чем их удалять воспользуйтесь механизмом экспорта списков.

События

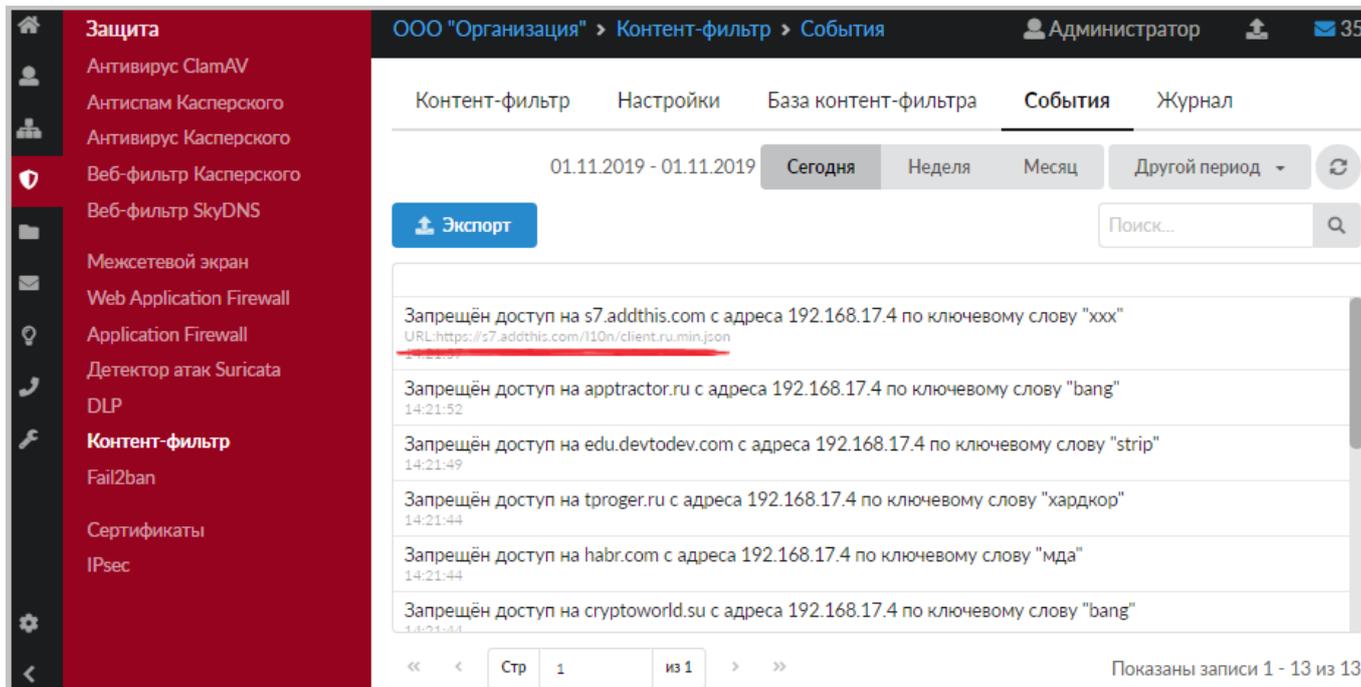
Вкладка «События» позволяет просматривать, фильтровать и экспортировать информацию о блокировках контента. Возможен отбор событий за текущий день, неделю, месяц. Для точного поиска можно задать период вручную.



При работе Пользователей «ИКС» с сайтами Интернет, модуль «Контент-фильтр» будет производить проверку контента. Все заблокированные ресурсы будут отображаться в окне вкладки «События» с пояснением по шаблону или слову произошла блокировка.



Посмотреть **полный URL заблокированного ресурса** можно щёлкнув по строке с событием:

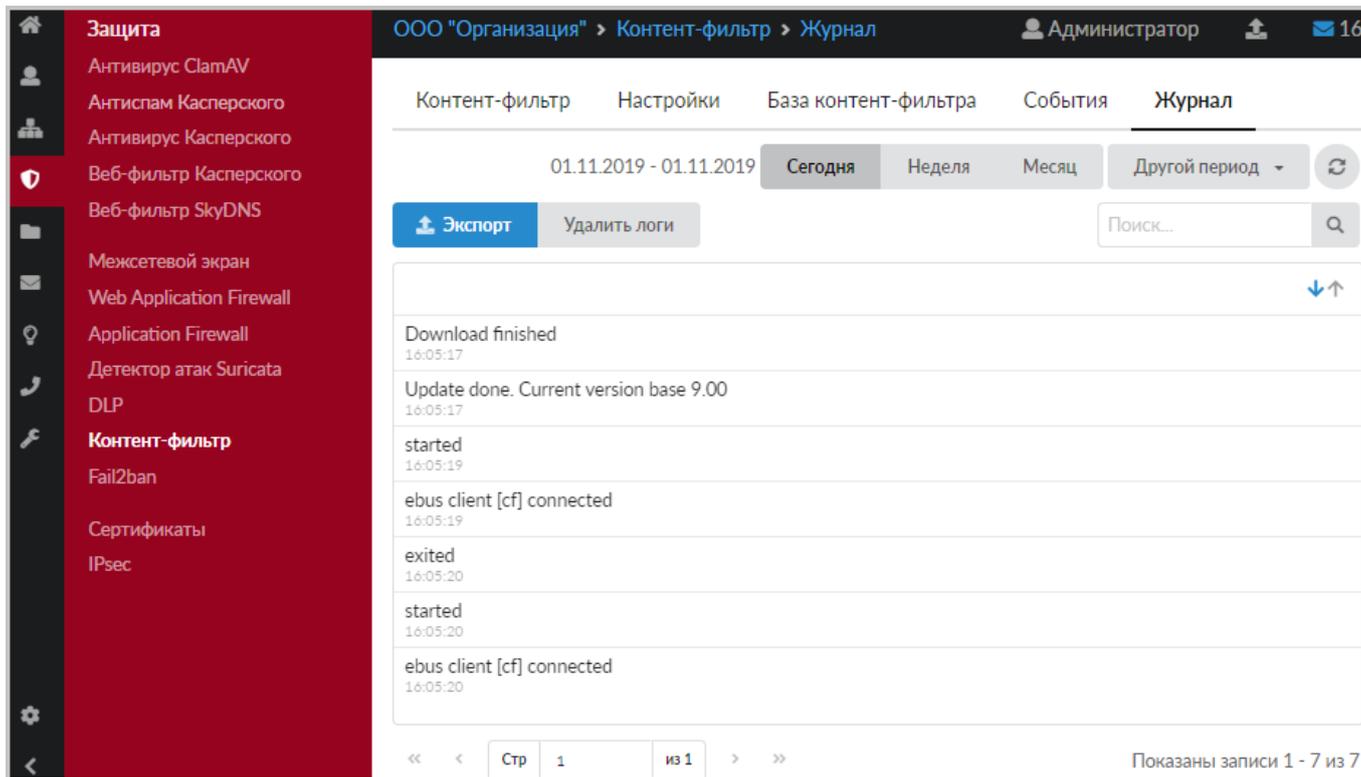


Для поиска по событиям есть поисковое поле.

Важно. Кнопка «Удалить логи» удаляет все логи, которые ведутся модулем «Контент-фильтр».

Журнал

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



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».

Важно. Кнопка «Удалить логи» удаляет ВСЕ логи, которые ведутся модулем «Контент-фильтр».

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:content>

Last update: **2019/12/03 14:39**

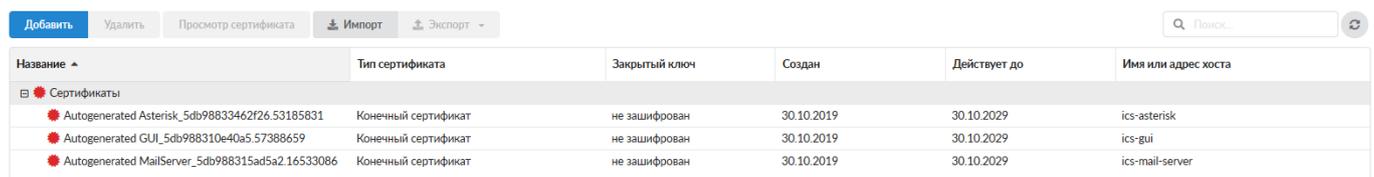


Сертификаты

Модуль «Сертификаты» расположен в Меню «Защита». Данный модуль предназначен для управления сертификатами, которые используются для установления защищённых SSL/TLS соединений типа клиент-сервер. Более подробно о SSL/TLS можно почитать здесь <https://ru.wikipedia.org/wiki/SSL> и <https://ru.wikipedia.org/wiki/TLS>.

Созданные сертификаты могут применяться как в «ИКС», так и в сторонних программах.

При первой установке «ИКС» автоматически создаются конечные сертификаты для WEB-интерфейса, телефонии и почты.



The screenshot shows the 'Certificates' module interface. At the top, there are buttons for 'Добавить' (Add), 'Удалить' (Delete), 'Просмотр сертификата' (View certificate), 'Импорт' (Import), and 'Экспорт' (Export). A search bar is also present. Below the buttons is a table with the following columns: 'Название' (Name), 'Тип сертификата' (Certificate type), 'Закрытый ключ' (Private key), 'Создан' (Created), 'Действует до' (Valid until), and 'Имя или адрес хоста' (Name or host address). The table contains three rows of certificates, all of which are 'Конечный сертификат' (End-entity certificate) and were created on 30.10.2019, with expiration dates of 30.10.2029. The host names are 'ics-asterisk', 'ics-gui', and 'ics-mail-server'.

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Autogenerated Asterisk_5db98833462f26.53185831	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-asterisk
Autogenerated GUI_5db988310e40a5.57388659	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-gui
Autogenerated MailServer_5db988315ad5a2.16533086	Конечный сертификат	не зашифрован	30.10.2019	30.10.2029	ics-mail-server

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.

Модуль позволяет создать новый сертификат или удалить существующий при помощи кнопок «Создать» и «Удалить»; экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт»; просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата».

Создание сертификатов

Чтобы создать новый сертификат, нажмите «Добавить».

Добавление сертификата

Общее

Настройки

Использование ключа

Netscape расширение

Название *

Новый сертификат

Код страны

RU - Russian Federation

Город

Город

Область

Область

Организация

Организация

E-mail

E-mail

Имя или адрес хоста *

test.ru

Добавить

Отмена

Во вкладке «Общее» заполняются данные сертификата: наименование, код страны, местоположение, сведения об организации, имя хоста или ip-адрес.

Добавление сертификата

[Общее](#)[Настройки](#)[Использование ключа](#)[Netscape расширение](#)

Тип сертификата

CA

Алгоритм

SHA 256

Тип шифрования

RSA

Срок действия сертификата

31.05.2020

Длина ключа *

2048

бит

[Добавить](#)[Отмена](#)

Во вкладке «Настройки» определяется роль сертификата - CA (корневой) или конечный, устанавливается метод шифрования, время действия и длина ключа в битах.

Добавление сертификата

Общее Настройки **Использование ключа** Netscape расширение

Шаблон

CA

Использование ключа

- CRL sign
- Certificate Sign
- Non Repudiation
- Digital Signature
- Key Encipherment

Расширенное использование ключа

- E-mail Protection
- TLS Web Client Authentication
- Code Signing
- TLS Web Server Authentication
- Time Stamping

Добавить

Отмена

Во вкладке «Использование ключа» можно выбрать шаблон использования открытого ключа сертификата в поле «Шаблон» или указать вручную в разделах «Использование ключа» («Key usage extensions») и «Расширенное использование ключа» («Extended key usage»). Более подробно можно почитать здесь https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/conf_keyusageextensionsandextendedkeyusage_r.html

Добавление сертификата

Общее Настройки Использование ключа **Netscape расширение**

- SSL Client
- SSL Server
- S/MIME
- Object Signing
- SSL CA
- S/MIME CA
- Object Signing CA

Добавить Отмена

Во вкладке «Netscape расширение» можно указать использование ключа для совместимости со старыми Netscape приложениями (выпущенными до принятия стандарта X.509 v3).

После нажатия кнопки «Добавить» будет предложено зашифровать ключ паролем. Введите пароль или откажитесь от его использования.

Общее Настройки Использование ключа **Netscape расширение**

Шифровать закрытый ключ паролем

Не шифровать закрытый ключ

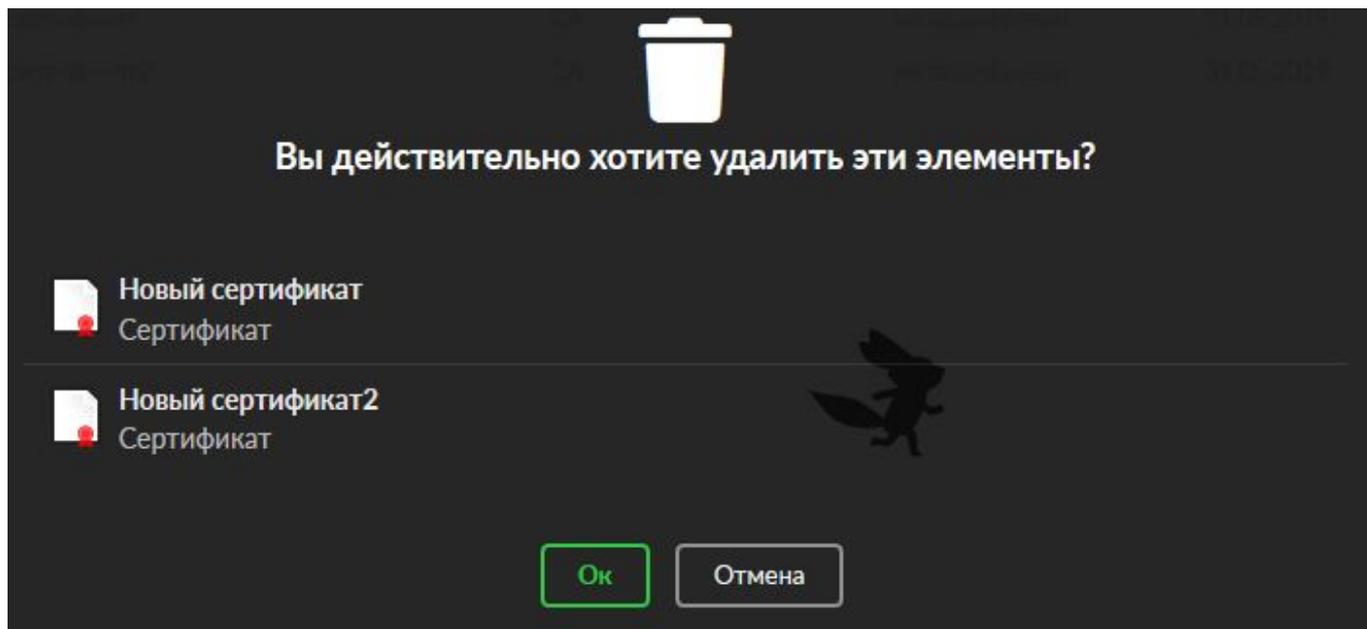
Ок Отмена

Важно: для служб ИКС всегда применяются только нешифрованные сертификаты.

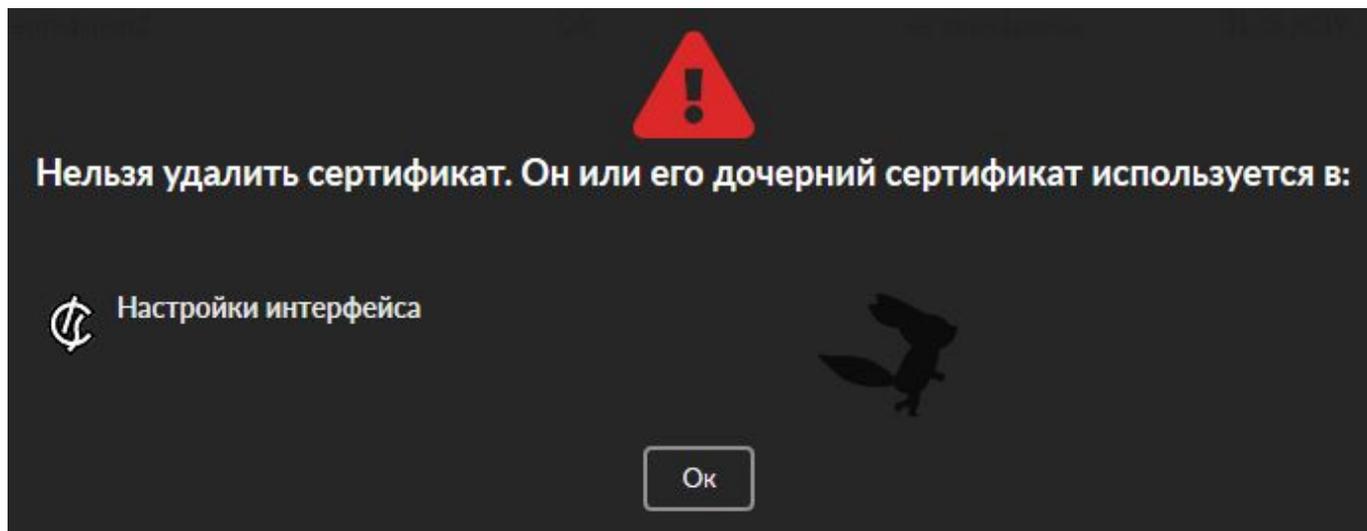
Важно: первоначально всегда должен создаваться корневой сертификат, затем - дочерние конечные сертификаты! К службам ИКС(кроме **SSL-фильтрации**), применяются только конечные сертификаты. Будьте внимательны: неверное применение сертификата к службам может сделать их недоступными для пользователя!

Удаление сертификатов

Для удаления сертификата выделите нужный сертификат в списке (или несколько сертификатов зажав клавишу Ctrl) и нажмите кнопку «Удалить»:



Если сертификат используется какой-либо службой «ИКС», то будет выдано уведомление об ошибке:



Импорт/экспорт сертификатов

Для импорта сертификата нажмите кнопку «Импорт»:

Импорт

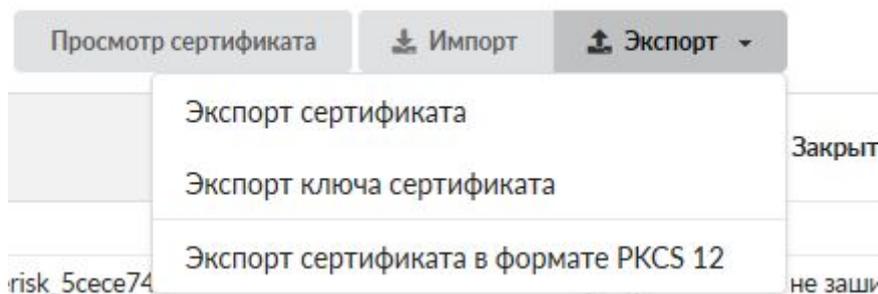
Сертификат * Ключ сертификата

Пароль сертификата в формате PKCS 12

Ок Отмена

В полях «Сертификат» и «Ключ сертификата» выбираются файл сертификата и файл ключа соответственно. Для импорта сертификата в формате PKCS12 необходимо в поле «Сертификат» выбрать соответствующий файл и в поле «Пароль сертификата в формате PKCS 12» указать пароль.

Для экспорта сертификата нажмите кнопку «Экспорт» и выберите необходимый вариант:



Просмотр сертификата

Для просмотра выделите нужный сертификат в списке и нажмите кнопку «Просмотр сертификата»:

Данные сертификата Autogenerated GUI_5cece744c3edb1.30259507

Общее

Название: Autogenerated GUI_5cece744c3edb1.30259507
Код страны: RU - Russian Federation
Имя или адрес хоста: ics-gui

Настройки

Тип сертификата: Конечный сертификат
Алгоритм: SHA 256
Тип шифрования: RSA
Создан: 28.05.2019
Действует до: 29.05.2029
Длина ключа: 2048 бит

Использование ключа

Использование ключа: Digital Signature
Key Encipherment
Расширенное использование ключа: TLS Web Server Authentication

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:serts>

Last update: **2019/11/10 19:25**



Установка доверенного SSL сертификата на сервер

ИКС создает самоподписанные сертификаты, поэтому браузер будет сообщать о недоверенном соединении. **Это нормально!** Если вы хотите использовать доверенные сертификаты, подписанные центром сертификации, необходимо выполнить нижеследующую инструкцию.

Если вы приобрели доверенный SSL сертификат, его необходимо преобразовать в **один файл .pem** (бандл), содержащий цепочку полученных сертификатов: `SSL_Certificate` → `Intermediate Certificate` → `Root Certificate`. Для этого откройте текстовый редактор и вставьте все тело каждого сертификата в один текстовый файл в следующем порядке:

- SSL Main Certificate (Основной сертификат) - `your_domain_name.crt`
- Intermediate Certificate (Промежуточный сертификат) - `DigiCertCA.crt`
- Root Certificate (Корневой сертификат) - `TrustedRoot.crt`

Результат должен выглядеть так:

```
-----BEGIN CERTIFICATE-----
#Your SSL Certificate (your_domain_name.crt)#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Intermediate Certificate (DigiCertCA.crt)#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Root Certificate (TrustedRoot.crt)#
-----END CERTIFICATE-----
```

Сделать это так же можно командой

```
cat your_domain_name.crt DigiCertCA.crt TrustedRoot.crt > yourDomain_bundle
```

Полученный файл Вы можете импортировать (как сертификат) на ИКС через веб-интерфейс в разделе [сертификаты](#)

Приватный ключ

Поддерживается только незашифрованный приватный ключ

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:setupserts>

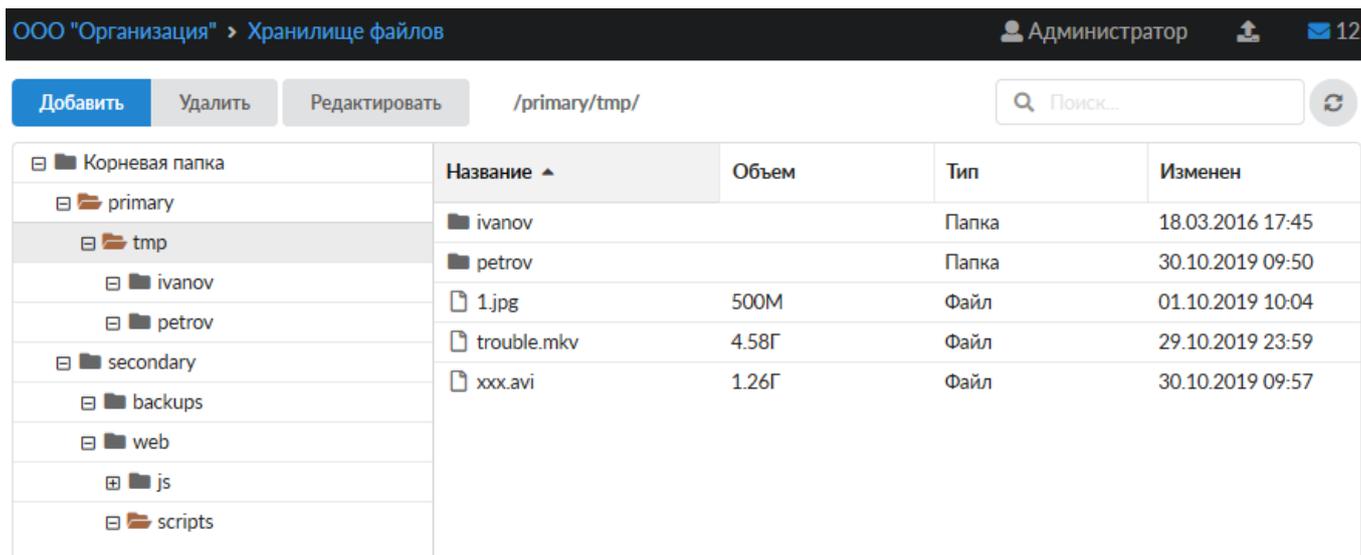
Last update: **2019/11/10 19:25**



Хранилище файлов

Общие положения

Хранилище файлов представляет собой список всех пользовательских ресурсов, расположенных на ИКС. Модуль состоит из двух частей: в левой части общее дерево папок, в правой - список файлов и папок выделенной папки в дереве. Также в левой части содержится информация об объеме папки или файла, типе, а также дате последнего изменения.



Посредством кнопок на верхней панели можно создавать, удалять и переименовывать все папки за исключением primary и папок, соответствующих разделам жестких дисков ИКС - эти папка являются корневыми и не подлежат редактированию.

Действия с папками

Поскольку хранилище файлов является универсальным центром контроля пользовательских ресурсов, вы можете создавать различные шары непосредственно из модуля. Для этого нужно выделить нужную папку в правой части модуля, нажать на появившуюся кнопку «Открыть доступ» и выбрать тип создаваемого ресурса: Веб-ресурс, Виртуальный хост, FTP-ресурс или Общий ресурс. После этого откроется окно добавления соответствующего ресурса.

Название ▲	Объем	Тип	Изменен
js		Папка	30.10.2019 09:50
<input checked="" type="checkbox"/> Разрешить веб-серверу запись			
Открыть доступ ▼			
scripts		Папка с открытым	
Веб-ресурс			
Виртуальный хост			
FTP-ресурс			
Общий ресурс			

Если к папке открыт доступ, то при выделении папки появится информация о ресурсе со ссылкой на соответствующий ресурс:

scripts		Папка с открытым ...	30.10.2019 09:50
Веб-ресурс:  scripts (http://192.168.17.246/scripts)			
<input checked="" type="checkbox"/> Разрешить веб-серверу запись			
Открыть доступ ▼			

В некоторых случаях веб-серверу требуются дополнительные права для работы с файлами. Для таких ситуаций используются расширенные настройки ресурса. Для того, чтобы разрешить веб-серверу запись в папку, выделите ресурс в правой части модуля и установите флажок «Разрешить веб-серверу-запись».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:storage>

Last update: **2019/11/10 19:25**



Веб

Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными. Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором это программное обеспечение работает. Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы — это HTML-страницы, изображения, файлы, медиа-поток или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Модуль «Веб» расположен в Меню «Файловый сервер». Данный модуль предназначен для настройки и управления веб-сервера и содержит четыре вкладки: «Веб-сервер», «Настройки», «Веб-ресурсы» и «Журнал».

Веб-сервер

ООО "Организация" > Веб-сервер Администратор 14

Веб-сервер Настройки Веб-ресурсы Журнал

Веб-сервер запущен
Отвечает за веб-доступ к файлам Выключить

Журнал

- [core:notice] [pid 54868] AH00094: Command line: '/usr/local/sbin/httpd -D NOHTTPACCEPT' 10:43:07
- [mpm_prefork:notice] [pid 54868] AH00163: Apache/2.4.41 (FreeBSD) configured -- resuming normal operations 10:43:07
- [mpm_prefork:notice] [pid 44205] AH00169: caught SIGTERM, shutting down 10:43:07
- nss_ldap: could not search LDAP server - Server is unavailable 10:32:34
- nss_ldap: failed to bind to LDAP server ldapi://127.0.0.1: Can't contact LDAP server 10:32:34

Вкладка «Веб-сервер». На данной вкладке отображается состояние веб-сервера, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки

Веб-сервер	Настройки	Веб-ресурсы	Журнал
Имя хоста * <input type="text" value="company.ru"/>		E-mail администратора * <input type="text" value="admin@company.ru"/>	
Порт HTTP * <input type="text" value="80"/>		Порт HTTPS * <input type="text" value="443"/>	
<input type="checkbox"/> Перенаправлять с HTTP на HTTPS		Сертификат для HTTPS <input type="text" value="(не использовать)"/>	

Вкладка «Настройки». Данная вкладка предназначена для настройки веб-сервера ИКС.

Поле «Имя хоста» определяет внешнее доменное имя хоста. Необходимо для корректной работы веб-ресурса по доменному имени.

Поле «E-mail администратора» позволяет указать e-mail ответственного за веб-сервера системного администратора на тот случай, если в работе сервера возникнут перебои.

Поле «Порт HTTP» предназначено для указания порта, по которому веб-сервер принимает HTTP-запросы (по умолчанию 80).

Поле «Порт HTTPS» предназначено для указания порта, по которому веб-сервер принимает HTTPS-запросы (по умолчанию 443).

В поле «Сертификат для HTTPS» можно назначить службе заранее созданный в соответствующем модуле сертификат для работы сервера по защищённому протоколу HTTPS с использованием SSL.

Флаг «Перенаправлять с HTTP на HTTPS» предназначен, чтобы веб-сервер всегда работал по защищенному соединению.

Автоматически создавать разрешающее правило

Доступ к WEB-серверу

Тип авторизации

Через домен

Учетная запись ИКС

Флаг «Автоматически создавать разрешающее правило» создает разрешающее правило в межсетевом экране на HTTP/HTTPS-порты веб-сервера из внешних сетей. **Внимание!** При установке данного флага будет открыта уязвимость Anti DNS Pinning (DNS rebinding), при данном действии вся ответственность полностью ложится на системный администратор.

Тип авторизации позволяет определить, каким образом пользователи будут авторизоваться на

ресурсе при входе, если веб-ресурс или виртуальный хост не предназначены для гостевого входа.

Веб-ресурсы

Веб-сервер Настройки **Веб-ресурсы** Журнал

Добавить ▾ Удалить Редактировать 🔍 Поиск... ↻

 **blablabla.com** (<http://blablabla.com>)
Ссылка на виртуальный хост

 **myhost.ru** (<http://myhost.ru>)
Виртуальный хост - сайт

Источник: 📁 /secondary/web/

DNS-записи: 🏠 @.myhost.ru. 🏠 ns1.myhost.ru. 🌐 www.myhost.ru.

База данных... Удалить Редактировать Выключить

 **scripts** (<http://192.168.17.246/scripts>)
Веб-ресурс

Вкладка «Веб-ресурсы». Данная вкладка предназначена для управления собственными интернет-сайтами, размещенными на ИКС.

В ИКС можно создавать следующие типы веб-ресурсов:

Веб-ресурс	Отвечает на http-запросы по ip-адресам интерфейсов ИКС.
Виртуальный хост	Позволяет создать неограниченное количество веб-ресурсов, отвечающих каждый за свой веб-сайт по имени сайта.
Виртуальный хост с перенаправлением	Позволяет ИКС перенаправлять запросы на указанное имя сайта в случае, когда сам сервер с сайтом находится к примеру в локальной сети предприятия (аналог перенаправления портов)
Ссылка на виртуальный хост	Создает псевдоним для виртуального хоста

Веб-ресурс

Добавление веб-ресурса

Имя ресурса *	Описание
<input type="text" value="scripts"/>	<input type="text"/>
Источник *	
<input type="text" value="/secondary/web/scripts/ ✕"/>	
<input type="checkbox"/> Разрешить листинг директорий	
<input checked="" type="checkbox"/> Разрешить выполнение PHP скриптов	
Кодировка по умолчанию	
<input type="text" value="UTF-8 Unicode"/>	

Для добавления веб-ресурса необходимо нажать «Добавить» - «Веб-ресурс», откроется диалоговое окно, в котором будет предложено ввести «Имя ресурса», «Источник» (обязательные параметры) и «Описание» (не обязательный параметр). Имя ресурса может быть любым доменным именем. Источник - это директория из структуры хранилища файлов ИКС, в которой будет располагаться содержимое сайта. При необходимости, возможно создать новую папку в каталоге. Описание предназначено для краткого описания ресурса, которое будет отображаться в списке веб-ресурсов, а также в хранилище файлов рядом с соответствующей папкой.

Флаг «Разрешить листинг директории» позволяет серверу отобразить список всех файлов и папок ресурса, в случае если в корневой папке не обнаружены индексные файлы index.html или index.php.

Флаг «Разрешить выполнение PHP скриптов» разрешает серверу выполнять на html-страницах php-скрипты.

Поле «Кодировка по умолчанию» определяет значение кодировки отображаемых html-страниц ресурса по умолчанию.

Дерево «Права доступа» позволяет определить список пользователей, имеющих доступ к чтению и записи на этом ресурсе. Установка флагов «Гостевой вход» позволяет просмотр и запись любым источником.

Права доступа

Имя ▲	Логин	Чтение	Запись
☐ Корневая группа		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Муми-дол		<input type="checkbox"/>	<input type="checkbox"/>
☐ Мумики		<input type="checkbox"/>	<input type="checkbox"/>
☐ Снорки		<input type="checkbox"/>	<input type="checkbox"/>
👤 Морра		<input type="checkbox"/>	<input type="checkbox"/>
👤 Снусмумрик		<input type="checkbox"/>	<input type="checkbox"/>
👤 Туге Янссон	root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Гостевой вход		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Виртуальный хост

Основной ресурс при создании сайта - виртуальный хост. Для добавления виртуального хоста необходимо нажать «Добавить» - «Виртуальный хост», откроется диалоговое окно, в котором будет предложено ввести «Виртуальный хост», «Описание» (необязательные параметры) и «Источник» (обязательный параметр). Виртуальный хост аналогичен имени веб-ресурса, но должен содержать доменное имя сайта, на которое он будет отвечать по http-запросу. Для корректной работы виртуального хоста в большинстве случаев требуется настройка dns-зон доменного имени.

Настройка виртуального хоста схожа с настройкой веб-ресурса. Кроме указанных настроек, в виртуальном хосте можно также настроить следующие параметры:

- Создать ссылку для www.myhost.ru
- Использовать Web Application Firewall

Флаг «Создать ссылку для *www.%domainname%*» предназначен для настройки DNS-записей для приема http-запросов как на имя сайта, указанное в названии, так и на него же с добавлением домена WWW.

Флаг «Использовать Web Application Firewall» подключает модуль [Web Application Firewall](#)

Настройки HTTPS

- Использовать настройки веб-сервера
- Использовать сертификат LetsEncrypt
- Указать сертификат вручную:

Перенаправлять с HTTP на HTTPS

Создать запись на DNS-сервере

Блок «Настройки HTTPS» предназначен для выбора для использования общих настроек веб-сервера, сертификата LetsEncrypt, либо указания данному сайту заранее созданный в соответствующем модуле сертификат. Указание сертификата вручную активирует флаг «Перенаправлять с HTTP на HTTPS», необходимый, чтобы данный сайт всегда работал по защищенному соединению.

Флаг «Создать запись на DNS-сервере» создает зону для данного хоста, а также записи на DNS-сервере ИКСа:

📁 myhost.ru.			
📁 myhost.ru.	NS (авто)		ns1.myhost.ru.
📁 @.myhost.ru.	A		192.168.170.246
📁 ns1.myhost.ru.	A		192.168.170.246
📁 www.myhost.ru.	CNAME		myhost.ru.

Также, как и веб-ресурс, вы можете настроить уровень доступа пользователей (только чтение) к виртуальному хосту.

Виртуальный хост с перенаправлением

Добавление виртуального хоста с перенаправлением

Виртуальный хост	Описание
<input type="text" value="test.local"/>	<input type="text" value="тестовая страница"/>

Перенаправлять HTTP на адрес

Перенаправлять HTTP на HTTPS

Перенаправлять HTTPS на адрес

Для добавления виртуального хоста с перенаправлением необходимо нажать «Добавить» - «Виртуальный хост с перенаправлением», откроется диалоговое окно, в котором будет предложено ввести «Виртуальный хост», «Описание» (необязательные параметры) и адрес для перенаправления (обязательный параметр).

Выбор режима перенаправления «Перенаправлять HTTP на адрес» активирует поле для ввода адреса, на который будут перенаправляться http-запросы, «Перенаправлять HTTP на HTTPS» - перенаправляет http запросы на https.

Поле «Перенаправлять HTTPS на адрес» предназначено для ввода адреса, на который будут перенаправляться https-запросы.

В качестве адресов для перенаправления возможно указывать: IP-адрес; домен, в том числе русскоязычный; <домен:порт>; <путь_до_файла>.

Настройка флагов «Создать запись на DNS-сервере» и «Использовать Web Application Firewall» аналогична соответствующим флагам виртуального хоста.

Ссылка на виртуальный хост

Добавление ссылки на виртуальный хост

Ссылка *	Описание
<input type="text" value="blablabla.com"/>	<input type="text"/>
Виртуальный хост *	
<input type="text" value="myhost.ru (http://myhost.ru) x"/>	
<input checked="" type="checkbox"/> Создать запись на DNS-сервере	
<input type="button" value="Добавить"/> <input type="button" value="Отмена"/>	

Если на ИКС создан виртуальный хост, и необходимо, чтобы он отвечал на запросы по другому доменному имени, можно воспользоваться ссылкой. Для добавления ссылки необходимо нажать «Добавить» - «Ссылка на виртуальный хост», откроется диалоговое окно, в котором будет предложено ввести «Ссылку», «Виртуальный хост» (обязательные параметры) и «Описание» (необязательный параметр). В качестве ссылки необходимо указать имя псевдонима, а поле «Виртуальный хост» выбрать из списка созданных виртуальных хостов тот, к которому будет относиться данная ссылка.

Настройка флага «Создать запись на DNS-сервере» аналогична соответствующему флагу виртуального хоста.

База данных

Каждый раз, когда создается новый веб-ресурс или виртуальный хост, в сервере баз данных MySQL за ним закрепляется база данных, с которой может взаимодействовать сайт, расположенный на ресурсе, посредством php-запросов. Для того, чтобы увидеть параметры базы данных ресурса, необходимо выделить его в общем списке и нажать кнопку «База данных».

Информация о базе данных



myhost.ru

Имя базы данных: db_d0735a48
Пользователь: user_d0735a48
Пароль: 10a302c

Скачать базу Очистить базу Загрузить базу **Ок**

Откроется диалоговое окно с параметрами подключения к базе данных: имя базы, логин и пароль для подключения. Эти параметры необходимо использовать для подключения к базе из php-скриптов. Также в окне отобразятся три функциональные кнопки:

- Кнопка «Скачать базу» предназначена для экспорта дампа базы данных ресурса.
- Кнопка «Очистить базу» предназначена для очистки базы данных ресурса.
- Кнопка «Загрузить базу» предназначена для загрузки дампа рабочей базы данных. При нажатии будет открыто новое диалоговое окно, в котором будет предложено выбрать файл дампа для загрузки, кодировку дампа, а также отметить флаг, определяющий сохранность предыдущих данных в базе после загрузки.

Загрузка базы данных в «ИКС» происходит асинхронно, это позволяет продолжить работу с «ИКС» не дожидаясь окончания загрузки. Процесс загрузки будет показан с права сверху. Во время загрузки кнопки «Редактировать», «Выключить», «Удалить», а так же «База данных» становятся недоступными. Отменить загрузку базы возможно через кнопку «Загрузка файлов» на верхней панели главного меню.

Журнал

Веб-сервер Настройки Веб-ресурсы **Журнал**

30.10.2019 - 30.10.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

↓ ↑

[mpm_prefork:notice] [pid 73352] AH00169: caught SIGTERM, shutting down
10:31:08

[mpm_prefork:notice] [pid 44205] AH00163: Apache/2.4.41 (FreeBSD) configured -- resuming normal operations
10:31:08

[core:notice] [pid 44205] AH00094: Command line: '/usr/local/sbin/httpd -D NOHTTACCEPT'
10:31:08

nss_ldap: failed to bind to LDAP server ldap://127.0.0.1: Can't contact LDAP server
10:32:31

nss_ldap: failed to bind to LDAP server ldapi://127.0.0.1: Can't contact LDAP server
10:32:31

Вкладка «Журнал». Отображает сводку всех системных сообщений службы «Веб-сервер» 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) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:web>

Last update: **2019/11/10 19:25**

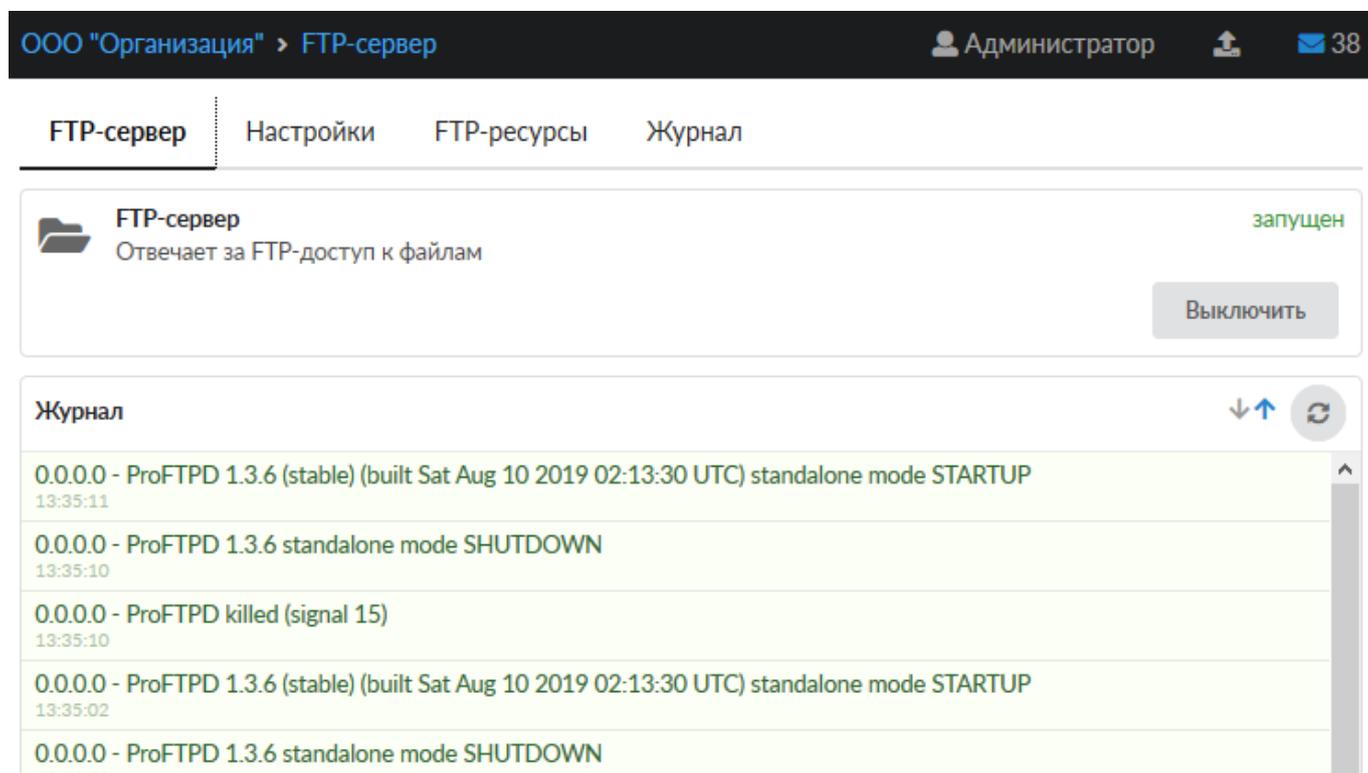


FTP

FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP—сервер позволяет размещать на сервере файлы и предоставлять им доступ по сети. Поддерживается анонимный вход и авторизация по логину и паролю. Для пользователей можно задавать различные права доступа.

Модуль «FTP» расположен в Меню «Файловый сервер». Данный модуль предназначен для настройки и управления ftp-сервером и содержит четыре вкладки: «FTP-сервер», «Настройки», «FTP-ресурсы» и «Журнал».

FTP-сервер



Вкладка «FTP-сервер». На данной вкладке отображается состояние ftp-сервера, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Примечание. При работе с FTP-сервером «ИКС» рекомендуется: использовать FTP-клиент с кодировкой UTF-8; название папок и файлов должно быть латиницей. В случаях не исполнения данных рекомендаций могут возникнуть проблемы при работе с FTP-сервером.

Настройки

FTP-сервер	Настройки	FTP-ресурсы	Журнал
Порт *		Порты для пассивного FTP *	
<input type="text" value="21"/>		<input type="text" value="10000-10030"/>	
<input checked="" type="checkbox"/> Автоматически создавать разрешающее правило		<input checked="" type="checkbox"/> Автоматически создавать разрешающее правило	
<input checked="" type="checkbox"/> Доступ к FTP-серверу		<input checked="" type="checkbox"/> Доступ для пассивного FTP	

Вкладка «Настройки». Данная вкладка предназначена для настройки ftp-сервера ИКС.

Поле «Порт» определяет порт передачи данных протокола (по умолчанию стандартный порт 21)

Поле «Порты для пассивного FTP» предназначен для указания диапазона 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 этот диапазон.

Флаги «Автоматически создавать разрешающее правило» создают разрешающие правила в межсетевом экране на соответствующие порты ftp-сервера из внешних сетей.

Максимальное количество соединений *	
<input type="text" value="30"/>	
Максимальное количество подключений с одного логина	Максимальное количество подключений с одного хоста
<input type="text" value="0"/>	<input type="text" value="0"/>
Сертификат для FTPS	
<input type="text" value="Нет"/>	

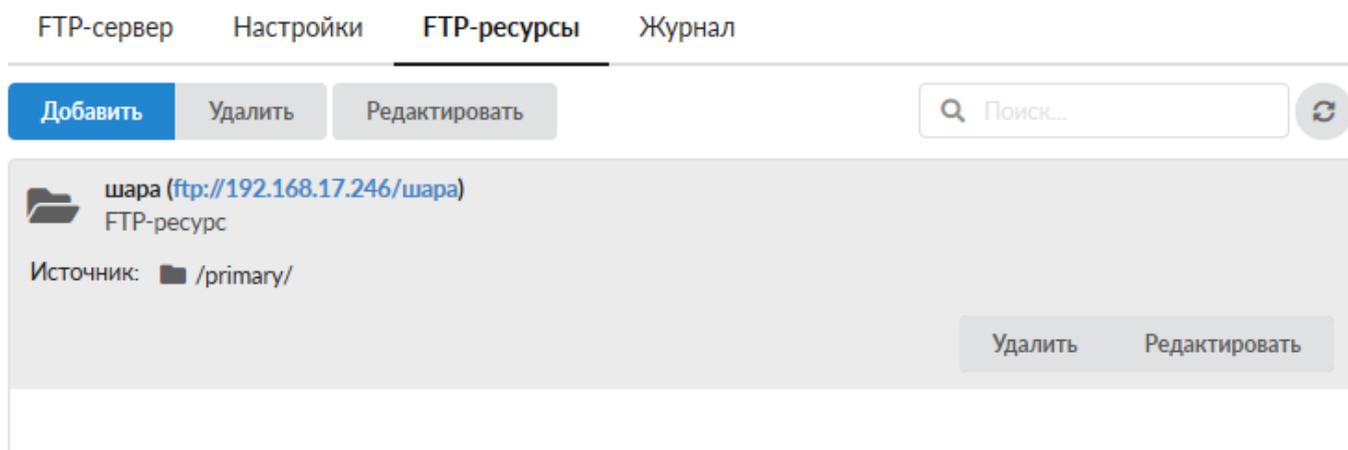
Поле «Максимальное количество соединений» задает максимальное количество одновременно подключенных клиентов.

Поле «Максимальное количество подключений с одного логина» ограничивает пользователя числом одновременно создаваемых FTP-сессий с его логина (по умолчанию не ограничено).

Поле «Максимальное количество подключений с одного хоста» ограничивает пользователя числом подключений с одного ip-адреса (по умолчанию не ограничено).

В поле «Сертификат для FTPS» можно назначить службе заранее созданный в соответствующем модуле сертификат для работы сервера по защищённому протоколу FTPS с использованием SSL.

FTP-ресурсы



Вкладка «FTP-ресурсы». Данная вкладка предназначена для управления ftp-ресурсами, размещенными на ИКС.

Для добавления ftp-ресурса необходимо нажать кнопку «Добавить», откроется диалоговое окно, в котором будет предложено ввести «Имя ресурса», «Источник» (обязательные параметры) и «Описание» (не обязательный параметр). Источник - это директория из структуры хранилища файлов ИКС, в которой будет располагаться содержимое FTP-шары. При необходимости, возможно создать новую папку в каталоге. Описание предназначено для краткого описания ресурса, которое будет отображаться в списке ftp-ресурсов, а также в хранилище файлов рядом с соответствующей папкой.

Добавление FTP-ресурса

Имя ресурса *	Описание
<input type="text" value="шара"/>	<input type="text"/>
Источник *	
<input type="text" value="/primary/ ✕"/>	

Дерево «Права доступа» позволяет определить список пользователей, имеющих доступ к чтению и записи на этом ресурсе. Установка флагов «Гостевой вход» позволяет просмотр и запись любым источником:

Права доступа

Имя ▲	Логин	Чтение	Запись
Корневая группа		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Муми-дол		<input type="checkbox"/>	<input type="checkbox"/>
Мумики		<input type="checkbox"/>	<input type="checkbox"/>
Снорки		<input type="checkbox"/>	<input type="checkbox"/>
Морра		<input type="checkbox"/>	<input type="checkbox"/>
Снусмумрик		<input type="checkbox"/>	<input type="checkbox"/>
Туге Янссон	root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Гостевой вход		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Журнал

FTP-сервер Настройки FTP-ресурсы **Журнал**

30.10.2019 - 30.10.2019 Сегодня Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

mod_ctrls/0.9.5: error: unable to bind to local socket: Address already in use
10:32:09

0.0.0.0 - ProFTPD 1.3.6 (stable) (built Sat Aug 10 2019 02:13:30 UTC) standalone mode STARTUP
10:32:11

0.0.0.0 - mod_lang/1.1: LangDefault 'ru', configured for server 'ftp server', is not a supported language, removing
10:32:11

0.0.0.0 - mod_lang/1.1: Perhaps proftpd has not yet been translated into 'ru'
10:32:11

Вкладка «Журнал». Отображает сводку всех системных сообщений службы «FTP-сервер» 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) - 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».

Особенности функционирования

При размещении двух и более FTP-ресурсов на «ИКС», а также открытия к одному из них «Гостевого доступа». Необходимо учитывать следующий аспект – для доступа к FTP-ресурсу через браузер, у которого нет гостевого доступа, необходимо обращаться ftp://логин_ftp:пароль_ftp@имя_ресурса.

В браузере Firefox если указан явный прокси и настроена NTLM авторизация FTP-ресурс будет доступен. В других браузерах не гарантируется доступ к FTP-ресурсу при данных настройках.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:ftp>

Last update: **2019/11/10 19:25**



Сетевое окружение

Для обмена данными в локальной сети используется протокол SMB (сокр. от англ. Server Message Block) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. В ИКС за реализацию этого протокола отвечает служба «Сетевое окружение».

Модуль «Сетевое окружение» расположен в Меню «Файловый сервер». Данный модуль предназначен для настройки и управления удаленным доступом и содержит четыре вкладки: «Сетевое окружение», «Настройки», «Общие ресурсы» и «Журнал».

Сетевое окружение

ООО "Организация" > Сетевое окружение Администратор 42

Сетевое окружение Идентификация Общие ресурсы Журнал

Сетевое окружение запущен
Отвечает за интеграцию с сетями Windows Выключить

Журнал ↓↑ ↻

- Entering to the domain: Succeeded to join domain - The requested operation was successful. 14:03:50
- Entering to the domain: Failed to join domain: failed to find DC for domain OFFICE1 - {Operation Failed} The requested operation was unsuccessful. 14:03:13
- daemon_ready: daemon 'smbd' finished starting up and ready to serve connections 10:32:52

Вкладка «Сетевое окружение». На данной вкладке отображается состояние службы, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Идентификация

Сетевое окружение **Идентификация** Общие ресурсы Журнал

Имя компьютера Описание

ICS

Автоматически создавать разрешающее правило

Доступ к общим Windows-ресурсам

Вкладка «Идентификация». Данная вкладка предназначена для определения режима

работы ИКС в локальной сети предприятия.

Поле «Имя компьютера» отвечает за назначение сетевого NetBIOS-имени для сервера.

Флаг «Автоматически создавать разрешающее правило» создает разрешающее правило в межсетевом экране для доступа к общим ресурсам из внешних сетей.

ИКС может находиться в рабочей группе либо быть присоединен к домену:

Рабочая группа	В сети предприятия не используется контроллер домена (AD), компьютеры находятся в одной рабочей группе, WINS-сервер отсутствует. По умолчанию ИКС находится в рабочей группе WORKGROUP, при необходимости ее возможно переименовать. Важно! Пользователи, имеющие в логине «\», не смогут авторизоваться (например, доменные).
Домен	В сети предприятия используется контроллер домена (AD). ИКС может быть присоединен к домену. Это позволит импортировать доменных пользователей, синхронизировать их, а также использовать доменную авторизацию на сетевых ресурсах ИКС. Важно! Авторизуются только доменные Пользователи.

При выборе режима «Рабочая группа » активируется поле для ввода названия группы.

При выборе режима «Домен » активируется блок полей, предназначенных для подключения к контроллеру домена (имя домена, DNS имя домена, а также нужно ли создавать перенаправление DNS-зоны, так как часто DNS-зона, в которой находится домен не может быть разрешена внешними DNS-серверами):

Рабочая группа

WORKGROUP

Домен

Имя домена

OFFICE1

DNS имя домена

OFFICE1.TEST.LOCAL

 ИКС успешно присоединен к домену

Создавать перенаправление DNS-зоны

DNS-сервер для перенаправления *

192.168.45.45

 OFFICE1.TEST.LOCAL

Флаг «Принудительно подписывать SMB запросы» отвечает за подписывание с помощью SMB. Подписывание SMB - механизм обеспечения безопасности протокола SMB, также называемый

подписями безопасности. Подписывание SMB предназначено для повышения безопасности протокола SMB. Может не поддерживаться старыми операционными системами (Win98, WinXP).

Принудительно подписывать SMB запросы

Подключиться

Обновить

Отключиться

После нажатия кнопки «Подключиться» ИКС применит выбранную роль в сетевом окружении. Если выбран роль «Домен», то сервер запросит логин и пароль пользователя с правами администратора для присоединения к домену.

Внимание: для того, чтобы ИКС мог присоединиться к домену и обмениваться данными с контроллером, необходимо, чтобы сервер-контроллер домена был занесен в список пользователей ИКС, и его авторизация проходила по ip-адресу. Так же необходимо, что бы ИКС использовал DNS контроллера домена.

После попытки подключения к домену, под полем с именем домена появится сообщение об успешном или неуспешном результате.

Общие ресурсы

Сетевое окружение Идентификация **Общие ресурсы** Журнал

Добавить Удалить Редактировать Поиск... ↻

primary (\\ICS\primary)
Общий ресурс
Источник: /primary/tmp/ Удалить Редактировать

Вкладка «Общие ресурсы». Данная вкладка предназначена для управления общими ресурсами, размещенными на ИКС.

Для добавления общего ресурса необходимо нажать кнопку «Добавить», откроется диалоговое окно, в котором будет предложено ввести «Имя ресурса», «Источник» (обязательные параметры) и «Описание» (не обязательный параметр). Источник - это директория из структуры хранилища файлов ИКС, в которой будет располагаться содержимое сетевой шары. При необходимости, возможно создать новую папку в каталоге. Описание предназначено для краткого описания ресурса, которое будет отображаться в списке общих ресурсов, а также в хранилище файлов рядом с соответствующей папкой.

Добавление общего ресурса

Имя ресурса * Описание

Источник *

Дерево «Права доступа» позволяет определить список пользователей, имеющих доступ к чтению и записи на этом ресурсе. Установка флагов «Гостевой вход» позволяет просмотр и изменение файлов шары любому подключившемуся к серверу.

Права доступа (авторизация через домен)

Имя ▲	Логин	Чтение	Запись
☐ Корневая группа		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
☐ Муми-дол		<input type="checkbox"/>	<input type="checkbox"/>
☐ Мумики		<input type="checkbox"/>	<input type="checkbox"/>
☐ Снорки		<input type="checkbox"/>	<input type="checkbox"/>
👤 Морра		<input type="checkbox"/>	<input type="checkbox"/>
👤 Снусмумрик		<input type="checkbox"/>	<input type="checkbox"/>
👤 Туве Янссон	OFFICE1\root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Гостевой вход		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Стоит отметить, что если ИКС присоединен к домену, то он будет авторизовывать только доменных пользователей.

Важно: следует отметить, что сетевое окружение работает только с логинами, написанными без использования заглавных букв (в случае если ИКС не присоединен к домену).

Важно: особенность приложения samba не позволяет использовать логин root.

Журнал

Сетевое окружение Идентификация Общие ресурсы **Журнал**

30.10.2019 - 30.10.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

↓ ↑

Entering to the domain: Succeeded to join domain - The requested operation was successful.
14:03:50

Entering to the domain: Failed to join domain: failed to find DC for domain OFFICE1 - [Operation Failed] The requested operation was unsuccessful.
14:03:13

daemon_ready: daemon 'smbd' finished starting up and ready to serve connections
10:32:52

Сетевое окружение Идентификация Общие ресурсы **Журнал**

07.05.2019 - 07.05.2019 **Сегодня** Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

↓ ↑

[2019/05/07 13:04:53.022121, 0] ../lib/util/become_daemon.c:124(daemon_ready)
13:04:53

STATUS=daemon 'nmbd' finished starting up and ready to serve connections
13:04:53

[2019/05/07 13:04:53.836038, 0] ../source3/winbindd/winbindd_cache.c:3171(initialize_winbindd_cache)
13:04:53

initialize_winbindd_cache: clearing cache and re-creating with version number 2
13:04:53

Вкладка «Журнал». Отображает сводку всех системных сообщений службы «FTP-сервер» 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) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:samba>

Last update: **2019/11/10 19:25**



Служба

Модуль «Служба» расположен в Меню «Почта». При открытии модуля в основном окне отобразятся вкладки «Почта», «Все службы» и «Журнал», при этом вкладка «Почта» будет активна.

Почта

Муми-дол > Почта

Тыве Янссон

Почта Все службы Журнал

Почтовый сервер запущен
Отправляет и получает почту

Статистика за сегодня
Принято: 155 писем
Отправлено: 36 писем
Спама: не обнаружено
Вирусов: не обнаружено

Выключить

Хранилище почты запущен
Контролирует почтовые домены и ящики

Выключить

07:20 07:40 08:00

- ошибка отправки
- отложено
- отправлено
- не принято
- принято
- спам (rbl)

connect from roundcube.ics.my[172.77.77.254]
03:33:38

Anonymous TLS connection established from roundcube.ics.my[172.77.77.254]: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
03:33:39

1998B3E964: client=roundcube.ics.my[172.77.77.254]
03:33:39

1998B3E964: message-id=<201910180033.x9l0XccF010271@roundcube.ics.my>
03:33:39

Вкладка «Почта». На вкладке отображается состояние основных служб почтового сервера - *Почтовый сервер* и *Хранилище почты* с возможностью «Выключить» (или «Включить» если служба выключена). Также присутствует виджет с информацией о полученных и отправленных письмах, график статистики почты, а также последние события журнала.

Все службы

Поиск...

Название	Состояние
Fail2ban Блокирует IP-адреса, с которых предпринимается слишком много попыток авторизации	запущен
Антиспам Rspamd Проверяет письма на спам, добавляет и проверяет DKIM-подпись	запущен
Антиспам SpamAssassin Проверяет письма на спам	не настроен
Веб-почта Предоставляет веб-доступ к почтовым ящикам ИКС	запущен
Почтовый сервер Отправляет и получает почту	запущен
Сборщик почты Получает почту с удаленного почтового сервера	выключен

Вкладка «Все службы». На вкладке отображается состояние всех служб почтового сервера, которые есть в ИКС с возможностью «Выключить» (или «Включить» если служба выключена). 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 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

Журнал

18.10.2019 - 18.10.2019 **Сегодня** Неделя Месяц Другой период

Экспорт Удалить логи

Поиск...

```

connect from roundcube.ics.my[172.77.77.254]
03:33:38
Anonymous TLS connection established from roundcube.ics.my[172.77.77.254]: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
03:33:39
1998B3E964: client=roundcube.ics.my[172.77.77.254]
03:33:39
1998B3E964: message-id=<201910180033.x910XccF010271@roundcube.ics.my>
03:33:39
1998B3E964: from=<root@roundcube.ics.my>, size=171412, nrcpt=1 (queue active)
03:33:39
disconnect from roundcube.ics.my[172.77.77.254] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
03:33:39

```

Вкладка «Журнал». Ображает 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:mail>

Last update: **2019/11/10 19:25**



Настройки почтового сервера

Модуль «Настройки» расположен в Меню «Почта». Данный модуль предназначен для настройки почтового сервера и содержит три вкладки: «Настройки», «Защита от спама» и «Адресная книга».

Вкладка «Настройки»

Сетевые настройки.

Порт SMTP *	Порт POP3 *	Порт IMAP *
<input type="text" value="25"/>	<input type="text" value="110"/>	<input type="text" value="143"/>
<input checked="" type="checkbox"/> Автоматически создавать разрешающее правило		
Интерфейсы для SMTP	Интерфейсы для POP3/IMAP	
<input type="text" value="(все)"/>	<input type="text" value="(все)"/>	

Порт SMTP:	<input type="text" value="25"/>
Порт POP3:	<input type="text" value="110"/>
Порт IMAP:	<input type="text" value="143"/>

Интерфейсы для SMTP:	<input type="text" value="(все)"/>
Интерфейсы для POP3/IMAP:	<input type="text" value="(все)"/>

Порт SMTP/POP3/IMAP - позволяет изменить стандартные порты приема и отправки почтовых сообщений. Поля «Интерфейсы для SMTP» и «Интерфейсы для POP3/IMAP» предназначены для указания интерфейсов, заданных на «ИКС», на которых будут работать протоколы SMTP/POP3/IMAP. По умолчанию работа идет на всех интерфейсах. При установке флажка в поле «Автоматически создавать разрешающее правило» будет выполнена установка разрешающего правила в межсетевом экране для портов SMTP/POP3/IMAP. Перейти к списку существующих правил и их настройке можно щелкнув по появившейся гиперссылке «Доступ к почтовому серверу».

Шифрование

Почтовый сервер «ИКС» по умолчанию работает в режиме «**Без шифрования**» по протоколам SMTP, POP3/IMAP. Данный режим рекомендуется использовать только в защищенной сети. Так как в данном режиме злоумышленники, при помощи прослушивания канала, могут получить информацию об имени и пароле Пользователя.

Режим «**Необязательное**». Если ПО клиента не поддерживает шифрование, пароль передается по не зашифрованному каналу, в открытом виде. Если ПО клиента поддерживает шифрование, то авторизация происходит уже внутри шифрованного соединения.

Режим «**С шифрованием**». В этом режиме при авторизации Пользоваться по протоколам SMTP, POP3/IMAP, STARTTLS пароль передается только внутри шифрованного соединения.

Ниже описана настройка блока «Шифрование» для режимов «Необязательное» и «С шифрованием».

SMTP <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">С шифрованием ▾</div> Сертификат <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Autogenerated MailServer_5da8560bcf7501.40267528 ✕</div> <input checked="" type="checkbox"/> Включить SMTPS Порт SMTPS * <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">465 ⬆ ⬇</div> <input checked="" type="checkbox"/> Автоматически создавать разрешающее правило <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">✔ Доступ к почтовому серверу по SMTPS</div>	POP3/IMAP <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">С шифрованием ▾</div> Сертификат <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Autogenerated MailServer_5da8560bcf7501.40267528 ✕</div> <input checked="" type="checkbox"/> Включить POP3S/IMAPS Порт POP3S * <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">995 ⬆ ⬇</div> Порт IMAPS * <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">993 ⬆ ⬇</div> <input checked="" type="checkbox"/> Автоматически создавать разрешающее правило <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">✔ Доступ к почтовому серверу по POP3S/IMAPS</div> Длина ключа DH (Diffie-Hellman) <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">2048 бит ▾</div>
--	---

- Поле «Сертификат для SMTP» - позволяет выбрать сертификат для протокола SMTP из заведенных на «ИКС». Включает использование шифрованного соединения по методу STARTTLS поверх использования обычного TCP-соединения по протоколу SMTP на стандартном 25 порту. Данное шифрование является компромиссным. Если удаленная сторона не поддерживает шифрование, то письмо будет отправляться/приниматься по не зашифрованному протоколу SMTP.
- Поле «Сертификат для IMAP/POP3» - позволяет выбрать сертификат для протоколов IMAP/POP3 из заведенных на «ИКС». Включает использование шифрованного соединения по методу STARTTLS поверх использования обычного TCP-соединения по протоколам IMAP/POP3 на стандартных портах 143/110 соответственно.

- Флаги «Включить SMTPS» и «Включить POP3S/IMAPS» позволяют включить шифрование для протоколов SMTPS, IMAPS, POP3S на не классических портах в параллель 25/110/143 портам. Главным отличием является обязательное использование шифрования, компромисс не возможен. В почтовом сервере «ИКС» используются только криптографические протоколы TLSv1, TLSv1.1, TLSv1.2. Использование SSL2 и SSL3 для безопасности, отключено.
- Поля «Порт SMTPS», «Порт POP3S», «Порт IMAPS» позволяют задать номера портов для протоколов SMTPS, IMAPS, POP3S соответственно.
- Поле «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. Стоит отметить, что рекомендуемая длина ключа 2048 бит, по умолчанию стоит 1024 бита для оптимизации первого запуска «ИКС».

Отправка писем

Отправка писем:

Максимальный размер письма *

 ^ v Мб

Ограничить частую отправку писем

Максимальное количество писем с одного IP-адреса в минуту

 ^ v

Игнорировать при отправке писем с адресов и сетей из белого списка

Следующие настройки нужны для задания различных ограничений при отправке писем:

- Поле «Максимальный размер письма» - задает ограничение на загрузку вложений через веб-почту (встроенный клиент roundcube).

- Флаг «Ограничить частую отправку писем» - включает ограничения, на отправку писем через почтовый сервер «ИКС».

- Поле «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, отправленные из веб-интерфейса предустановленного клиента электронной почты.

- Флаг «Игнорировать при отправке писем с адресов и сетей из белого списка» - создает исключение в ограничении «Ограничить частую отправку писем» для IP-адресов и сетей указанных в блоке «Белый список» ниже.

Почтовая очередь

Почтовые сообщения, которые не были отправлены, помещаются в очередь на повторную отправку.

Почтовая очередь:

Интервал между попытками отправки *

30 ↑ ↓ мин.

Время ожидания в очереди от *

180 ↑ ↓ мин.

до *

300 ↑ ↓ мин.

Максимальное время нахождения письма в очереди *

5760 ↑ ↓ мин.

Отправка писем:

Максимальный размер письма: 100 ↑ ↓ МБ

Ограничить частую отправку писем:

Максимальное количество писем с одного IP-адреса в минуту: 10 ↑ ↓

Игнорировать при отправке писем с адресов и сетей из белого списка:

Следующие настройки нужны для задания различных интервалов времени при повторной отправке почтовых сообщений:

- Поле «Интервал между попытками отправки» - позволяет задать время запуска демона (демон – это программа работающая в фоновом режиме), через которое он будет проверять время нахождения письма в очереди (по умолчанию составляет 30 минут).

- Поле «Время ожидания в очереди» - позволяет задать интервал времени для письма в очереди, при котором демон попытается повторно отправить данное письмо из очереди (по умолчанию составляет от 180 минут до 300 минут). Например, письмо было не отправлено, при этом демон по умолчанию запускается каждые 30 минут, это означает, что демон запустится через время delta, где delta может принимать значение из промежутка - [0m;30m]. Таким образом повторная отправка будет произведена через 180+delta. В случае, если повторная отправка не произошла, письмо вновь попадает в очередь отправки, счетчик времени нахождения письма в очереди становится равным нулю и нижняя граница (в нашем случае 180 минут) для данного письма будет сдвинута автоматически, но не превысит верхней границы. Попытки отправить письмо будут повторяться до тех пор, пока общее время нахождения письма в очереди не достигнет значения указанного в поле «Максимальное время нахождения

письма в очереди».

- Поле «Максимальное время нахождения письма в очереди» - позволяет указать максимальное общее время нахождения письма в очереди, по достижению которого отправителю будет отправлено уведомление о том, что его письмо было не отправлено (по умолчанию 5760 минут).

Отправка через внешний SMTP.

Релей по умолчанию: Порт:

Использовать SMTPS
 Использовать SMTP-авторизацию

Логин*: Пароль*:

Подменять адрес отправителя

Адрес отправителя*:

Релей по умолчанию: : SSL

Использовать SMTP-авторизацию:

Логин:

Пароль:

Подменять адрес отправителя:

Адрес отправителя:

В «ИКС» можно настроить отправку исходящей почты через другой SMTP-сервер для всех писем, кроме писем адрес назначения которых является локальный домен или получатель. Для того, чтобы включить отправку исходящей почты через другой SMTP-сервер, необходимо прописать его адрес (доменное имя или IP) в поле «релей по умолчанию» и задать порт для подключения. Флаг «SSL» используется только для соединения по протоколу SMTPS на порту 465. Таким образом, флаг для отправки писем на порт назначения 465 обязателен. При соединении на 25 порт, флаг SSL не должна стоять, т.к. 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, то необходимо установить флаг «Использовать SMTP-авторизацию» и указать логин и пароль пользователя. Стоит отметить, что при отправке почтовых сообщений через SMTP сервера mail.ru / yandex.ru / gmail.com и др., необходимо

поставить флаг «Подменять адрес отправителя», т.к. для данных почтовых серверов необходимо, чтобы адрес отправителя (заголовок FROM) совпадал с пользователем, под которым была выполнена авторизация, а также задать адрес отправителя в поле «Адрес отправителя».

Списки ограничений

Списки ограничений:

Белый список

Черный список

Позволяет добавить списки белых и черных адресов, с которых разрешена или запрещена входящая корреспонденция. При нажатии на кнопку «Белый список» будет открыто новое диалоговое окно, в котором возможно добавить: IP-адрес, доменное имя, сеть (в том числе заведенную в «ИКС»), почтовый сервер (например, @mail.ru), почтовый ящик. С которых «ИКС» будет всегда принимать почтовые сообщения без проверки серыми списками и проверки соответствия прямой и обратной записей в DNS, а так же без авторизации. **Внимание! Следует заносить в этот список только отправителей, которым действительно стоит доверять.**

При нажатии на кнопку «Черный список» будет открыто новое диалоговое окно, в котором возможно добавить: IP-адрес, доменное имя, сеть, почтовый сервер (например, @mail.ru), почтовый ящик. С которых «ИКС» не будет принимать почтовые сообщения.

Общие настройки

Домен по умолчанию для авторизации

(не указан)

Жесткий диск для хранения почты *

Основной системный раздел Mirror ✕

Имя сервера в команде SMTP HELO при отправке письма

testics.local

При создании ящика автоматически создавать папки

Sent ✕

Drafts ✕

Junk ✕

Trash ✕

Домен по умолчанию для авторизации

Данный блок позволяет выбрать заведенный на «ИКС» почтовый домен при авторизации клиента. Например, на «ИКС» заведен почтовый домен domain.local, а Пользователю, из

данного домена, задано имя ящика – usermail. То при выборе в данном блоке «domain.local», Пользователь при обращении к почтовому серверу «ИКС» через почтового клиента или через web-интерфейс в поле «Имя пользователя» может указывать только – usermail, а не usermail@domain.local.

Жесткий диск для хранения почты

Данный блок позволяет переместить хранилище почты на отдельный жесткий диск. По умолчанию почта хранится в основном системном разделе (там, где установлен «ИКС»). При изменении места хранения почты, будет произведено копирование всех писем с текущего жесткого диска на новый. Ход копирования почты с диска на диск возможно отслеживать в Меню – Обслуживание – Система – Задачи. Если новый жесткий диск уже содержит файлы с почтой, то копирование производится не будет (только для «ИКС» 5.1.7 и выше).

Имя сервера в команде SMTP HELO при отправке письма

Позволяет задать имя хоста, которое будет передано в команде SMTP HELO или EHLO удаленной стороне при отправке письма.

При создании ящика автоматически создавать папки

Позволяет задать список стандартных папок, создаваемых в почтовом ящике. При необходимости можно изменить состав.

Антивирусная проверка вложений

Антивирусная проверка вложений:

- Проверять почту антивирусом Clamav
- Проверять почту антивирусом Касперского

Данный блок включает проверку входящих и исходящих писем на наличие в них вирусов. При положительном результате вместо самого письма получателю придет сообщение о результатах проверки, а само письмо будет во вложении к сообщению. Проверка антивирусом (Clamav, DrWeb, Касперского, для использования антивируса необходимо произвести соответствующую настройку) активируется за счет установки соответствующего флага напротив имени антивируса.

DKIM-подпись

DKIM-подпись:

- Проверять DKIM-подпись
- Создавать DKIM-подпись

Селектор

Более подробно о DKIM-подписях возможно посмотреть здесь https://ru.wikipedia.org/wiki/DomainKeys_Identified_Mail.

- Флаг «Проверять DKIM-подпись». Включает проверку входящих писем на наличие и правильность DKIM-подписи.
- Флаг «Создать DKIM-подпись». Активирует добавление DKIM-подписи в отправленные с «ИКС» письма.
- Поле «Селектор». По умолчанию, в «ИКС» используется селектор default. Так как для одного домена может быть несколько почтовых серверов, то необходимо для каждого почтового сервера в одном домене создавать свой DKIM-селектор.

Разное

- Использовать DLP
- Перекодировать тему в UTF-8
- Поддержка SMTPUTF8

Использовать DLP

При установке флага включает проверку почтовых сообщений модулем DLP (устанавливая флаг в Меню – Защита – DLP – Настройки – флаг «Использовать DLP для почты»), при условии правильной настройки и функционирования модуля DLP.

Перекодировка тему в UTF-8

Позволяет установить флаг «Перекодировать тему в UTF-8». При установленном данном флаге, письма отправляемые с почтового сервера «ИКС», будут иметь кодировку темы письма UTF-8.

Поддержка SMTPUTF8

Данный флаг включает/выключает поддержку кодировки UTF-8 при приеме отправке писем.

Вкладка "Защита от спама"

Во вкладке «Защита от спама» можно выполнить настройки серверов, содержащих черные списки, а также настроить режим работы серого списка в «ИКС».

Черные списки DNSBL

Добавить	Удалить
dul.dnsbl.sorbs.net	
bl.spamcop.net	
cbl.abuseat.org	

Серые списки (greylisting)

Использовать серые списки

Игнорировать повторную отправку *
10 сек.

Ожидать повторной отправки *
5 часов

Хранить в белом списке *
14 дней

Черные списки DNSBL (DNS Blackhole List)

Данный блок позволяет добавить/удалить хосты содержащие черные списки DNSBL. Данные списки используются для борьбы со спамом. Почтовый сервер «ИКС» при получении письма обращается ко всем хостам, указанным в данном списке, и проверяет в них наличие IP-адреса отправителя, с которого принимает сообщение. При не ответе или положительном ответе одного из хостов «ИКС» считает, что происходит попытка приёма спам-сообщения. Сообщение не принимается, а серверу отправителя сообщается ошибка 5xx (неустраняемая ошибка).

Серые списки (Greylisting)

Данный блок предназначен для установки автоматической блокировки спама. При установке флажка «Использовать серые списки» «ИКС» будет отслеживать поведение почтовых серверов, которые отправляют письма на «ИКС». О методологии блокировки можно прочитать https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%8B%D0%B9_%D1%81%D0%BF%D0%B8%D1%81%D0%BE%D0%BA.

Настройка серых списков происходит по трем параметрам – поле «игнорировать повторную отправку» в секундах (предполагается, что достоверный почтовый сервер не отправит в данное время повторно письмо); поле «ожидать повторной отправки» указывается в часах (предполагается, что письмо должно прийти не позже указанного времени); поле «хранить в белом списке» указывается в днях (предполагается, что почтовый сервер прошедший проверку не будет подвержен ей определенное количество дней).

Вкладка «Адресная книга»

Порт *

Base DN

Использовать Адресную книгу ИКС

Вкладка «Адресная книга» определяет параметры адресной книги почтового сервера «ИКС» для клиентских программ Пользователей. Здесь можно определить порт на котором работает LDAP, настроить параметр Base DN (базу поиска для LDAP, можно указать несколько через точку с запятой), включить или выключить использование адресной книги, флаг «Использовать Адресную книгу ИКС». Стоит отметить, что данный флаг позволяет передавать всем почтовым клиентам адресную книгу, но при установленном данном флаге возможно не передавать адресную книгу в Roundcube (соответствующая настройка производится в Меню - «Почта» - «Веб-почта» - вкладка «Настройки»).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:mail_setup

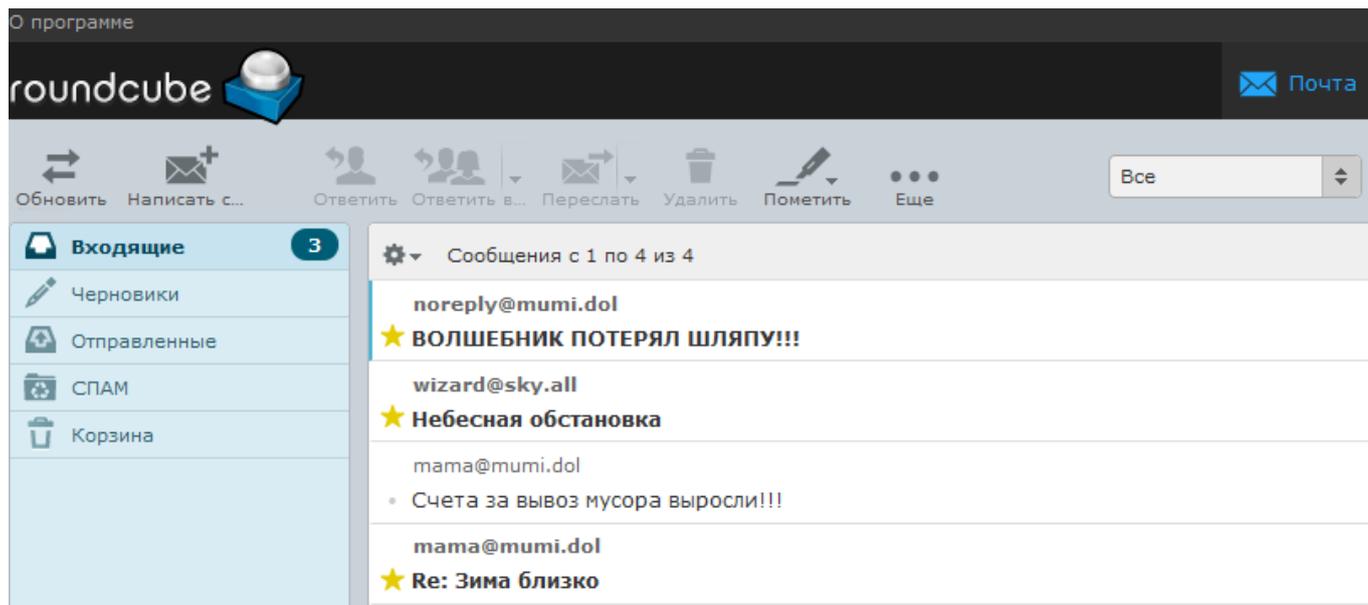
Last update: **2019/11/10 19:25**



Веб-почта

Модуль «Веб-почта» предоставляет доступ к почтовым ящикам почтового сервера «ИКС» с помощью веб-приложения Roundcube.

Перейти в веб-интерфейс почтового клиента можно по ссылке из окна авторизации, если в [Настройках интерфейса](#) не стоит флаг «Скрывать ссылку на веб-почту в окне авторизации», либо набрав в адресной строке браузера конструкцию вида `адрес_ИКС:порт_веб_почты/rc`. Веб-интерфейс Roundcube доступен только по протоколу HTTPS.



Модуль «Веб-почта» расположен в Меню «Почта». При открытии модуля в основном окне отобразятся вкладки «Веб-почта», «Настройки» и «Журнал», при этом вкладка «Веб-почта» будет активной.

Веб-почта

Веб-почта **Настройки** Журнал

 **Веб-почта**
Предоставляет веб-доступ к почтовым ящикам ИКСзапущен

Выключить

Журнал ↓↑ 

Successful login for daddy@mumi.dol (ID: 2) from 172.77.77.254(X-Real-IP: 192.168.17.211) in session 80bb4c9ba0b1925250d3b496f41b165f
08:40:02

User daddy@mumi.dol [172.77.77.254]; Message for mama@mumi.dol; 250: 2.0.0 Ok: queued as B7E933FA33
08:42:11

Successful login for mama@mumi.dol (ID: 3) from 172.77.77.254(X-Real-IP: 192.168.17.211) in session ceb88de0163b53286dab2b7ceecc57d4

Вкладка «Веб-почта». На данной вкладке отображается состояние службы «Веб-почта» с возможностью «Выключить» (или «Включить» если служба выключена) и последние сообщения в журнале.

Настройки

Веб-почта **Настройки** Журнал

Плагины:

- Сохранение адресата в адресную книгу
- Цветовые метки писем

Опции ответа

Начать новое сообщение перед цитируемым ▾

- Использовать адресную книгу ИКС
- Разрешить изменение адреса отправителя

Вкладка «Настройки». Позволяет устанавливать различные настройки для веб-интерфейса Roundcube.

Плагины

Флаг «Сохранить адресата в адресную книгу» отвечает за сохранение адресата в адресной книге «ИКС». Флаг «Цветовые метки писем» добавляет раздел «Подсветка сообщений» в веб-интерфейсе Roundcube. Данный раздел находится в настройках Roundcube.

Опции ответа

Позволяет установить один из трех вариантов при формировании ответа на письмо:

- Не цитировать оригинальное сообщение
- Начать новое сообщение перед цитируемым
- Начать новое сообщение после цитируемого

Дополнительные плагины можно активировать установлением следующих флагов:

- *«Использовать адресную книгу «ИКС»*: позволяет выбирать адресата из существующей адресной книги ИКС;
- *«Разрешить изменение адреса отправителя»*: разрешает подмену адреса отправителя на произвольный, при отправке письма;
- *«Использовать подпись»*: Позволяет устанавливать автоматически подпись в создаваемом письме. Работает только для Roundcube. Стоит отметить, что подпись автоматически сгенерируется только для аккаунтов, созданных после настройки подписи. Изменения вносимые в существующую подпись будут применены только к вновь созданным ящикам после внесенных изменений. В подписи можно использовать переменные в виде - [имя переменной]. Возможные значения переменных: `sn` (имя пользователя), `ou` (группа в которой он находится), `mail` (почтовый адрес), `description` (поле «описание» Пользователя), `notes` (поле «комментарий» Пользователя), `telephonenumber` (поле «телефон» Пользователя), `title` (поле «должность» Пользователя), `url` (поле «веб-сайт» Пользователя), `postaladdress` (поле «адрес» Пользователя), `pager` (поле «icq» Пользователя), `ounotes` (поле «описание» группы в которой состоит Пользователь). Значения переменных берутся из описания пользователя. Для вставки изображений используется кодирование изображения в `data:url`. Это делается следующим образом: используя сервис <http://dataurl.net/#dataurlmaker> (или подобный) изображение конвертируется в формат ``, а затем полученный текст вставляется в html-код подписи.

Внешний вид Roundcube

Логотип для Roundcube:

 Выбрать изображение .png

Восстановить по умолчанию

Фон сообщений в Roundcube:

 Выбрать изображение .jpg

Восстановить по умолчанию

Иконка для Roundcube (favicon):

 Выбрать изображение .ico

Восстановить по умолчанию

Позволяет загрузить и изменить логотип, иконку и фон в Roundcube. Также есть возможность восстановить по умолчанию данные настройки.

Журнал

Веб-почта Настройки **Журнал**

18.10.2019 - 18.10.2019

Сегодня

Неделя

Месяц

Другой период ▾



↑ Экспорт

Удалить логи

Поиск...



↓↑
Successful login for daddy@mumi.dol (ID: 2) from 172.77.77.254(X-Real-IP: 192.168.17.211) in session 80bb4c9ba0b1925250d3b496f41b165f 08:40:02
User daddy@mumi.dol [172.77.77.254]; Message for mama@mumi.dol; 250: 2.0.0 Ok: queued as B7E933FA33 08:42:11
Successful login for mama@mumi.dol (ID: 3) from 172.77.77.254(X-Real-IP: 192.168.17.211) in session ceb88de0163b53286dab2b7ceecc57d4 08:42:47
User mama@mumi.dol [172.77.77.254]; Message for daddy@mumi.dol; 250: 2.0.0 Ok: queued as 01F753FA5E 08:43:15
User mama@mumi.dol [172.77.77.254]; Message for daddy@mumi.dol; 250: 2.0.0 Ok: queued as E97D13FA7A 08:44:07

Вкладка «Веб-почта». 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».

From:
<https://doc.a-real.ru/> - **Документация**

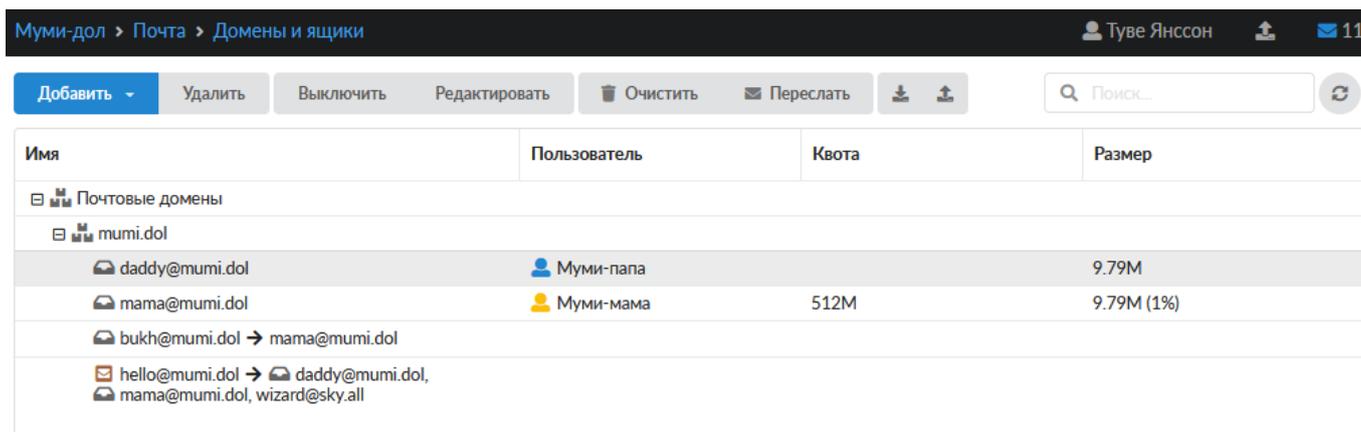
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:rc>

Last update: **2019/11/10 19:25**



Домены и ящики

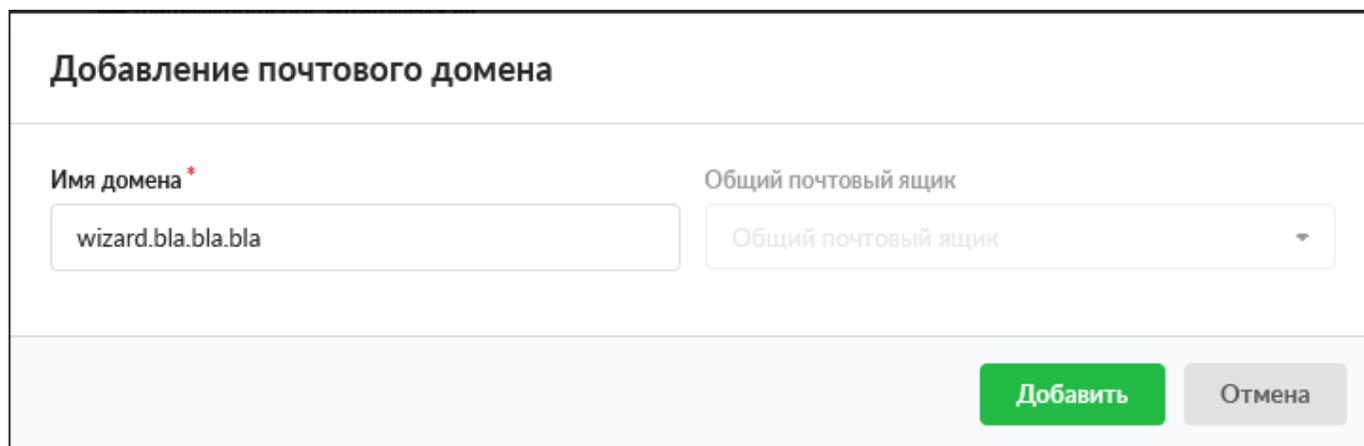
Модуль «Домены и ящики» расположен в Меню «Почта». Данный модуль предназначен для присвоения и работы с почтовыми доменами и ящиками Пользователей «ИКС». При открытии модуля «Домены и ящики» в основном окне отображаются: почтовые домены, почтовые домены с перенаправлением, почтовые ящики, ссылки на почтовые ящики; и для почтовых ящиков отображаются Пользователи, установленные квоты и текущий размер ящиков. Также данный модуль содержит строку поиска и функциональные кнопки (добавить, удалить, выключить, редактировать, очистить, переслать, скачать, закатать) активирующиеся при выборе почтового ящика или домена.



Для того, чтобы почтовый домен был доступен из внешней сети и мог обмениваться данными с другими почтовыми серверами, необходима настройка DNS-записей.

После того, как почтовые ящики для Пользователей будут созданы, они могут подключаться к ИКС с помощью почтовых клиентов (например, *Mozilla Thunderbird* или *Microsoft Outlook*) или воспользоваться веб-интерфейсом для почты. Стоит отметить, что при создании почтовых доменов и ящиков соответствующие домены и аккаунты появляются в разделе jabber-сервер. Верно и обратное.

Добавление почтового домена.



Для добавления почтового домена необходимо нажать «Добавить» - «Почтовый домен», откроется диалоговое окно, в котором будет предложено ввести «Имя домена» (Обязательный

параметр) и «Общий почтовый ящик» (не обязательный параметр). Имя домена может быть любым несуществующим именем, если обмен письмами будет происходить внутри корпоративной сети, или действующим именем домена. Общий почтовый ящик будет возможно указать только после его создания (см. ниже), письма, в данный ящик, будут попадать если в письме будет указан не существующий ящик в данном домене.

Если в [Настройках почты](#) установлен флаг «Создавать DKIM-подпись», то она добавится автоматически к домену. При необходимости скопировать DKIM-подпись необходимо выделить домен и нажать «Редактировать» или в основном окне двойным кликом по имени домена открыть форму редактирования:

Для удаления почтового домена необходимо выделить его и нажать «Удалить», при этом все почтовые ящики и ссылки на почтовые ящики, находящиеся в данном домене, будут удалены.

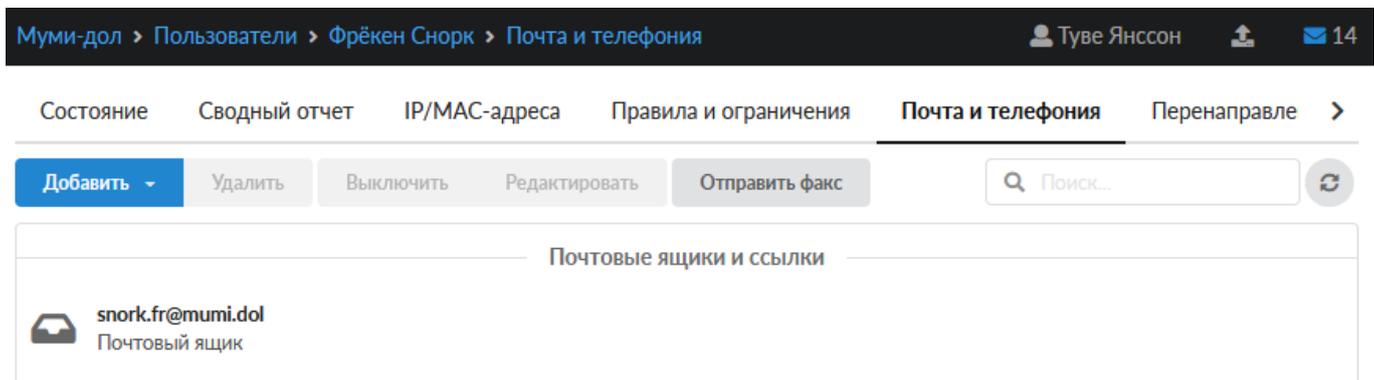
Добавление почтового ящика.

The screenshot shows a form titled "Добавление почтового ящика" (Add mailbox). It contains the following fields and controls:

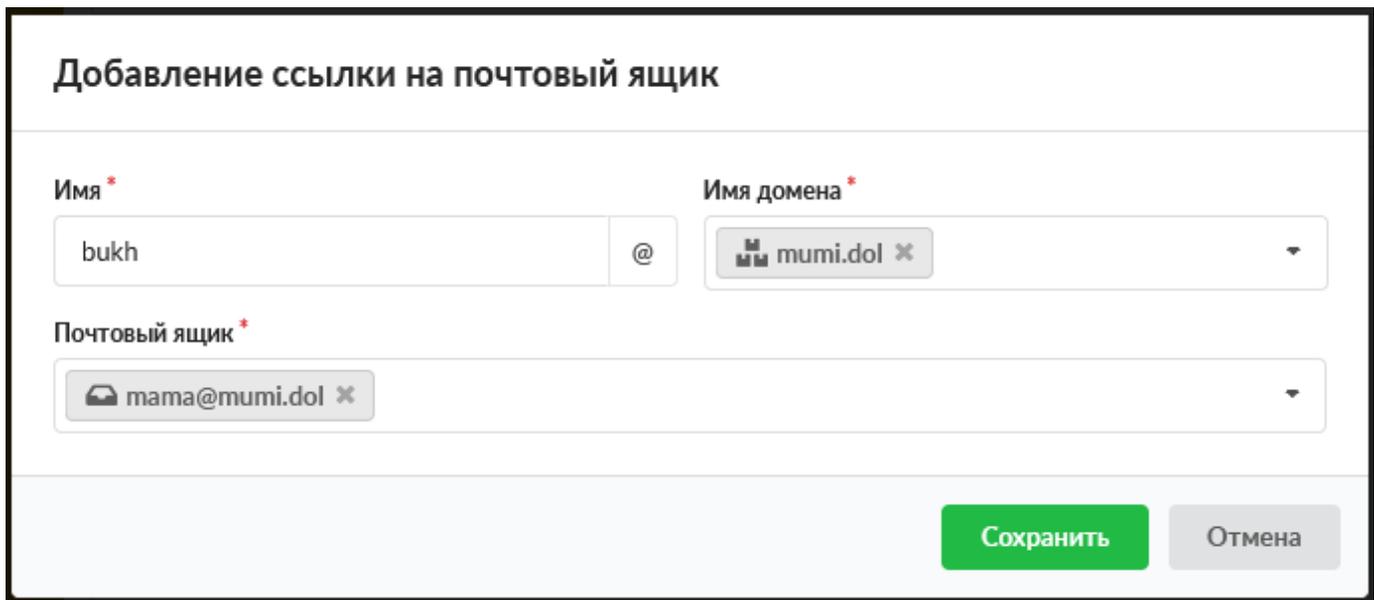
- Имя ящика *** (Mailbox name): Input field with "snork.fr" and an "@" symbol.
- Имя домена *** (Domain name): Dropdown menu with "mumi.dol" selected.
- Пароль *** (Password): Input field with masked characters and a "Generate" button (circular arrow icon).
- Пользователь *** (User): Dropdown menu with "Фрёкен Снорк" selected.
- Квота** (Quota): A checkbox that is currently unchecked.
- Quota value:** Input field with "(нет)" (none) and a unit "МБ" (MB) with up/down arrows.
- Buttons:** "Добавить" (Add) in green and "Отмена" (Cancel) in grey.

Для добавления почтового ящика необходимо нажать «Добавить» - «Почтовый ящик», откроется диалоговое окно, в котором будет предложено ввести: имя ящика; пароль; выбрать пользователя, за которым данный ящик будет закреплен; выбрать имя домена, за которым данный ящик будет закреплен, или ввести новый домен. Пароль может быть сгенерирован автоматически при нажатии на кнопку в правой части поля. При необходимости в данном диалоговом окне возможно установить флаг «Квота» и указать квоту - максимально зарезервированное место на жестком диске «ИКС» для хранения писем для данного почтового ящика. В случае превышения этой квоты письма приниматься не будут. По умолчанию квота отсутствует.

Почтовые ящики так же можно просматривать во вкладке «Почта и телефония» в модуле каждого пользователя:



Добавление ссылки на почтовый ящик.



Для добавления ссылки на почтовый ящик необходимо нажать «Добавить» - «Ссылка на почтовый ящик», откроется диалоговое окно, в котором будет предложено ввести: имя ящика, имя домена для данного ящика и выбрать существующий почтовый ящик, на который будут перенаправляться все входящие письма.

Добавление почтового домена с перенаправлением.

Почтовый сервер «ИКС» может выступать в качестве почтового шлюза (релея) для соединения логически разделенных сетей. Почтовый шлюз «ИКС», работая в качестве почтового релея, так же проверяет проходящие через него сообщения на вирусы и спам (при условии соответствующих настроек). Для этого следует использовать «Почтовый домен с перенаправлением».

Добавление почтового домена с перенаправлением

Имя домена *	Имя хоста для перенаправления *
<input type="text" value="morra.dol"/>	<input type="text" value="monsters.all"/>

Для добавления почтового домена с перенаправлением необходимо нажать «Добавить» - «Почтовый домен с перенаправлением», откроется диалоговое окно, в котором будет предложено ввести: имя домена на «ИКС» и имя хоста куда будет происходить перенаправление входящих писем.

Ручное удаление писем.

В случае необходимости удалить все письма или часть писем с одного почтового ящика необходимо выделить почтовый ящик, и нажать «Очистить». Откроется диалоговое окно, в котором будет предложено: выбрать «Все письма» для удаления или выбрать «Письма за период» и указать период.

Ручное удаление писем

Все письма
 Письма за период

с до

Ручная пересылка писем.

В случае необходимости переслать все письма или часть писем с одного почтового ящика на другой необходимо выделить почтовый ящик, с которого хотим переслать письма, и нажать «Переслать». Откроется диалоговое окно, в котором будет предложено: выбрать «Все письма» для пересылки или выбрать «Письма за период» и указать период; а также необходимо выбрать существующий почтовый ящик на «ИКС» куда будут пересланы письма.

Ручная пересылка писем

Все письма

Письма за период

с

до

На ящик *

Для скачивания всего содержимого почтового ящика в формате Roundcube необходимо выбрать почтовый ящик и нажать «Скачать». При загрузке, необходимо выбрать почтовый ящик, нажать «Закачать» и выбрать предварительно созданный архив Roundcube. **Важно: при загрузке в почтовый ящик архива все письма содержащиеся в данном почтовом ящике будут удалены.**

From:
<https://doc.a-real.ru/> - Документация

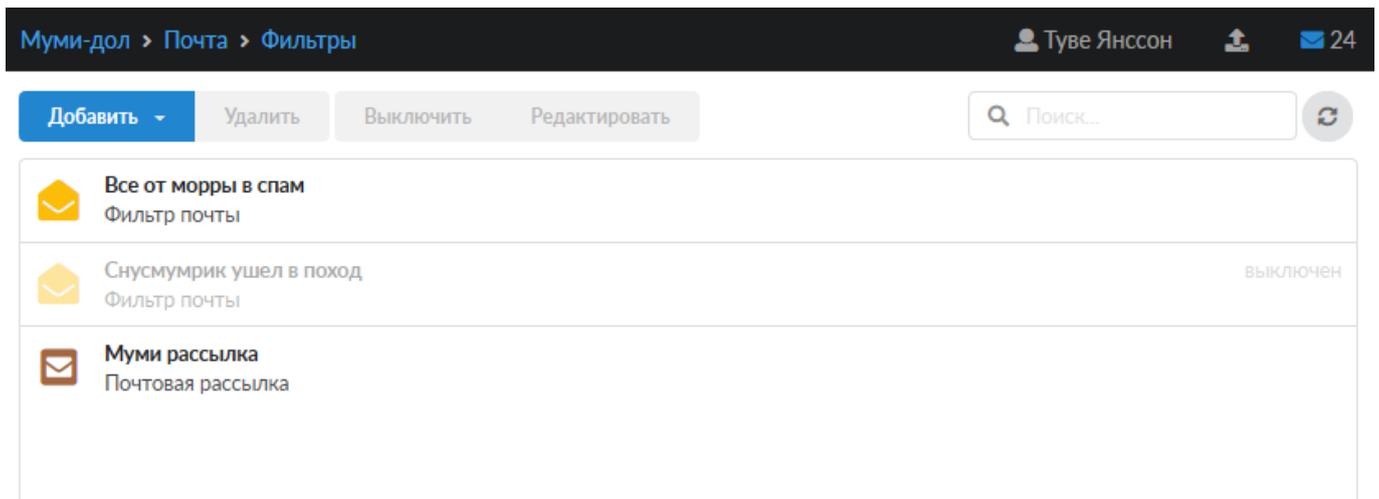
Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:mail_boxes

Last update: **2019/11/10 19:25**



Фильтры

Модуль «Фильтры» расположен в Меню «Почта». Данный модуль предназначен для того, чтобы настраивать автоматические правила для входящих и исходящих писем. С помощью фильтров можно перемещать, удалять, копировать и подменять адресатов в письме. При открытии модуля «Фильтры» будет отображен список фильтров и рассылок, созданных в ИКС, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать), активирующиеся при выборе объекта.



Важно! Если на письмо сработают условия двух фильтров, то будут произведены действия, указанные в обоих фильтрах, при этом на один почтовый ящик придет не более одной копии письма, а действие «Удалить» будет произведено в конце и удалит оригинал письма.

Почтовый фильтр.

Добавление фильтра почты

Название *

Применять

Условия: *

Добавить ▾ Удалить Редактировать

Действия: *

Добавить ▾ Удалить Редактировать

Добавить Отмена

Для создания почтового фильтра необходимо в основном окне нажать «Добавить» - «Фильтр почты». Будет открыто новое диалоговое окно, в котором будет предложено: ввести название фильтра; к каким почтовым сообщениям применять данный фильтр; условие срабатывания фильтра; и действие применимое к почтовому сообщению при срабатывании условия.

Почтовый фильтр может быть применен:

- *к сообщениям, удовлетворяющим всем условиям* - почтовый фильтр работает если все параметры из блока «Условия» будут выполнены
- *к сообщениям, удовлетворяющим любому из условий* - почтовый фильтр работает если хотя бы один из параметров из блока «Условия» будет выполнен
- *ко всем сообщениям* - почтовый фильтр применит действия, указанные в блоке «Действия», ко всем почтовым сообщениям.

Блок «Условия» позволяет задать любое количество условий. Для создания условия необходимо нажать кнопку добавить и выбрать в выпадающем списке идентификатор условия («Тема», «Отправитель», «Получатель», «Размер(Кб)»), будет открыто новое окно, в котором будет предложено выбрать способ проверки совпадения условия («содержит», «не содержит», «совпадает с», «не совпадает с», «начинается с», «заканчивается на») и значение для идентификатора.

Блок «Действия» позволяет задать любое количество применяемых действий к письму при срабатывании блока «Условия». Для создания действия необходимо нажать кнопку добавить и выбрать в выпадающем списке собственно само действие («Переместить в», «Отправить копию на», «Удалить», «Заменить домен отправителя на», «Заменить домен получателя на»), будет открыто новое окно, в котором будет предложено ввести значение для выбранного действия,

которое можно выбрать из выпадающего списка или ввести в ручную (исключением является действие «Удалить»). Примеры настройки почтовых фильтров можно посмотреть [здесь](#).

Почтовая рассылка.

Объект «Почтовая рассылка» предназначен для управления фильтром, который рассылает копии писем указанному списку адресов при условии совпадения адреса назначения.

Добавление почтовой рассылки

Название *

Адрес назначения *

Разрешать только с домена рассылки

[Добавить](#) [Удалить](#) [Импорт](#) 3 записи

daddy@mumi.dol
mama@mumi.dol
wizard@sky.all

[Сохранить](#) [Отмена](#)

Для создания почтовой рассылки необходимо в основном окне нажать «Добавить» - «Почтовая рассылка». Будет открыто новое диалоговое окно, в котором будет предложено: указать название почтовой рассылки; указать адрес назначения (почтовый ящик, на который будет приходить письмо-оригинал, при этом в «ИКС» он не должен быть заведен, поскольку он представляет собой ссылку); указать почтовые ящики, куда необходимо отправить письмо-оригинал, в таблице адресов; и при необходимости установить флаг «Разрешать только с домена рассылки» (т.е. рассылка будет происходить только в том случае, если отправитель письма-оригинала будет иметь тот же домен, что и ссылка указанная в поле «Адрес назначения»).

Для импорта списка почтовых адресов в рассылку следует использовать файл, в котором

каждый новый адрес начинается с новой строки.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

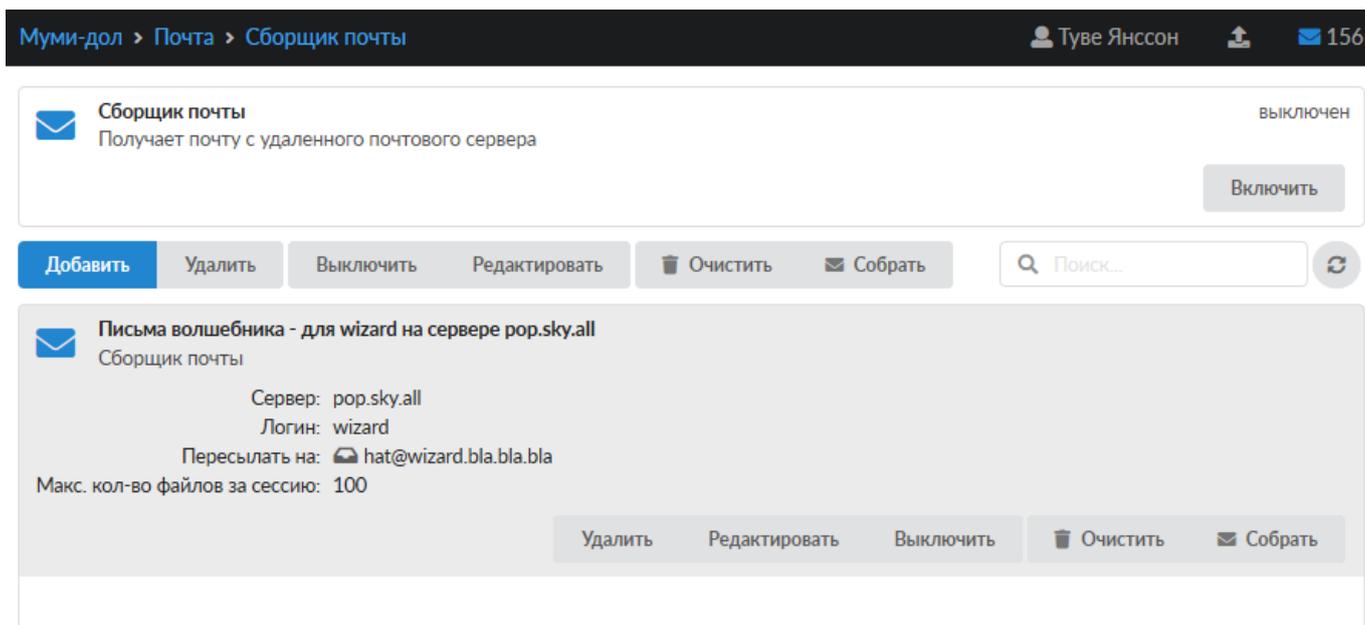
https://doc.a-real.ru/doku.php?id=ics70:mail_filters

Last update: **2019/11/10 19:25**



Сборщик почты

Модуль «Сборщик почты» расположен в Меню «Почта». Он предназначен для управления почтовыми аккаунтами, расположенными на других почтовых серверах. В основном окне модуля «Сборщик почты» отображается состояние службы «Сборщик почты» с возможностью «Выключить» (или «Включить» если служба выключена), настроенные сборщики почты, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать, очистить, собрать).



Добавление сборщика почты

Для добавления нового сборщика почты необходимо нажать «Добавить», будет открыто новое диалоговое окно, в котором необходимо указать название и настройки подключения к внешнему почтовому серверу.

Добавление сборщика почты

Название *

Сервер * **Тип сервера:**

Использовать SSL

Логин * **Пароль ***

Автоматически определять получателя

Пересылать на

Для настройки доступа к стороннему серверу необходимо заполнить поля:

- *Сервер* - ip-адрес или доменное имя сервера, с которого будет происходить сбор почты;
- *Тип сервера* - POP3 или IMAP;
- *Использовать SSL* - в случае необходимости использования шифрованного соединения;
- *Логин и пароль* - данные для входа на удаленный почтовый ящик, с которого будет осуществляться сбор почты;

Режим «**Автоматически определять получателя**» предполагает, что на внешнем почтовом домене (например, @почта.рф), где расположен почтовый ящик (например, пример@почта.рф), с которого собираются почтовые сообщения, имеет ряд ссылок на себя (например, раз@почта.рф, два@почта.рф, три@почта.рф). А на почтовом сервере «ИКС», располагается домен, например, @икс.рф и заведены почтовые ящики раз@икс.рф, два@икс.рф и три@икс.рф. Тогда сборщик почты «ИКС», работающий в режиме «Автоматически определять получателя», будет собирать почтовые сообщения с пример@почта.рф и автоматически распределять письма на раз@икс.рф, два@икс.рф и три@икс.рф в зависимости от того на какую ссылку они пришли (раз@почта.рф, два@почта.рф и три@почта.рф соответственно). В случае, если в не обязательном поле «Ящик по умолчанию» указан почтовый ящик, то сборщик почты будет туда помещать почтовые сообщения, для которых он не смог автоматически определить получателя.

Режим «**Пересылать на**» предполагает указание одного почтового ящика, куда будет производится сборка почтовых сообщений с внешнего почтового ящика.

Собирать:

все сообщения, удалять сообщения с сервера

Интервал:

5 минут

Собирать не более, писем за сессию *

100

Добавить Отмена

В поле «Собирать» необходимо выбрать, как будет производиться сборка почтовых сообщений:

- все сообщения, удалять сообщения с сервера
- только не собранные ранее сообщения, удалять сообщения с сервера
- только не собранные ранее сообщения, оставлять сообщения на сервере

Поле «Интервал» определяет время между обращениями к удаленному почтовому серверу для сбора почтовых сообщений. По умолчанию каждые пять минут; минимум каждые пять секунд; максимум раз в сутки.

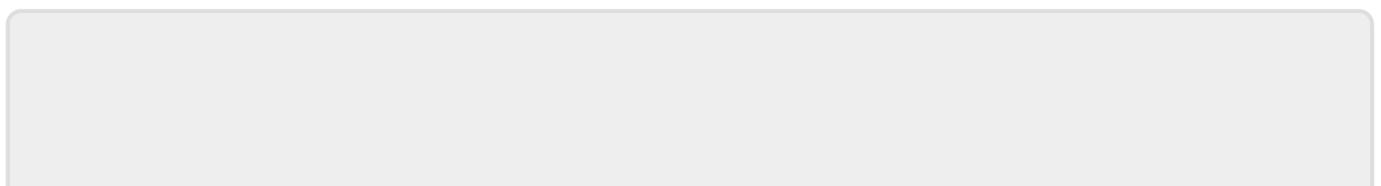
Поле «Собирать не более, писем за сессию» отвечает за максимальное количество почтовых сообщений, собираемых за одну сессию, по умолчанию сто почтовых сообщений.

Очистка сборщика

Для удаления информации о собранных ранее письмах следует использовать кнопку «Очистить». После подтверждения действия, эти данные будут удалены и при очередной сборке будут получены более ранние письма. Например, такая операция полезна при необходимости заново получить уже собранные письма.

Принудительная сборка писем

Для принудительной сборки писем следует использовать кнопку «Собрать». После подтверждения действия будет произведена внеочередная попытка сборки писем в соответствии с настройками созданных сборщиков.



From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:mail_getmail

Last update: **2019/11/10 19:25**



Антиспам SpamAssassin

Модуль «Антиспам SpamAssassin» расположен в Меню «Почта». Он предназначен для определения, является ли письмо спамом, в этом случае тема письма будет изменена. При открытии модуля в основном окне отобразится состояние службы «Антиспам SpamAssassin» с возможностью «Выключить» (или «Включить» если служба выключена) и настройки службы.

Муми-дол > Почта > Антиспам SpamAssassin Туге Янссон  21

 **Антиспам SpamAssassin**
Проверяет письма на спам

запущен

Выключить

Проверять почту

Количество баллов, при котором письмо считается спамом *

^
v

Обновить базы сейчас

Базы антиспама обновлены

Флаг «Проверять почту» активирует работу службы.

Поле «Количество баллов, при котором письмо считается спамом» позволяет задать порог при котором будет считать письмо спамом. Порог равный нулю указывает, что все письма являются спамом.

Кнопка «Обновить базы сейчас» запускает немедленную проверку актуальности баз антиспама и в случае необходимости обновляет их.

Логирование событий данного модуля происходит в Меню - Обслуживание - Журнал и уведомления - вкладка «Системный журнал» - необходимо выбрать журнал «Антиспам SpamAssassin».

Подробнее про SpamAssassin - <https://wiki.apache.org/spamassassin/RoundingIssues>.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:spamassassin>

Last update: **2019/11/10 19:25**



Антиспам Rspamd

Модуль «Антиспам Rspamd» расположен в Меню «Почта». Он предназначен для определения, является ли письмо спамом, в этом случае тема письма будет изменена, а также для отклонения подобных писем. При открытии модуля в основном окне отобразится состояние службы «Антиспам Rspamd» с возможностью «Выключить» (или «Включить» если служба выключена) и настройки службы.

Муми-дол > Почта > Антиспам Rspamd Туге Янссон 22

Антиспам Rspamd запущен
Проверяет письма на спам, добавляет и проверяет DKIM-подпись Выключить

Проверять почту

Количество баллов, при котором:

В письмо добавляется заголовок SPAM* Письмо отклоняется*

6 15

Дополнительные проверки:

Включить проверку SPF Включить проверку SURBL

Пропускать проверку писем из сетей

Локальные сети

Флаг «Проверять почту» активирует работу службы.

Поле «Количество баллов, при котором в письмо добавляется заголовок SPAM» позволяет задать порог при котором письмо будет считаться спамом, при этом тема письма будет изменена. Порог равный нулю указывает, что все письма являются спамом.

Поле «Количество баллов, при котором письмо отклоняется» позволяет задать порог при котором письмо будет считаться спамом, при этом письмо будет отклонено. Порог равный нулю указывает, что все письма являются спамом.

Флаг «Включить проверку SPF» включает дополнительную проверку SPF

Флаг «Включить проверку SURBL» включает дополнительную проверку SURBL

Поле «Пропускать проверку писем из сетей» предназначено для указания сетей, письма которых не будут подлежать проверкам антиспама.

Подробнее про Rspamd - <https://rspamd.com/doc/>.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:rspamd>

Last update: **2019/11/10 19:25**



Антиспам Касперского

Модуль «Антиспам Касперского» расположен в Меню «Защита» и в Меню «Почта». Антиспам проверяет на спам входящие и исходящие почтовые сообщения и сортирует их в соответствии с установленными параметрами. Модуль «Антиспам Касперского» имеет три вкладки: «Антиспам Касперского», «Настройки», «Журнал».

Антиспам Касперского

The screenshot shows the Kaspersky Anti-Spam control panel. At the top, there is a navigation bar with 'ИКС > Почта > Антиспам Касперского' on the left and 'Администратор' and '17' on the right. Below the navigation bar are three tabs: 'Антиспам Касперского', 'Настройки', and 'Журнал'. The 'Антиспам Касперского' tab is active, displaying the service status as 'запущен' (running). It shows the version '6.0.0.281', the license expiration date '19.04.2020', and the last database update '09.09.2019 14:29:00'. A 'Выключить' (Turn off) button is visible. Below this is the 'Журнал' (Log) section, which contains a list of events: 'started' at 15:37:58, 'start initialization ...' at 15:37:58, 'databases not found' at 15:38:01, 'trying to update databases' at 15:38:01, 'update success' at 15:40:03, and 'auto databases update every 300 seconds' at 15:40:31. There are navigation icons for the log, including arrows and a refresh button.

На первой вкладке модуля отображается состояние службы, кнопка «Выключить» (или «Включить» если служба выключена), Служба «Антиспам Касперского» отвечает за работоспособность предустановленного Антиспам Касперского, который проверяет почтовые письма. В виджете службы «Антиспам Касперского», также отображается: текущие версии базы и антиспама Касперского, дата истечения лицензии и последние события журнала за текущую дату.

Важно: по умолчанию служба находится в состоянии «не настроен». Чтобы активировать ее, отметьте в настройках почты флажок «Использовать Антиспам Касперского». Конечно, при этом у вас должен быть приобретен лицензионный ключ.

Настройки

ИКС > Почта > Антиспам Касперского > Настройки Администратор 1

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

Проверять почту

- Перенаправлять спам в папку СПАМ

Проверять наличие обновлений баз антивируса

Каждые 5 минут (рекомендуется)

Время ожидания ответа *

6000

- Предоставлять статистическую информацию в Kaspersky Lab
- Проверять репутацию IP
- Использовать облачные технологии детектирования спама (UDS, SURBL, репутация URL)

Если эта опция отключена, то запросы к облачным сервисам Kaspersky Lab не производятся. Эта опция отключает использование списков SURBL (списки по умолчанию и пользовательские списки).

Размер кэша для облачных сервисов Kaspersky Lab (КБ) *

30720

Сохранить Обновить

Менеджер лицензий позволяет загружать и просматривать сведения о файле лицензии программы.

Флаг **«Проверять почту»** активирует проверку почтовых сообщений на спам.

Флаг **«Перенаправлять спам в папку СПАМ»** включает автоматическое перенаправление писем, содержащих спам, в соответствующую папку. Без этого флага письмам будет только добавляться в тему слово «СПАМ».

Проверять наличие обновлений баз данных антиспама задает период обновления баз антивируса.

Документация - <https://doc.a-real.ru/>

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

- Сканировать сообщения на спам
 - Применять лингвистический анализ к сообщению
 - Использовать метод детектирования спама DMARC (комбинация SPF и DKIM)
 - Использовать технологию детектирования спама на основе DNS
 - Использовать списки SURBL и DNSBL

Если определены пользовательские списки DNSBL и SURBL, то они используются вместо списков по умолчанию

Список адресов сервиса SURBL

Список адресов сервиса DNSBL

- Использовать технологию детектирования спама Анти-Фишинг
- Использовать сервис Enforced Anti-Spam Updates (EASUS)
- Использовать технологию детектирования спама Распознавание Изображений
- Анализировать сообщения на ненормативную лексику
- Анализировать сообщения с кодировкой восточных языков
- Анализировать сообщения с кодировкой на кириллице

Указанные опции позволяют определить параметры проверки писем на спам.

ИКС > Почта > Антиспам Касперского > Настройки

Администратор

Антиспам Касперского **Настройки** Журнал

Менеджер лицензий Установлено лицензий: 1

Белый список IP адресов	Чёрный список IP адресов
<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>	<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>
Белый список фраз	Чёрный список фраз
<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>	<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>
Белый список E-mail адресов	Чёрный список E-mail адресов
<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>	<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>

Так же на этой вкладке можно настроить вручную **белые** и **черные** списки почтовых доменов, ip-адресов и ключевых фраз, содержащихся в сообщении.

Журнал

ИКС > Почта > Антиспам Касперского > Журнал

Администратор

Антиспам Касперского Настройки **Журнал**

09.09.2019 - 09.09.2019 Сегодня Неделя Месяц Другой период

Экспорт Удалить логи Поиск...

started 15:37:58
start initialization ... 15:37:58
databases not found 15:38:01
trying to update databases 15:38:01
update success 15:40:03
auto databases update every 300 seconds 15:40:31
initialization success 15:40:31
EbusClient: connected

Стр 1 из 1 Показаны записи 1 - 8 из 8

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, сообщения о состоянии системы (включение/выключение) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**»

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:kastiel>

Last update: **2019/11/10 19:25**



Статистика и очередь

Модуль «Статистика и очередь» расположен в Меню - «Почта» и предназначен для формирования статистических данных по почтовому серверу «ИКС», а также для управления почтовой очередью. При открытии модуля в основном окне отобразятся вкладки «Статистика» и «Почтовая очередь», при этом вкладка «Статистика» будет активна.

Статистика

Муми-дол > Почта > Статистика
Туге Янссон 20

Статистика Почтовая очередь

25.10.2019 - 25.10.2019
Сегодня
Неделя
Месяц
Другой период ▾

Детализация писем
 Группировка *

По месяцам ✕

 Отправитель

(любой)

 Получатель

(любой)

 Время с по

00:00

00:00

Показать

Время	Отправитель	Получатель	Статус	Ср. задержка	Размер
14:25:59	mama@mumi.dol	daddy@mumi.dol	Получено	0.97 сек.	+720.94K
14:31:01	daddy@mumi.dol	mama@mumi.dol	Получено	0.14 сек.	+81.46K
14:31:33	daddy@mumi.dol	hat@wizard.bla.bl a.bla	Получено	0.13 сек.	+1.42K
14:31:33	daddy@mumi.dol	mama@mumi.dol	Получено	0.16 сек.	+1.40K
14:34:19	hat@wizard.bla.bl a.bla	daddy@mumi.dol	Получено	3.7 сек.	+7.56M
14:35:11	hat@wizard.bla.bl a.bla	mama@mumi.dol	Получено	4.9 сек.	+7.56M
14:36:40	hahaha@morra.all	mama/Junk@mu mi.dol	Получено	0.51 сек.	+815.10K
14:37:15	hahaha@morra.all	mama/Junk@mu mi.dol	Получено	2.5 сек.	+7.56M
14:38:49	mama@mumi.dol	wizard@sky.all	Ошибка отправки	0.11 сек.	+1.31K
14:38:49	MAILER- DAEMON@mumi.dol	mama@mumi.dol	Получено	0.08 сек.	+3.16K
Всего			9 п, 1 ош	13.2 сек.	+24.27M

Вкладка «Статистика». На вкладке расположены два блока: блок «Параметры» и блок отображения статистических результатов (соответствующих заданным параметром в первом блоке). В качестве параметров для отображения статистики почтового сервера возможно указание следующих параметров:

Флаг «Детализация писем» предназначен для просмотра всех писем за период. При установке этого флага поле «Группировка» становится неактивным.

Детализация писем

Группировка *

По дням ✕

Отправитель

daddy@mumi.dol

Получатель

(любой)

Время с 00:00 по 08:00

Показать

Поле «Группировка» предназначено для формирования отчета по времени (по месяцам, дням или часам), доменам (по доменам отправителя, по доменам получателя) или ящикам (по ящикам отправителя, по ящикам получателя). Возможен выбор только одного значения для группировки записей.

Поле «Отправитель» позволяет задать часть или полное значение почтового адреса отправителя.

Поле «Получатель» позволяет задать часть или полное значение почтового адреса получателя.

Поля «Время с» и «по» предназначены для указания временного промежутка для фильтрации записей.

Для отображения статистических данных по почтовому серверу «ИКС», соответствующих введенным параметрам необходимо нажать кнопку «Показать». Вывод будет представлен во втором блоке в виде таблицы. Столбцы таблицы варьируются в зависимости от применяемого фильтра.

Почтовая очередь

Вкладка « Почтовая очередь » . Во вкладке показаны почтовые сообщения, ожидающие отправки. Стоит отметить, что почтовые сообщения могут быть как вновь попавшие в

почтовую очередь, так и повторно (к примеру, отклонены серым списком вышестоящего почтового сервера). При выборе любого объекта из списка можно увидеть код ошибки (если почтовое сообщение попало в очередь повторно), по которой он не был доставлен, а также можно попытаться отправить индивидуально или удалить его из очереди. Управлять почтовой очередью можно посредством кнопок «Очистить очередь» и «Отправить все».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:mail_stat

Last update: **2019/11/10 19:25**



Служба

XMPP (Extensible Messaging and Presence Protocol — расширяемый протокол обмена сообщениями и информацией о присутствии), ранее известный как **Jabber** — основанный на XML, открытый, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к режиму реального времени. Изначально спроектированный легко расширяемым, протокол, помимо передачи текстовых сообщений, поддерживает передачу голоса, видео и файлов по сети. В отличие от коммерческих систем мгновенного обмена сообщениями, таких, как AIM, ICQ, WLM и Yahoo, XMPP является децентрализованной, расширяемой и открытой системой. Любой желающий может открыть свой сервер мгновенного обмена сообщениями, зарегистрировать на нём пользователей и взаимодействовать с другими серверами XMPP.

Модуль «Служба» расположен в Меню «Jabber». При открытии модуля в основном окне отобразятся вкладки «Jabber» и «Журнал», при этом вкладка «jabber» будет активна.

Jabber

Муми-дол > Jabber Тыве Янссон 6

Jabber Журнал

Jabber-сервер запущен
Отправляет и получает сообщения XMPP Выключить

Журнал ↓↑ ↻

mod_posix: Prosody is about to detach from the console, disabling further console output
15:26:39

mod_posix: Successfully daemonized to PID 52734
15:26:39

mumi.dol:groups: Groups loaded successfully
15:26:39

wizard.bla.bla.bla:groups: Groups loaded successfully
15:26:39

Вкладка «Jabber». На данной вкладке отображается состояние службы, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Журнал

30.10.2019 - 30.10.2019

Сегодня

Неделя

Месяц

Другой период ▾



↑ Экспорт

Удалить логи

Поиск...



mod_posix: Prosody is about to detach from the console, disabling further console output

15:26:39

mod_posix: Successfully daemonized to PID 52734

15:26:39

mumi.dol:groups: Groups loaded successfully

15:26:39

wizard.bla.bla.bla:groups: Groups loaded successfully

15:26:39

Вкладка «Журнал». Отображает сводку всех системных сообщений службы «Jabber» 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) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

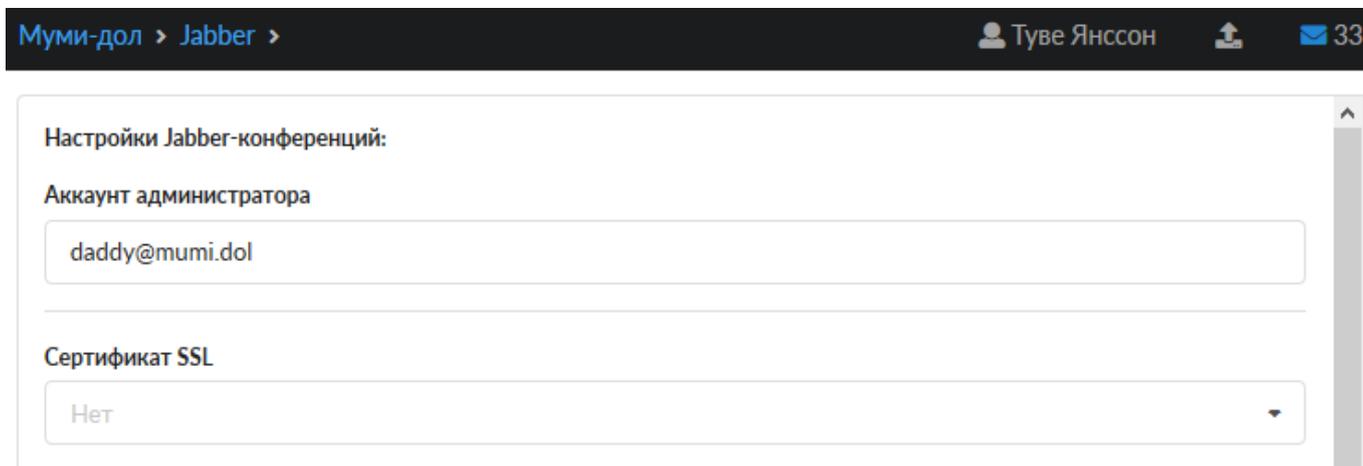
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:jabber>

Last update: **2019/11/10 19:25**



Настройки jabber-сервера

Модуль «Настройки» расположен в Меню «Jabber». Данный модуль предназначен для настройки jabber-сервера.



Муми-дол > Jabber > Тыве Янссон 33

Настройки Jabber-конференций:

Аккаунт администратора

daddy@mumi.dol

Сертификат SSL

Нет

Настройки Jabber-конференций

Конференция - место общения нескольких пользователей jabber. Имеет неповторяющееся в пределах одного сервера имя. Чтобы войти в конференцию, нужно найти соответствующий пункт меню в вашей программе-клиенте. Например, Join Group в Tkabber или Join Groupchat в Psi. Затем ввести имя комнаты и сервер, на котором она находится, например, conference.ur4k.loc. Для того, чтобы создать новую комнату, обычно, нужно просто войти в несуществующую комнату на нужном сервере конференций. Список существующих комнат можно увидеть, используя Service Discovery применительно к серверу конференций.

Аккаунт администратора

admin@jabber.ru

Параметр «Аккаунт администратора» определяет пользователя, который всегда будет администратором в любой создаваемой комнате.

Сертификат SSL

Поле «Сертификат SSL» необходимо для создания защищенного соединения «клиент-сервер». По умолчанию данные по протоколу передаются в открытом виде. Чтобы избежать этого, нужно выбрать в поле заранее сгенерированный SSL-сертификат для Jabber-сервера.

Сертификат SSL

Server ✕

Настройки общего ростера

Настройки общего ростера:

- Использовать общий ростер
- Привязывать пользователей к аккаунтам в общем ростере

- Использовать общий ростер
- Привязывать пользователей к аккаунтам в общем ростере

Флаг «Использовать общий ростер» включает или отключает общий ростер.

Флаг «Привязывать пользователей к аккаунтам в общем ростере» отвечает за отображение новых добавленных аккаунтов в общий ростер и, соответственно, у других абонентов в списке контактов.

Прокси-сервер для передачи файлов

Прокси-сервер для передачи файлов:

- Использовать прокси-сервер

Адрес *

192.168.17.246

Порт *

5000

- Использовать прокси-сервер

Адрес *

192.168.18.6

Порт *

5000

Jabber-сервер ИКС поддерживает передачу файлов через прокси-сервер (Out-of-band). Для этого нужно установить флаг «Использовать прокси-сервер», указать внешний ip-адрес ИКС в поле «Адрес», на котором работает Jabber-сервер, который доступен обоим клиентам, желающим передать файл.

Сетевые настройки

Сетевые настройки:

Разрешить s2s-соединения

Разрешить s2s-соединения

Флаг «Разрешить s2s-соединения» включает поддержку s2s-соединения

From:
<https://doc.a-real.ru/> - **Документация**

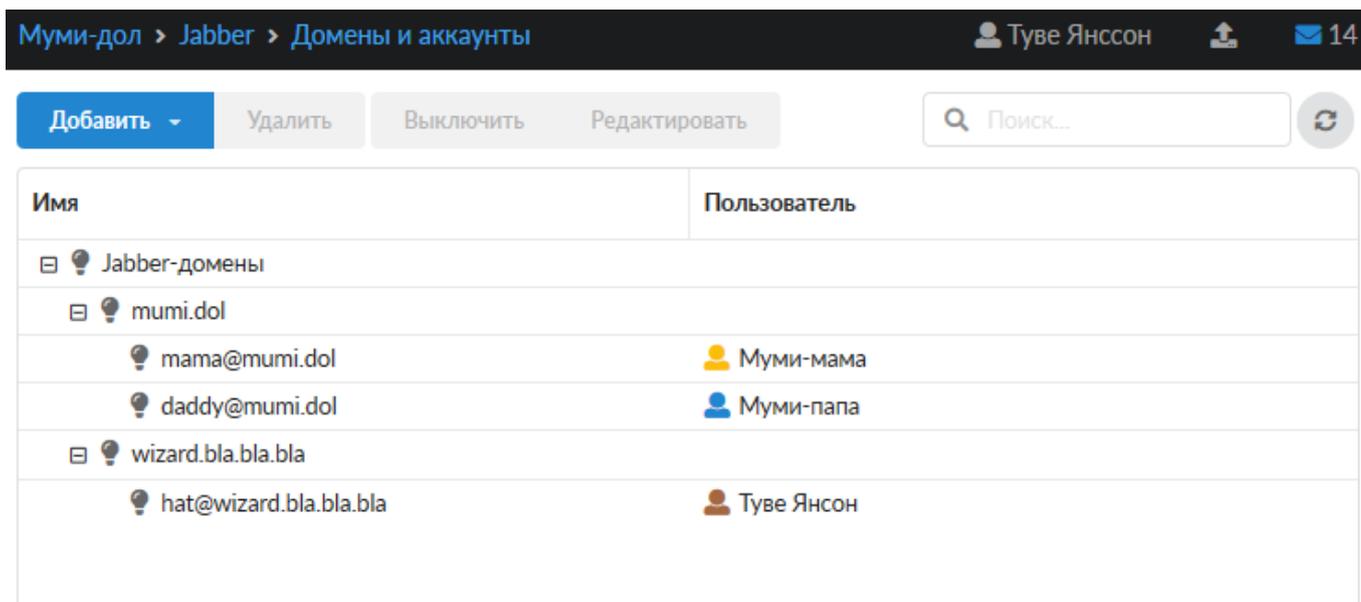
Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:jabber_setup

Last update: **2019/11/10 19:25**



Домены и аккаунты

Модуль «Домены и аккаунты» расположен в Меню «Jabber». Данный модуль предназначен для присвоения и работы с jabber- доменами и аккаунтами Пользователей «ИКС». При открытии модуля «Домены и аккаунты» в основном окне отображаются: jabber-домены и jabber-аккаунты; и для аккаунтов отображаются Пользователи. Также данный модуль содержит строку поиска и функциональные кнопки (добавить, удалить, выключить, редактировать) активирующиеся при выборе аккаунта или домена.



Добавление jabber-домена

Для добавления jabber-домена необходимо нажать «Добавить» - «Jabber-домен», откроется диалоговое окно, в котором будет предложено ввести «Имя домена» (Обязательный параметр). Имя домена может быть любым несуществующим именем, если общение по протоколу Jabber будет происходить внутри корпоративной сети, иначе необходимо настроить пересылку jabber-сообщений на реально существующем домене, зарегистрированном за организацией.



Для удаления jabber-домена необходимо выделить его и нажать «Удалить», при этом все аккаунты, находящиеся в данном домене, будут удалены.

Добавление jabber-аккаунта

Для добавления jabber-аккаунта необходимо нажать «Добавить» - «Jabber-аккаунт», откроется диалоговое окно, в котором будет предложено ввести: имя аккаунта; пароль; выбрать пользователя, за которым данный аккаунт будет закреплен; выбрать имя jabber-домена или ввести новый домен. Пароль может быть сгенерирован автоматически при нажатии на кнопку в правой части поля.

Добавление jabber-аккаунта

Имя аккаунта *	Имя домена *
<input type="text" value="fr.snork"/> @	<input type="text" value="mumi.dol"/>
Пароль *	Пользователь *
<input type="password" value="••••••••"/>  	<input type="text" value="Фрёкен Снорк"/>

Важно: при создании jabber-доменов и аккаунтов соответствующие домены и аккаунты появляются в разделе **Почта**. Изменение jabber-доменов и аккаунтов влечет также соответственное изменение почтовых доменов и ящиков. При удалении jabber-доменов и аккаунтов также удалятся соответствующие почтовые домены и ящики. Верно и обратное.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:jabber_doamin

Last update: 2019/11/10 19:25



Ростер

Shared roster (англ. Общий ростер) - способ настройки XMPP-сервера, когда изменение ростера клиента инициируется со стороны сервера. При подключении к серверу клиент получает набор групп и содержащихся в них контактов. Помимо контактов клиент автоматически получает подписку от всех контактов, а также предоставляем всем свою. Таким образом любой контакт из ростера видит статус любого другого контакта.

Модуль «Ростер» расположен в Меню «Jabber». В данном модуле можно управлять списком контактов всех созданных на ИКС jabber-доменов так, как они будут отображаться в контакт-листе пользователя, подключившегося к ИКС по своему jabber-аккаунту.

Муми-дол > Jabber > Ростер Тыве Янссон 15

Добавить | Удалить | Редактировать Поиск...

Имя ▲	Jabber-аккаунт
☐ Общий ростер	
☐ Сотрудники (по умолчанию)	
Муми-папа	daddy@mumi.dol
Муми-мама	mama@mumi.dol
☐ Остальные контакты (не отображаются в списке контактов)	
Тыве Янссон	hat@wizard.bla.bla.bla

Аккаунты можно группировать в группы контактов, созданные через кнопку «Добавить». Откроется диалоговое окно, в котором будет предложено ввести название группы (обязательное поле). В «ИКС» реализована функция drag-and-drop, поэтому контакты легко можно переместить в созданную группу.

Также данный модуль содержит строку поиска и функциональные кнопки (добавить, удалить, редактировать) активирующиеся при выборе группы. Стоит отметить, что при удалении группы контактов аккаунты, входящие в данную группу, автоматически перемещаются в группу «Остальные контакты» и не отображаются в списке контактов.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:roster>

Last update: **2019/11/10 19:25**



Служба

VoIP — система связи, передающая аудио-сигнал по IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается с целью удаления избыточности.

За обработку VoIP-данных в ИКС отвечает служба «Телефония», разработанный на базе сервера ip-телефонии Asterisk. Это свободное решение компьютерной телефонии с открытым исходным кодом, оно достаточно надежное и давно зарекомендовало себя с положительной стороны. В настоящее время служба поддерживает передачу данных по протоколам SIP и IAX.

Модуль «Служба» расположен в Меню «Телефония». При открытии модуля в основном окне отобразятся вкладки «Телефония» и «Журнал», при этом вкладка «Телефония» будет активна.

Телефония

Муми-дол > Телефония Тыве Янссон 126

Телефония Журнал

Телефония запущен

Сервер ip-телефонии Выключить

Журнал ↻

13:51:16	WARNING[100660]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 243441799-621711339-745490028 on non-critical invite transaction.
13:51:16	WARNING[100660]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 1185699723-1823746910-1796332489 on non-critical invite transaction.
13:51:16	WARNING[100660]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 1451050601-1554936374-1767744853 on non-critical invite transaction.
13:51:16	WARNING[100660]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 1214533415-1473170206-111449998 on non-critical invite transaction.
13:51:16	WARNING[100660]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 38429614-621293654-153131721 on non-critical invite transaction.

Вкладка «Телефония». На данной вкладке отображается состояние службы «Телефония» с возможностью «Выключить» (или «Включить» если служба выключена) и последние сообщения в журнале.

Журнал

Телефония **Журнал**

03.09.2019 - 03.09.2019 **Сегодня** Неделя Месяц Другой период ↕

↑ Экспорт Удалить логи Поиск...

02.09.2019 20:00:...	WARNING[101186]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 499818799-1042623314-337603912 on non-critical invite transaction.
02.09.2019 20:00:...	WARNING[101186]: chan_sip.c:4128 in int retrans_pkt(const void *): Timeout on 1846359375-1587676799-1736543200 on non-critical invite transaction.
02.09.2019 20:00:...	ERROR[101170]: netsock2.c:305 in int ast_sockaddr_resolve(struct ast_sockaddr **, const char *, int, int): getaddrinfo("dynamic", "(null)", ...): hostname nor servname provided, or not known
02.09.2019 20:00:...	WARNING[101170]: acl.c:835 in int resolve_first(struct ast_sockaddr *, const char *, int, int): Unable to lookup 'dynamic'

Вкладка «Журнал». Отображает сводку всех системных сообщений службы «Телефония» 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) - 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».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:asterisk>

Last update: **2019/11/10 19:25**



Настройки телефонии

Модуль «Настройки» расположен в Меню «Телефония». Данный модуль предназначен для настройки сервера телефонии.

Настройки портов

Муми-дол > Телефония > Настройки Тыве Янссон  126

Настройки

Порт SIP (UDP) * ↑ ↓ Порт IAX * ↑ ↓

Порты для входящих соединений RTP *

Автоматически создавать разрешающее правило

Доступ для звонков через сервер IP-телефонии

Первыми указаны настройки портов SIP (через UDP) и IAX, а также диапазон портов для входящих соединений RTP. По-умолчанию используются следующие значения:

SIP	5060
IAX	4569
RTP	10000-20000

Установка флага «Автоматически создавать разрешающее правило» добавит в межсетевой экран разрешающее правило для указанных портов.

TCP для SIP

TCP для SIP

Порт для SIP через TCP * ↑ ↓

Автоматически создавать разрешающее правило

Доступ для TCP подключений IP-телефонии

Флаг «TCP для SIP» включает поддержку отправки и получения SIP пакетов по протоколу TCP

на выбранном порту. Данную опцию необходимо включать, если у вас используются внешние или внутренние номера, настроенные для работы через тип подключения «Без Шифрования (TCP)»

Установка флага «Автоматически создавать разрешающее правило» добавит в межсетевой экран разрешающее правило для указанного порта.

Шифрование

Сертификат для шифрования (TLS и SRTP)

 Autogenerated Asterisk_5d691ccc41df69.68833519 ✕

Порт для SIP через TLS *

5061

Автоматически создавать разрешающее правило

 Доступ для TLS подключений IP-телефонии

Поле «Сертификат для шифрования (TLS и SRTP)» позволяет выбрать, изменить или удалить сертификат шифрования для телефонии. По умолчанию выбран автоматически сгенерированный сертификат. При выбранном сертификате активируется обязательное поле «Порт для SIP через TLS» (по умолчанию это порт 5061). Установка флага «Автоматически создавать разрешающее правило» добавит в межсетевой экран разрешающее правило для указанного порта.

Важно: для использования шифрования, необходимо выбрать тип подключения «С шифрованием (TLS и SDES sRTP)» в настройках конкретного телефонного номера и настроить устройство на стороне абонента.

Важно! После смены следующих настроек - порт SIP через UDP/TCP/TLS - сервер телефонии будет перезапущен, текущие вызовы будут прерваны.

Общие настройки сервера телефонии

Драйвер канала SIP

- chan_sip
 chan_pjsip

Время ожидания ответа*

 сек.

- Использовать BLF
 SRV lookup

Запись звонков

- Записывать звонки
 Начинать новую запись при переводе

Драйвер канала SIP позволяет выбрать модуль реализации протокола SIP, который будет использоваться сервером телефонии ИКС. Доступно два канальных драйвера: `chan_sip` и `chan_pjsip`

Выбор драйвера `chan_pjsip` сохраняет текущее поведение модуля телефонии и обеспечивает почти такой же функционал телефонии ИКС, как если бы она работала на `chan_sip`. Однако, некоторые параметры все же отличаются. В зависимости от выбранного канального драйвера, становятся недоступны некоторые опции во всем модуле ip-телефонии.

Отличия в настройке [внешних каналов](#):

- Опции *insecure*, *canreinvite* и *строка регистрации* доступны только для модуля `chan_sip`.
- Опция *direct_media* доступна только для модуля `chan_pjsip`. Опция определяет, могут ли медиаданные передаваться напрямую между конечными точками. Если *no*, то все RTP потоки проходят через Asterisk

Отличия в общих настройках телефонии:

- Опция *SRV lookup* доступна только для модуля `chan_sip`.

Кроме того, *конференции* с режимом распределения видео *SFU* и *xphone* работают только на канальном драйвере `pjsip`.

Важно! После смены настройки драйвера канала SIP сервер телефонии будет перезапущен, текущие вызовы будут прерваны/не обработаны. Текущие регистрации транков не будут прерваны, необходимо всем внутренним/внешним транкам заново переподключиться и перерегистрироваться на сервере (т.е. всем внутренним телефонам необходимо заново подключиться к «ИКС», а в случае проблем с провайдером телефонии переподключить его).

Поле «**Время ожидания ответа**» позволяет задать период времени, по истечении которого сервер телефонии посчитает абонента неответившим на звонок и переведёт звонящего абонента в следующий набор правил. Время по-умолчанию - 30 секунд. Некоторые правила телефонии позволяют переопределить это время для конкретного правила.

Флаг «**Использовать BLF**» включает поддержку функции Busy Lamp Field, позволяющую в реальном времени отслеживать состояния абонентов АТС (занят/свободен). **Важно:** конечное оборудование (телефонный аппарат) должно поддерживать эту функцию.

Флаг «**SRV lookup**» активирует DNS-поиск SRV-записей. Недоступен при выборе chan_pjsip в качестве драйвера канала SIP. SRV-записи DNS – это средство задания логических разрешимых адресов. Позволяет перенаправлять вызовы в разные точки без необходимости изменения логического адреса. Использование SRV-записей открывает доступ ко многим преимуществам DNS, тогда как их отключение лишает возможности размещать SIP-вызовы на основании доменных имен. В настоящее время поддержка SRV-записей в телефонии несколько неэффективна. Следует учитывать, что если возвращено несколько SRV-записей, служба будет использовать только первую из них.

Голосовая почта

Голосовая почта

- Использовать голосовую почту
- Перенаправлять на голосовую почту при неответе
- Отправлять сообщения голосовой почты на e-mail

Номер для голосовой почты *

Переадресация вызовов

Переадресация

Номер для безусловной переадресации *

Номер для переадресации *

Безусловная переадресация

Данная опция позволяет перевести входящий звонок, предназначенный одному абоненту, другому абоненту, пока происходит звонок. Для этого необходимо набрать номер безусловной переадресации, а затем номер другого абонента. Дождаться ответа второго абонента не нужно.

Обычная переадресация

Данная опция позволяет перевести входящий звонок, предназначенный одному абоненту, другому абоненту, 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 вызовов

Перехват звонков

Номер для перехвата*

*8

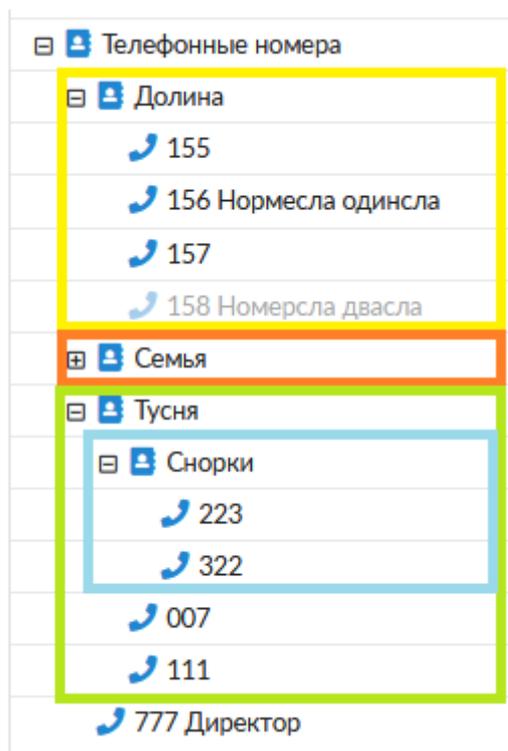
Номер для направленного перехвата*

**

Перехват в рамках группы

Данная опция позволяет ответить на входящий звонок, предназначенный одному абоненту, другому абоненту, 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 номер *8. Комбинацию клавиш для перехвата вызова можно поменять в поле «**Номер для перехвата**».

Важно: перехват вызова осуществляется только в пределах одной группы телефонных номеров!



Например при изображенной структуре номеров:

Вызов, поступивший на номер 155 могут перехватить только 156 и 157.

Вызов, поступивший на номер 223 могут перехватить только 322, 007 и 111.

Номер 777, находящийся на верхнем уровне, может перехватывать все номера.

Направленный перехват

Этот тип перехвата звонков предназначен для перехвата входящего звонка на конкретный внутренний номер вне зависимости от группы внутренних номеров.

Чтобы перехватить вызов, предназначенный другому абоненту, со своего телефона необходимо ввести во время звонка комбинацию * * (две звездочки - по умолчанию) + внутренний номер вызываемого абонента. Комбинацию клавиш для направленного перехвата вызова можно поменять в поле «**Номер для направленного перехвата**».

Факсы

Факсы

Поддержка T38

Обнаружение ошибок

Не задано

Максимальный размер пакета

Не задано

Конвертировать принятые факсы в PDF

Флаг «**Поддержка T38**» включает поддержку стандарта T.38 для передачи факсимильных сообщений.

Поле «**Обнаружение ошибок**» позволяет выбрать тип корректировки входящих сообщений:

- Значение «*Redundancy*» - *Redundancy error correction* - исправление ошибок избыточности
- Значение «*FEC*» - *Forward error correction* - прямое исправление ошибок
- Значение «*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. По умолчанию все факсимильные сообщения будут иметь формат *tiff*

NAT

Данный блок отвечает за настройку поведения модуля телефонии, если он находится за NAT.

Использовать NAT (ICS за NAT)

IP-адрес *

10.0.0.7

Список сетей

 Муми локалка (192.168.17.242/24) ✕

Флаг **«Использовать NAT»** включает преобразование IP-адресов внутри пакетов телефонии. Для корректной работы этого блока, необходимо указать внутренние локальные сети и внешний IP. В поле **«IP-адрес»** - необходимо указать внешний IP-адрес, используемый для преобразования IP-адресов в обработке SIP, если пункт назначения SIP-сообщений находится за пределами IP-сети, определенной в поле **«Список сетей»**. Таким образом, все указанные в этом поле сети сервер телефонии будут считаться локальными, для них не будут применяться правила преобразования IP-адресов внутри пакетов IP-телефонии.

Почтовый сервер

Данный блок отвечает за настройку пересылки факсов, уведомлений и сообщений голосовой почты.

Почтовый сервер для факсов, уведомлений и сообщений голосовой почты

Использовать SMTP ИКС

Адрес отправителя

 noreply@mumi.dol ✕

Использовать указанный SMTP

SMTP сервер

smtp.host.ru

Порт

25

SSL

Логин

Пароль

Адрес отправителя

noreply@hostname

Необходимо выбрать, какой сервер будет использоваться для отправки писем: почтовый сервер ИКС или внешний SMTP-сервер. В первом случае достаточно указать в поле **«Адрес отправителя»** один из почтовых адресов, созданных в ИКС. Во втором необходимо заполнить поля **«SMTP-сервер»**, **«Порт»**, **«Логин»**, **«Пароль»** и **«Адрес отправителя»**, а также, если необходимо, установить флаг **«SSL»**.

Кодеки

В данном блоке можно выбрать определенные используемые модулем телефонии кодеки для всех номеров, заданные по-умолчанию.

В левом столбце «Использовать» перечислены кодеки, которые используются всеми номерами, если не задано иное в настройках отдельных номеров. Порядок следования кодеков в этом столбце имеет значение - кодеки, расположенные вверху имеют больший приоритет, чем нижние. Иными словами, список кодеков будет представлен удаленной стороне во время установления сеанса связи в порядке их следования в этом списке.

Доступные, но не используемые модулем телефония кодеки, перечислены в правом столбце «Доступные кодеки»

Кодеки

Использовать	>	Доступные кодеки	
G.711 a-law	<	G.726	^
G.729		G.711 u-law	
GSM		G.723	
VP8 Video		Opus	▼

Модуль телефонии в ИКС поддерживает следующие кодеки:

Аудио:

- G.711 a-law
- G.711 u-law
- G.723
- G.726
- G.729
- Opus
- GSM

Видео:

- H.264
- VP8
- VP9

Для работы видеозвонков необходимо добавить в столбец «Использовать» хотя бы один видеокodeк

Для работы xphone рекомендуется использовать следующий набор кодеков: G.711 a-law, Opus, VP8, VP9

Мелодия при удержании вызовов

В данном блоке указывается мелодия, которая будет воспроизводиться звонящему при удержании вызова

Мелодия при удержании вызова

▶ Воспроизвести

🗑 Удалить мелодию

📄 Загрузить новую мелодию

Сохранить

Обновить

Для загрузки мелодии необходимо нажать кнопку «Загрузить новую мелодию» и выбрать звуковой файл. После загрузки мелодию можно прослушать или удалить с помощью соответствующих функциональных кнопок.

From:

<https://doc.a-real.ru/> - Документация

Permanent link:

https://doc.a-real.ru/doku.php?id=ics70:asterisk_setup

Last update: **2019/11/10 19:25**



Xphone

Модуль «Xphone» расположен в Меню «Телефония». Данный модуль представляет собой встроенный в ИКС web-софтфон, работающий через браузер, и предназначен для совершения и приема звонков. При доступе со внешних сетей не гарантируется стабильная работа видео потоков.

Модуль поддерживает видеозвонки, конференции, а так же постановку вызова на удержание и безусловную переадресацию звонка.

В самом модуле расположен только флаг «Включить Xphone», который позволяет использовать Xphone в браузере.

Включение

Xphone работает только на драйвере канала SIP - **PJSIP**. Чтобы убедиться, что данная настройка выбрана правильно, необходимо перейти в Меню → Телефония → Настройки → блок «Драйвер канала SIP» и выбрать пункт «chan_pjsip», затем нажать «Сохранить».

Драйвер канала SIP

- chan_sip
 chan_pjsip

Важно! При изменении настройки драйвер канала SIP сервер телефонии будет перезапущен, текущие вызовы будут прерваны.

После этого, интерфейс Xphone станет доступен по адресу в web-браузере <https://ip-ics:81/xphone/>

Так же ссылка на Xphone доступна в окне авторизации в web-интерфейс «ИКС».

Логин

Пароль

Войти

[Программа авторизации](#) [Captive portal](#) [Веб-почта Xphone](#)

Для корректной работы Xphone необходим современный браузер с поддержкой технологии WebRTC. Ориентировочный список поддерживаемых браузеров:

- **Chrome:** Версия 76+
- **Opera:** Версия 63+
- **Firefox:** Версия 69+
- **Yandex браузер:** 19.9.3.314+

Настройка внутренних номеров

Добавление номера для Xphone происходит аналогично добавлению [телефонного номера](#). Существенным отличием является выбор пункта «доступ Xphone».

Доступ

SIP-клиент Xphone

Тип подключения

Без шифрования (UDP) ▾

Важно: если телефонный номер принадлежит Xphone, то использование данного номера возможно только с web-софтфона Xphone. Поскольку Xphone использует шифрование медиа данных DTLS-SRTP, соответственно, номер конфигурируется с использованием только этого типа шифрования.

Авторизация

Для авторизации необходимо:

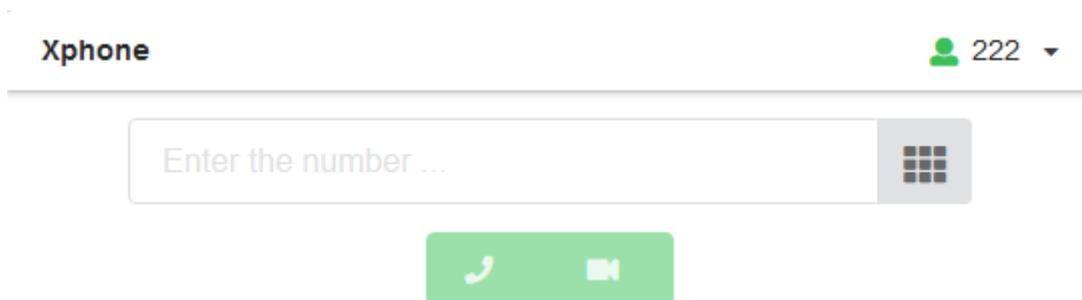
1. Войти в интерфейс xphone, указав URL в браузере в следующем формате: <https://ip-ics:81/xphone/>. Если URL введен правильно, отобразится страница входа в xphone
2. Ввести номер добавочного внутреннего номера ИКС
3. Если авторизация прошла успешно, появится внутренний интерфейс модуля

Интерфейс

Справа сверху располагается зеленая иконка Пользователя и добавочный внутренний номер, под которым авторизован Пользователь в Xphone. При наведении мыши на это поле появится кнопка «logout», нажав на которую можно отменить авторизацию на сервере телефонии под этим добавочным номером

В самом центре расположено поле для ввода номера. В нем можно вводить номер телефона

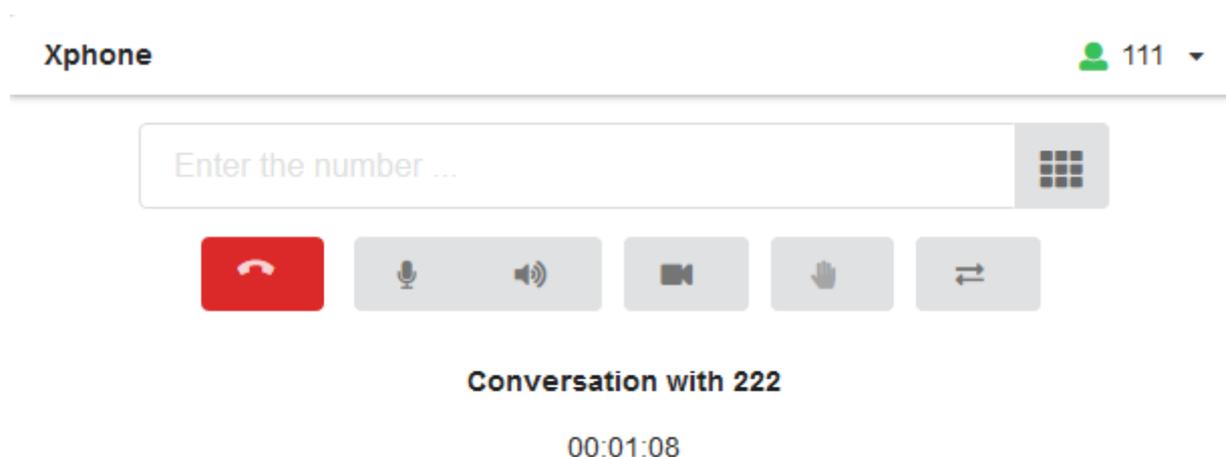
как с клавиатуры, так и через экранные клавиши, нажав соответствующую кнопку, справа от этого поля. Во время звонка данное поле так же доступно, в нем можно вводить номера, которые будут преобразованы в DTMF-команды. Чуть ниже располагаются кнопки инициации вызова.



Важно: xphone при запуске сам определит наличие веб-камеры. Если её нет - будет недоступна кнопка совершения видеозвонка.

Выполнение вызова

Для инициирования вызова необходимо ввести номер вызываемого абонента в соответствующее поле, а затем нажать одну из двух кнопок - аудиозвонок или видеозвонок. Затем начнется установление соединения с сервером, на экране появится надпись « Dialing NUMBER... ». Как только соединение с удаленной стороной будет установлено, появится таймер, говорящий о том, что сеанс связи начался, удаленная сторона взяла трубку. Если вызов установить не удастся - появится ошибка, сообщающая о причине отказа.

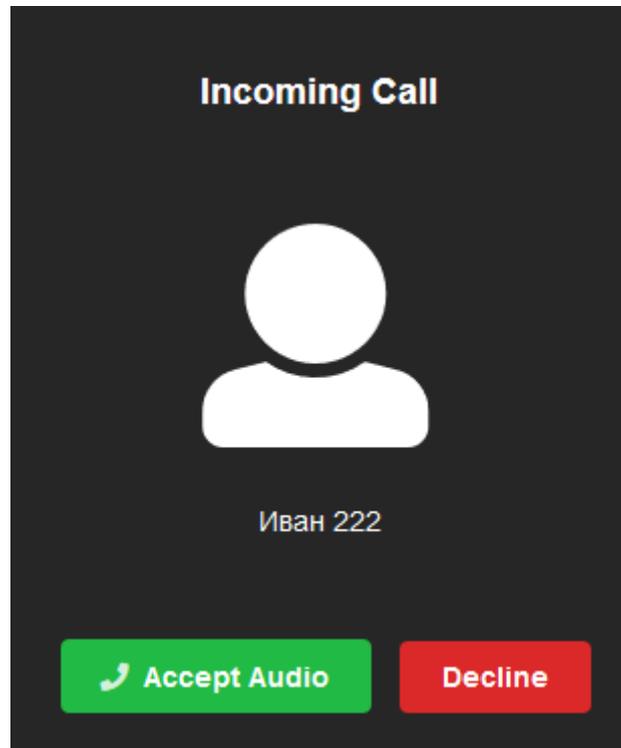


Для завершения вызова необходимо нажать соответствующую красную кнопку. Вызов так же будет завершен, если закрыть окно или вкладку браузера.

Прием входящего звонка

Во время входящего звонка на xphone, появится всплывающее окно, в котором можно увидеть

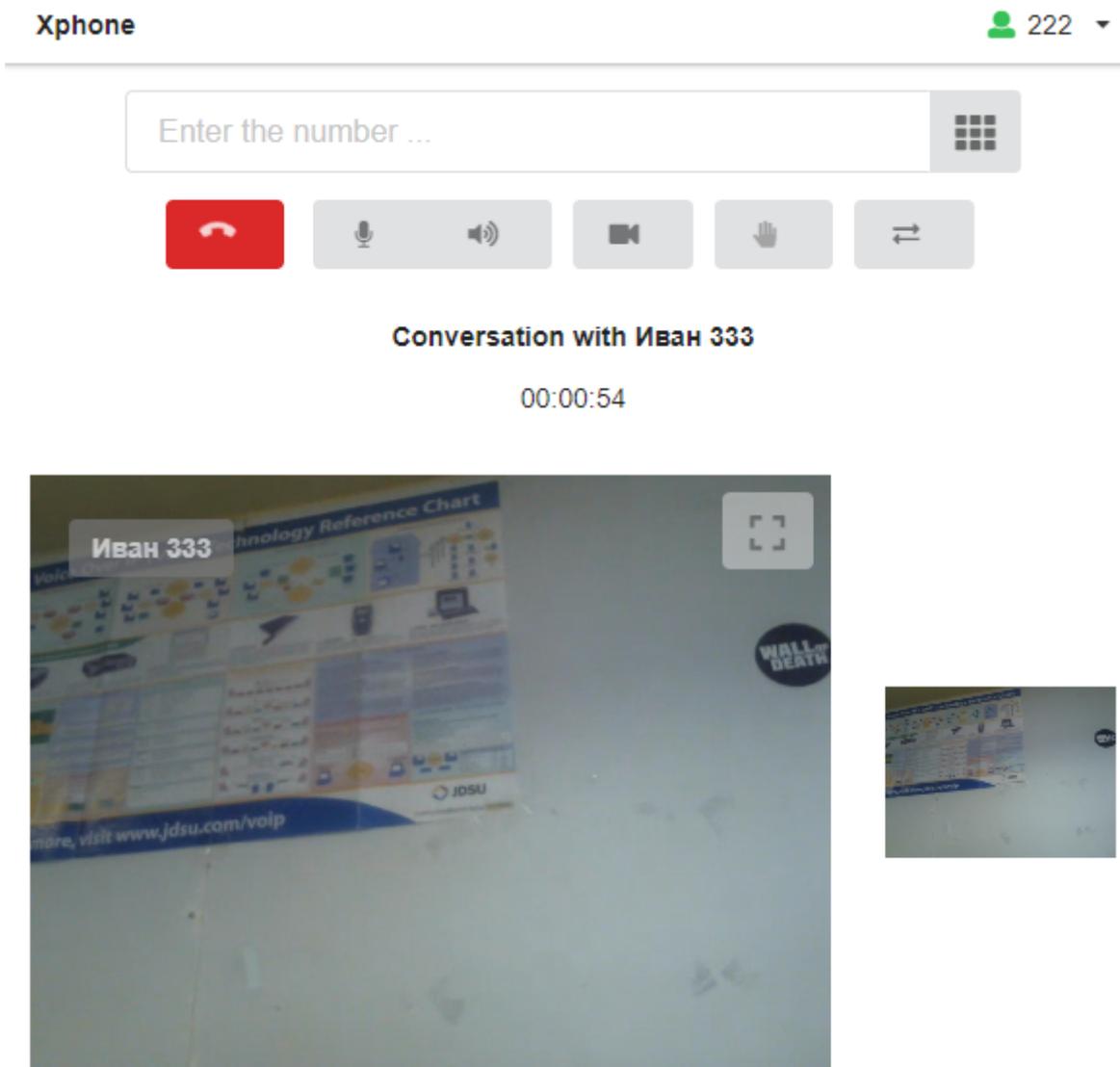
номер и callerid входящего абонента. На входящий звонок можно ответить как с аудио (кнопка «Accept Audio»), так и с видео (кнопка «Accept Video»). Вызов так же можно отклонить, нажав кнопку «Decline». Кнопка «Accept Video» появляется только тогда, когда инициатор вызова сделал именно видеовызов и в браузере устройства, на которое поступил входящий звонок, имеется доступ к веб-камере



Опции во время вызова

Доступные опции:

- Вкл/выкл микрофон
- Вкл/выкл звук собеседника
- Вкл/выкл локальное видео (если видеовызов)
- Постановка вызова на удержание и снятие с удержания (кроме конференций)
- Безусловный перевод звонка (кроме конференций)



Конференции

Для корректной работы видеоконференций через xphone, необходимо в настройках номера конференции (Меню - Телефония - Телефонные номера - Конференция) выбрать в блоке «Режим распределения видео» - *Источники видео - все пользователи конференции (SFU, pjsip only)*.

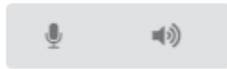
В режиме видеоконференции в интерфейсе появится дополнительная метка Users, отображающая количество участников конференции. При наведении на нее указателем мыши, появится всплывающее сообщение, в котором будут отображены номера телефонов и CallerID участников конференции. Видео говорящего в данный момент участника конференции будет выделено синей рамкой.

Всем участникам конференции доступно следующее DTMF [меню](#).

Xphone

111

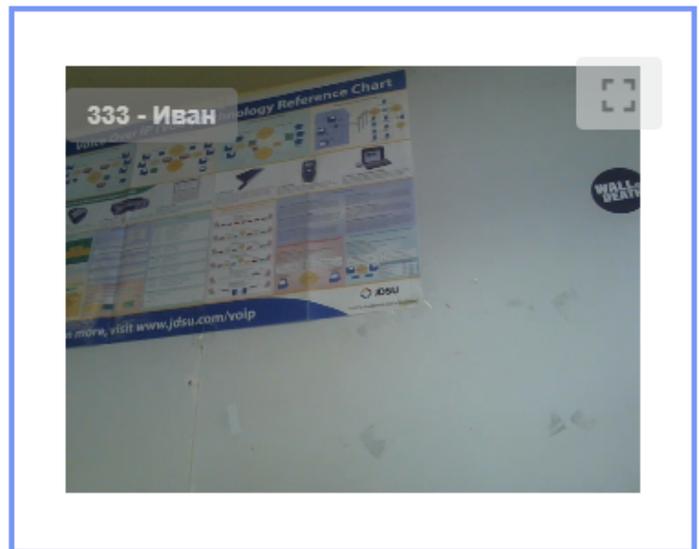
Enter the number ...



Users - 3

Conversation with 777

00:00:53



From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:xphone>

Last update: **2019/11/10 19:25**



Телефонные номера

Модуль «Телефонные номера» расположен в Меню «Телефония». Данный модуль предназначен для присвоения и работы с телефонными номерами Пользователей «ИКС». При открытии модуля «Телефонные номера» будет отображено дерево групп и телефонных объектов, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать, отправить факс, импорт, экспорт) активирующиеся при выборе группы или номера.

Муми-дол > Телефония > Телефонные номера

Туже Янссон 108

Добавить Удалить Выключить Редактировать Отправить факс Импорт Поиск...

Номера	Ip-адрес	Пользователь
Телефонная книга		
Хаттифнаты		
+7-987-654-32-10 Морра		
+7-777-777-77-77 Волшебник		
Телефонные номера		
Долина		
Семья		
Тусня		
007		Снусмумрик
111	192.168.17.43	Муми-троль
223		Снорк
322	192.168.17.5	Фрёкен Снорк
999		
777 Директор		Туже Янссон

В корне дерева находятся две группы объектов: «Телефонные номера» и «Телефонная книга». «Телефонные номера» предназначены для занесения в них телефонных объектов, являющихся внутренними. Для объектов «Телефонный номер» отображаются IP-адреса, для которых зарегистрированы номера и пользователи, закрепленные за этими номерами. Кроме телефонного номера, в «ИКС» могут быть заведены объекты «Факс» и «Конференция». Для объединения объектов следует использовать «Группы номеров».

Телефонный номер.

Объект «Телефонный номер» предназначен для совершения звонков через сервер телефонии. Для добавления телефонного номера необходимо нажать «Добавить» - «Телефонный номер», откроется диалоговое окно с двумя вкладками «Общее» и «Кодеки», при этом активна будет вкладка «Общее».

Добавление телефонного номера

Общее	Кодеки
--------------	--------

Номер *	Пароль
<input type="text" value="555"/>	<input type="password" value="••••••••"/>  
Описание (CallerID)	
<input type="text" value="Папа - домашний"/>	
Время ожидания	Максимальное число каналов
<input type="text" value="30"/>   сек.	<input type="text" value="(любое)"/>  
Пользователь *	
<input type="text" value="Муми-папа x"/> 	
<input type="checkbox"/> Разрешать подключаться извне	

Вкладка «Общее». Для создания объекта будет предложено ввести «Номер» (Обязательный параметр) и «Пароль» (не обязательный параметр). Пароль может быть сгенерирован автоматически при нажатии на кнопку в правой части поля. Поле «Описание» предназначено для краткого описания телефонного номера, которое будет отображаться в правилах телефонии, журнале звонков рядом с соответствующим номером, а так же будет использоваться как CallerID. Поле «Время ожидания» позволяет задать период времени, по истечении которого сервер телефонии посчитает абонента не ответившим на звонок, по умолчанию этот параметр задается в модуле «Настройки» меню «Телефония». Поле «Максимальное число каналов» определяет число каналов, которые номер может использовать. Поле «Пользователь» является обязательным, в нем необходимо выбрать Пользователя «ИКС», к которому будет прикреплен номер. Флаг «Разрешать подключаться извне» определяет, будет ли доступен номер для подключения из внешних сетей.

Важно: если вы указали флажок «Разрешить подключаться извне» для телефонного номера, то рекомендуется установить сложный пароль для того, чтобы он не был подобран злоумышленниками.

Доступ

SIP-клиент Xphone

Тип подключения

Без шифрования (UDP)

Уведомлять о пропущенных звонках на почту

Отправлять сообщения голосовой почты на почту

Email *

daddy@mumi.dol

Email *

daddy@mumi.dol

Флаги «Уведомлять о пропущенных звонках на почту» и «Отправлять сообщения голосовой почты на почту» активируют поля для указания соответствующих адресов.

В поле «Тип подключения» можно выбрать, использовать ли шифрование sip-пакетов и медиаданных (RTP) для этого номера с помощью сертификата, выбранного на вкладке общих настроек телефонии; без шифрования возможны два варианта подключения:

- Без шифрования (UDP) - это значение выбрано по умолчанию
- Без шифрования (TCP)

Чтобы включить шифрование, необходимо в поле «Тип подключения» выбрать значение - С шифрованием (TLS и SDES-sRTP). Данное значение активирует одновременное шифрование SIP-сигнализации через TLS и sRTP-медиаданных.

Каждый тип подключения требует соответствующей настройки своего транспорта, которая задается в меню «телефония» во вкладке «настройки».

Флаг «Доступ Xphone» отвечает за доступ к внутреннему номеру web-софтфона xphone.

Внимание! Как только флаг «Доступ Xphone» будет установлен, то доступ к номеру будет только для web-софтфона xphone. Для всех остальных sip-телефонов данный номер не будет доступен, так как xphone использует шифрование медиа данных только DTLS-sRTP, соответственно, добавочный номер конфигурируется с использованием только этого типа шифрования.

Общее **Кодеки**

- Использовать настройки по умолчанию
- Указать вручную

Использовать	>	Доступные кодеки
G.711 a-law	<	G.726
G.729		G.711 u-law
GSM		G.723
VP8 Video		Opus

Добавить Отмена

Вкладка «Кодеки». По-умолчанию используются кодеки, указанные в модуле «Настройки» меню «Телефония». При выборе флага «Указать вручную» будет активировано поле, в котором можно указать необходимые для данного номера кодеки, выбрав их из списка доступных.

Стоит отметить, что если с данного номера будут совершаться видео звонки, то должен быть выбран хотя бы один из кодеков: VP8, VP9, H.264.

Если не было создано DNS-зоны (с соответствующими записями), относительно **имени системы**, и создается первый телефонный номер, то «ИКС» предложит создать соответствующие записи.

Факс

Объект «Факс» предназначен для приема факсов на указанный номер и сохранения их в формате TIFF в папке Хранилища файлов.

Добавление номера факса

Номер *	Описание
<input type="text" value="100"/>	<input type="text" value="Волшебник"/>
Сохранять в папку *	
<input type="text" value="/primary/Шляпа Волшебника/"/>	
<input checked="" type="checkbox"/> Отправлять на почту	
Email *	
<input type="text" value="wizard@mumi.dol"/>	

Для добавления факса необходимо нажать «Добавить» - «Факс», откроется диалоговое окно, в котором будет предложено ввести два обязательных параметра : «Номер» и «Сохранять в папку». Поле «Описание» предназначено для краткого описания номера, которое будет отображаться в правилах телефонии и журнале звонков рядом с соответствующим номером. Флаг «Отправлять на почту» активирует поле для ввода адреса, на который будут дублироваться TIFF-файлы.

Стоит добавить, в модуле предусмотрена кнопка «Отправить факс» для отправки факса на внешний номер, которая активна независимо от выбранного в дереве объекта. При нажатии на нее откроется диалоговое окно, в котором будет предложено выбрать документ для отправки, внешний канал и ввести номер, на который необходимо отправить этот файл.

Отправить факс

Загрузить документ *
<input type="text" value="IMG_0214.jpg"/>
Внешний канал *
<input type="text" value="Муми SIP"/>
Отправить на номер *
<input type="text" value="100"/>

Конференция

Объект «Конференция» предназначен для определения телефонного номера, позвонив на который, каждый абонент будет слышать всех подключенных абонентов, также позвонивших на данный номер.

Администраторы

Ведущие

Ждать ведущего перед входом

Режим распределения видео

Для добавления конференции необходимо нажать «Добавить» - «Конференция», откроется новое диалоговое окно, в котором будет предложено ввести обязательный параметр «Номер». Поле «Число участников» позволяет определить, ограничивать ли количество участников, или выбрать значения от 2 до 9999. Поле «PIN-код» позволяет задать числовой код для доступа в конференцию, возможен выбор значения от 1 до 9999. Флаг «Объявлять число участников» определяет, оповещать ли вызывающую сторону о количестве Пользователей в конференции. Флаг «Воспроизводить объявление о первом участнике» отвечает за объявление Пользователю о том, что он входит в пустую конференцию. Язык диктора зависит от выбранного языка системы в «ИКС». Флаг «Запись вызовов» определяет включать ли запись аудиозвонка конференции.

Администраторы

Ведущие

Ждать ведущего перед входом

Режим распределения видео

По умолчанию всем участникам конференции доступно следующее DTMF меню:

1. выключить свой микрофон
2. выйти из конференции
3. уменьшить громкость приходящего к нему звука
4. вернуть громкость к дефолтному значению
5. увеличить громкость

Поле «Администраторы» предназначено для указания номеров Пользователей «ИКС», которые будут являться администраторами конференции. Для администратора во время конференции доступно расширенное DTMF меню:

1. выключить свой микрофон
2. выйти из конференции
3. уменьшить громкость приходящего к нему звука
4. вернуть громкость к дефолтному значению
5. увеличить громкость
6. стать единственным источником видео
7. отменить предыдущий пункт
8. закрыть/открыть конференцию
9. удалить из конференции последнего вошедшего

Поле «Ведущие» предназначено для указания номеров Пользователей «ИКС», которые будут являться источниками видеосигнала для всех остальных участников конференции, если выбраны настройки трансляции видео «Последний вошедший ведущий» или «Первый вошедший ведущий». Так же, статус ведущего позволяет начинать конференцию, если установлена галка «Ждать ведущего перед входом». Для ведущих во время конференции доступно расширенное DTMF меню:

1. выключить свой микрофон
2. выйти из конференции
3. уменьшить громкость приходящего к нему звука
4. вернуть громкость к дефолтному значению
5. увеличить громкость
6. стать единственным источником видео
7. отменить предыдущий пункт

Флаг «Ждать ведущего перед входом» определяет, будут ли обычные пользователи, зашедшие в конференцию, ждать, пока не присоединится хотя бы один ведущий конференции. Как только ведущий заходит - конференция начинает работать и все участники начинают слышать друг друга.

Поле «**Режим распределения видео**» предназначено для настройки способа распределения видео между участниками конференции. Участники видеоконференции должны использовать одинаковый видео кодек.

- Значение «**Источник видеосигнала не задан**» указывает, что нет источника видеосигнала по умолчанию, который увидят участники конференции, и источник видеосигнала будет выбран позже посредством DTMF меню.
- Значение «**Следовать за спикером**» переключает видеосигнал на говорящего в данный момент участника конференции.
- Значение «**Последний вошедший ведущий**» выбирает последнего вошедшего в конференцию пользователя, от которого есть видеосигнал и который отмечен как ведущий в качестве единственного источника видео для всех участников конференции.

Когда данный пользователь покидает конференцию, предыдущий ведущий, от которого поступает видеосигнал, становится источником видео для всех участников конференции.

- Значение **«Первый вошедший ведущий»** выбирает первого вошедшего в конференцию пользователя, от которого есть видеосигнал и который отмечен как ведущий в качестве единственного источника видео для всех участников конференции. Если данный участник выходит из конференции, то следующий пользователь, отмеченный как ведущий и от которого поступает видеосигнал, становится источником видеосигнала всех участников конференции.
- Значение **«Источники видео - все пользователи конференции (SFU)»** - Включает полноценную видеоконференцию, где каждый участник может транслировать свое видео, и видеть несколько видеопотоков других участников. Для корректной работы этого режима необходимо выбрать драйвер канала «chan_rj45» в модуле «Настройки» меню «Телефония». *Рекомендуемый режим работы видеоконференции для использования xhoney.*

Группа номеров

Объект «Группа номеров» предназначен для объединения телефонных номеров, факсов и конференций в группы, которые можно применять как объекты в правилах телефонии.

Добавление группы номеров

Название *

Семья

Добавить

Отмена

Для добавления группы номеров необходимо нажать «Добавить» - «Группа номеров», откроется диалоговое окно, в котором будет предложено ввести «Название» (обязательный параметр) и «Описание» (необязательный параметр). Стоит отметить, что созданные ранее номера, факсы и конференции можно перенести в нужную группу простым перетаскиванием соответствующей записи в нужную позицию списка.

Группировка номеров телефонии влияет на работу функции *Перехват в рамках группы*. Подробнее об этом написано в разделе «настройки»

Телефонная книга

«Телефонная книга» - объект таблицы телефонных номеров, предназначенный для номеров, заведенных на «ИКС», но не являющихся внутренними.

Добавить Удалить Выключить Редактировать Отправить факс Импорт			<input type="text" value="Поиск..."/>	
Номера ▲	Ip-адрес	Пользователь		
☐ Телефонная книга				
☐ Хаттифнаты				
☎ 8-999-555-44-33 Основной				
☎ 8-999-333-22-11 Запасной				
☎ +7-987-654-32-10 Морра				
☎ +7-777-777-77-77 Волшебник				
☐ Телефонные номера				
☐ Долина				
☐ Семья				

Номера телефонов входящих звонков на ИКС из внешних каналов сопоставляются с данной адресной книгой. Если входящий номер есть в этой книге, имя будет передано как CallerID на конечное устройство

Если в таблице номеров выбрать строку «Телефонная книга» и нажать кнопку «Добавить», будет предложено добавить: «Номер телефонной книги» или «Организация».

При выборе «Номер телефонной книги» откроется новое диалоговое окно, в котором необходимо ввести номер телефона абонента, не входящего в состав подопечных «ИКС» (внешний номер абонента), а также ввести описание. При поступлении или совершении звонка, такому абоненту, в журнале звонков отобразится номер телефона и заданное описание. Для объединения внешних абонентов в группу, необходимо нажать «Добавить» - «Организация», при этом будет открыто новое диалоговое окно, в котором необходимо указать название создаваемой группы. Стоит отметить, что созданные ранее номера телефонной книги можно перенести в нужную группу простым перетаскиванием соответствующей записи в нужную позицию списка.

При выборе объектов «Телефонной книги» активируются функциональные кнопки «Импорт» и «Экспорт».

При «Экспорте» телефонной книги, будет создан файл ics-<дата-время>-phonebook.txt. Форматом данных в *.txt файле является json. Стоит учесть, что экспортируются только телефонные номера, добавленные в телефонную книгу. Внутренние номера «ИКС» не экспортируются. Для импорта телефонных номеров следует использовать файл, формат данных в котором должен соответствовать формату данных при экспорте, либо иметь следующий формат: «телефонный номер, описание» и каждый новый абонент с новой строки. В последнем случае номера будут импортированы в корень телефонной книги.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:phone_numbers

Last update: **2019/11/10 19:25**



Внешние каналы

Модуль «Внешние каналы» расположен в Меню «Телефония». Данный модуль предназначен для того, чтобы настроить входящие и исходящие звонки во внешнюю сеть. При открытии модуля «Внешние каналы» будет отображен список провайдеров и туннелей, созданных в ИКС, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать) активирующиеся при выборе объекта.

Муми-дол > Телефония > Внешние каналы Туве Янссон 13

Добавить Удалить Выключить Редактировать

Муми SIP Зарегистрирован
Провайдер SIP(egggaaa@sipnet.ru)

Адрес сервера: sipnet.ru
Номер: 484-139-81-85
Логин: egggaaa
Правило: При звонке на номер, начинающийся с 9, отрезать 1 цифру с начала набранного номера
Режим DTMF: auto

Удалить Редактировать Выключить

IAX в муми-доле
Провайдер IAX(mumiki@iax.blablaba.com)

В ИКС поддерживаются два вида каналов - SIP и IAX, а также два вида аналогичных туннелей. Туннели предназначены для соединения телефонии двух ИКС. Чтобы настроить новый канал, нажмите кнопку «Добавить» и выберите тип нужного канала (транка).

Провайдер SIP

Объект «Провайдер SIP» предназначен для установки соединения с использованием протокола SIP. Для добавления внешнего канала необходимо нажать «Добавить» - «Провайдер SIP». Откроется диалоговое окно, в котором будет предложено ввести обязательные параметры: название, адрес сервера и порт.

Добавление провайдера SIP

Название *

Муми SIP

Максимальное число каналов

10

Адрес сервера *

sipnet.ru

Порт *

5060

Номер

4841398185

Логин

egggaaa

Пароль

••••••••

Автоматически создавать правило, используя префикс:

9

Поля «**Адрес сервера**» и «**Порт**» - предназначены для указания соответствующих настроек провайдера ip-телефонии для подключения. **Важно: при выборе порта необходимо учитывать значение поля «Тип подключения», так как обычно провайдеры предоставляют возможность подключения для разных протоколов на разных портах.**

Поле «**Номер**» предназначено для указания внешнего номера для совершения звонков через сервер телефонии ИКС.

Поля «**Логин**» и «**Пароль**» отвечают за данные для авторизации при подключении ИКС к серверу провайдера.

Поле «**Максимальное число каналов**» предназначено для указания максимального числа одновременных соединений через провайдера (по умолчанию 100).

Флаг «**Автоматически создавать правило, используя префикс**» активирует поле 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.

Режим DTMF	Опция insecure	Опция canreinvite	Опция direct_media
auto	invite	yes	no
Тип подключения			
С шифрованием (TLS и SDES sRTP)			

Опции «**Режим DTMF**», «**insecure**», «**canreinvite**» позволяют настроить режимы тонального набора, при этом две последние доступны только при выборе драйвера `chan_sip` в [настройках Телефонии](#). Опция «**direct_media**», наоборот, доступна только для драйвера `chan_pjsip` и определяет, могут ли медиаданные передаваться напрямую между конечными точками. Если `no`, то все RTP потоки проходят через Asterisk.

В поле «**Тип подключения**» можно выбрать, использовать ли шифрование sip-пакетов и медиаданных (RTP) для этого номера с помощью сертификата, выбранного на вкладке общих настроек телефонии; без шифрования возможны два варианта подключения: через *UDP* (это значение выбрано по умолчанию) и через *TCP*. Чтобы включить шифрование, необходимо в поле «Тип подключения» выбрать значение «*С шифрованием (TLS и SDES-sRTP)*». Данное значение активирует одновременное шифрование SIP-сигнализации через TLS и sRTP-медиаданных.

Важно: каждый тип подключения требует соответствующей настройки своего транспорта, которая задается в [настройках Телефонии](#). То есть, для каждого типа подключения необходимо задать нужный порт.

Указать строку регистрации вручную

Строка регистрации *

From User

egggaaa

Поддерживать подключение

 ↑ ↓ мс

Сохранить

Отмена

Если провайдер имеет специфические настройки, то следует полностью прописать строку регистрации, установив соответствующий флаг. Стоит отметить, что строка регистрации доступна только для драйвера `chan_sip`. Для драйвера `chan_pjsip` она создается автоматически.

Важно: в некоторых случаях провайдер SIP-телефонии не может распознать абонента, набирающего внешний вызов. Если при регистрации провайдера работают входящие

звонки, но не проходят исходящие, то в поле «fromUser» необходимо указать номер телефона либо логин подключения (в зависимости от особенностей провайдера).

Поле «**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.

Провайдер IAX

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 медиа-потока. Аналогично провайдеру SIP, провайдер IAX в качестве параметров запрашивает сервер и порт подключения, телефонный номер, при необходимости логин и пароль, внешний префикс, режим DTMF и, если нужно, строку регистрации.

Туннели

Туннели предназначены для соединения серверов телефонии нескольких ИКС. При создании туннеля необходимо ввести обязательные параметры: название и логин. Настройка полей для указания максимального числа каналов, пароля, префикса, строка регистрации и опции «From User» аналогично настройке соответствующих полей объекта [Провайдер SIP](#).

Тип подключения

Сервер

Адрес клиента

(auto)

Клиент

Адрес сервера *

192.168.17.243

Порт *

5060

Опция, отличная от настроек провайдера SIP - «**Тип подключения**». При использовании канала связи для подключения к внешнему серверу провайдера, то необходимо использовать опцию «клиент». В случае, когда к ИКС подключаются другие клиенты по внешнему каналу, используйте опцию «сервер». Другими словами, один из ИКС выбирается сервером, а второй клиентом.

From:
<https://doc.a-real.ru/> - **Документация**

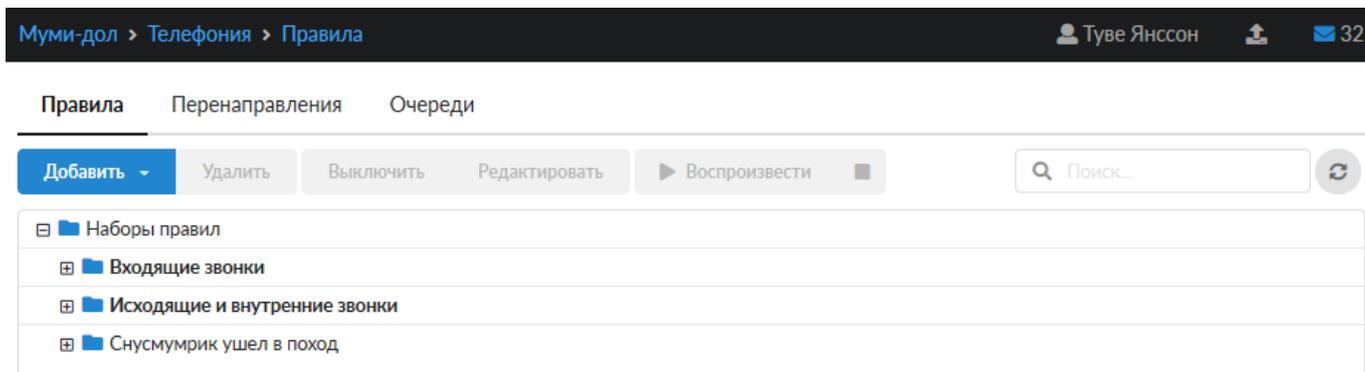
Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:trunks>

Last update: **2019/11/10 19:25**



Правила

Модуль «Правила» расположен в Меню «Телефония». При открытии модуля в основном окне отобразятся вкладки «Правила», «Перенаправления» и «Очереди», при этом вкладка «Правила» будет активна. Этот модуль предназначен для управления логикой обработки и маршрутизации входящих и исходящих вызовов.

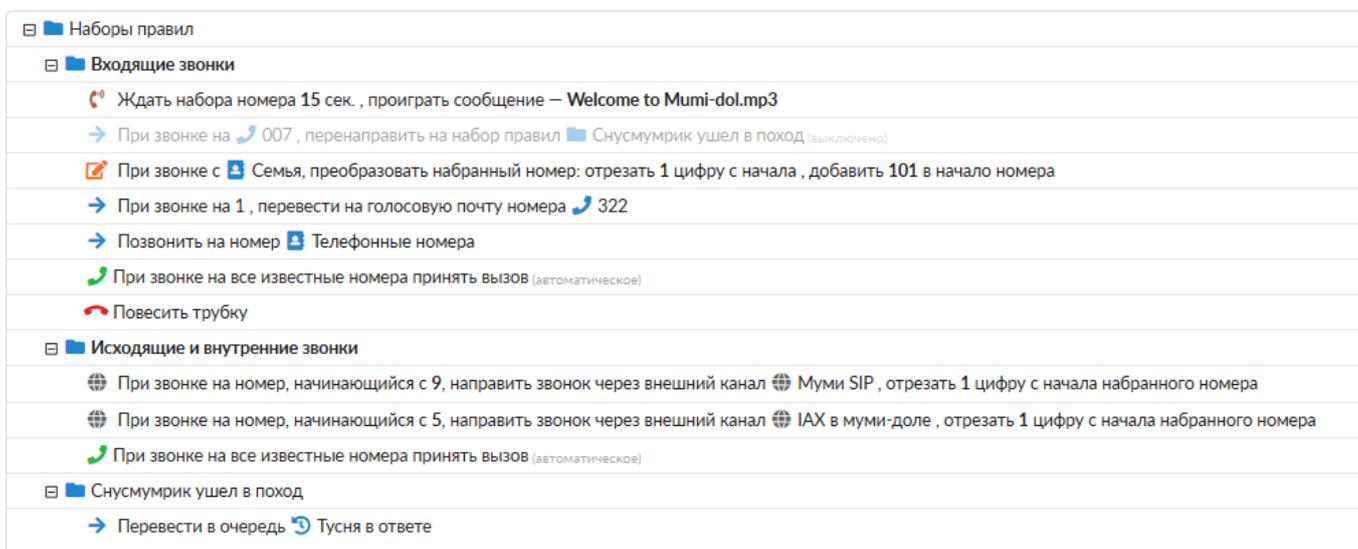


Правила

На данной вкладке отображаются наборы правил телефонии, а также строка поиска и функциональные кнопки (добавить, удалить, выключить, редактировать, воспроизвести), активирующиеся при выборе правила или набора.

Все звонки по умолчанию разделяются на две группы: **«входящие»** и **«внутренние и исходящие»**. В набор «Входящие звонки» попадают звонки, входящие на ИКС с внешних транков. В набор «Исходящие и внутренние звонки» попадают исходящие и входящие звонки с внутренних телефонных номеров ИКС.

Правила в наборах выполняются друг за другом, по очереди, сверху вниз.



При необходимости, можно добавить, выключить, удалить правила или поменять их порядок перетаскиванием строки в нужную позицию списка в существующих наборах, либо добавить

собственные наборы правил. Правила, которые можно добавить в набор:

принять вызов	Предназначено для приема звонка, дальнейшие правила не будут учитываться
повесить трубку	Предназначено для завершения звонка, дальнейшие правила не будут учитываться
ждать набора номера	Предназначено для задания времени ожидания набора пользователем дополнительного номера с возможностью проигрывания сообщения, например для голосового меню
перенаправить вызов	Предназначено для перенаправления вызова на конкретные номера, в набор правил, очередь или на голосовую почту
преобразовать номер	Предназначено для преобразования номера звонящего или набранного номера
звонок через внешний канал	Предназначено для маршрутизации вызова через конкретного провайдера и преобразования набранного номера

Во всех правилах, кроме «Принять вызов» можно указать условия срабатывания правила, применяемые к номеру звонящего или набранному номеру.

Действие
Условия

Номер звонящего

Совпадает с
 Начинается с

Длина номера от

до

С провайдера

Применять к вызовам, перенаправленным с таких номеров

Для задания условий на вкладке «Условия» следует заполнить следующие поля: выбрать вариант сравнения номера звонящего и/или набранного номера. В поле «Совпадает с» можно выбрать номер, группу номеров или указать внешний номер вручную. В поле «Начинается с» можно указать комбинацию цифр, стоящую в начале номера, дополнительно можно задать длину номера, используя соответствующие поля. Для номера звонящего также можно задать конкретного провайдера, с которого поступает звонок и применять к вызовам, перенаправленным с таких номеров, отметив соответствующий флаг.

Время действия

Во всех правилах, кроме «Принять вызов» и «Повесить трубку» можно указать время действия: объект «Временной промежуток», созданный на ИКС или дни недели и часы.

Принять вызов

Правило «Принять вызов» предназначено для приема звонка, все правила, идущие после него не будут учитываться. Для добавления этого правила необходимо нажать «Добавить» - «Принять вызов», откроется диалоговое окно, где будет предложено выбрать, на какие именно номера следует принять вызов: все известные номера, конкретные номера либо все номера, кроме указанных.

Принять вызов на:

- Все известные номера
- Все известные номера, кроме

- Только определённые номера

Повесить трубку

Правило «Повесить трубку» предназначено для завершения звонка, все правила, идущие после него не будут учитываться. Для добавления этого правила необходимо нажать «Добавить» - «Повесить трубку», откроется диалоговое окно, где будет предложено указать условия для срабатывания этого правила.

Ждать набора номера

Правило «Ждать набора номера» предназначено для ожидания набора номера. Для добавления этого правила необходимо нажать «Добавить» - «Ждать набора номера», откроется диалоговое окно с двумя вкладками «Действие» и «Условия», при этом активна будет вкладка «Действие».

Действие Условия

Ждать набора номера

 ↑ ↓ сек.

Проиграть сообщение

 Загрузить   Воспроизвести   Удалить мелодию

Описание *

Поле «Ждать набора номера» предназначено для указания времени ожидания ввода пользователем номера в секундах.

Флаг «Проиграть сообщение» активирует функциональные кнопки для загрузки, воспроизведения и удаления мелодии ожидания, а также поле «Описание» (по умолчанию в это поле после загрузки файла будет подставлено его название).

Перенаправить вызов

Правило «Перенаправить вызов» предназначено для перенаправления вызова на другие номера, наборы правил, очереди или голосовую почту. Для добавления этого правила необходимо нажать «Добавить» - «Ждать набора номера», откроется диалоговое окно с двумя вкладками «Действие» и «Условия», при этом активна будет вкладка «Действие».

Действие	Условия
<input type="radio"/> Позвонить на номера	<div><input type="text" value="Семья"/></div> <div><input checked="" type="checkbox"/> Ждать ответа</div> <div><input type="text" value="15"/> сек.</div> <div><input type="checkbox"/> Разрешить перенаправление при неответе</div>
<input checked="" type="radio"/> Перенаправить на набор правил	<div><input type="text" value="Снусмумрик ушел в поход"/></div>
<input type="radio"/> Перевести в очередь	<div><input type="text" value="Тусня в ответе"/></div>
<input type="radio"/> Перевести на голосовую почту номера	<div><input type="text" value="007"/></div>

Позвонить на номера. Для перенаправления вызова на другие номера, необходимо выбрать номер или группу из списка телефонных номеров ИКС, при этом вызов будет поступать на все указанные номера одновременно. Возможно указать время ожидания ответа в соответствующем поле, активировав его флагом «Ждать ответа», прежде чем сервер перейдет к проверке следующего правила. Флаг «Разрешить перенаправление при неответе» активируется в случае указания одного конкретного номера, в этом случае, при неответе этого номера наличии у этого номера перенаправлений, произойдет перенаправление вызова номерам, указанным в перенаправлениях.

Перенаправить на набор правил. Для перенаправления вызова в другой набор правил, необходимо выбрать набор правил в соответствующем поле. Переход к следующему правилу произойдет после перебора всех правил указанного набора, в случае если не произойдет приема или прекращения вызова.

Перевести в очередь. Для перенаправления вызова в очередь, необходимо выбрать очередь в соответствующем поле. Если в настройках очереди указано, в какой набор правил необходимо выйти, то вызов перейдет к первому правилу этого указанного набора.

Перевести на голосовую почту номера. Для перенаправления вызова на голосовую почту, необходимо выбрать телефонный номер ИКС в соответствующем поле. Следующие правила не будут выполнены.

Действие Условия

Использовать внешний канал *

Муми SIP ✕

Отрезать с начала набранного номера

1 ^ цифру v

Добавить в начало номера

Перезвонить при занятости

через

10 ^ сек. v

Поле «Использовать внешний канал» является обязательным, в нем необходимо указать провайдера или туннель, созданные на ИКС. Также возможно указать, сколько цифр с начала номера надо заменить и на какие в соответствующих полях.

Флаг «Перезвонить при занятости» активирует поле для указания таймаута, через который вызов будет совершен повторно при недоступности провайдера.

Перенаправления

На данной вкладке отображаются перенаправления телефонии при неответе вызываемого абонента. Такие правила предназначены для перенаправления звонков, если вызываемый абонент не отвечает или занят. Также вкладка содержит строку поиска и функциональные кнопки (добавить, удалить, выключить, редактировать), активирующиеся при выборе перенаправления.

Правила **Перенаправления** Очереди

Добавить Удалить Выключить Редактировать Поиск... ↻

При неответе номера 📞 111 позвонить на 📞 322, 📞 223 и ждать ответа 15 сек.
Перенаправление при неответе (При неответе Муми-троля переадресовать вызов Сноркам)
Обрабатывать, если номер занят

Удалить Редактировать Выключить

При неответе номера 📞 007 позвонить на 📠 Тусня
Перенаправление при неответе (Если Снусмумрик не отвечает позвонить всей тусне)

Для добавления перенаправления необходимо нажать кнопку «Добавить», откроется диалоговое окно, где будет предложено указать обязательные параметры: вызываемый номер и номера, на которые будет перенаправлен вызов. В качестве телефонных номеров в оба поля

также можно указать группу номеров, будут подразумеваться номера, которые находятся в этой группе. В поле «Позвонить на» может также быть указан внешний номер, не созданный на ИКС.

Добавление перенаправления при неответе

При неответе номера *

☎ 111 ×

Позвонить на *

☎ 322 × ☎ 223 ×

Описание

При неответе Муми-троля переадресовать вызов сноркам

Ждать ответа

15 сек.

Обрабатывать, если номер занят

Добавить Отмена

Поле «Описание» предназначено для указания текста, которое будет отображаться в интерфейсе ИКС рядом с названием правила.

Флаг «Ждать ответа» активирует поле для указания времени ожидания в секундах.

Флаг «Обрабатывать, если номер занят» указывает, что правило перенаправления будет применяться также при занятости указанных номеров.

Перенаправления при неответе так же можно просматривать во вкладке «Перенаправления» в модуле каждого пользователя.

Муми-дол > Пользователи > Муми-троль > Перенаправления Тыве Янссон 21

Правила и ограничения | Почта и телефония | **Перенаправления** | OpenVPN | Приложения | Стати

Добавить | Удалить | Выключить | Редактировать | Поиск...

При неответе номера ☎ 111 позвонить на ☎ 322, ☎ 223 и ждать ответа 15 сек.
Перенаправление при неответе (При неответе Муми-троля переадресовать вызов Сноркам)

При неответе номера 📠 Тусня позвонить на ☎ 101
Перенаправление при неответе

Если у пользователя создан телефонный номер и в ИКС созданы перенаправления, в которых

этот номер указан в поле «При неответе номера», то во вкладке будут отображены все такие перенаправления. При этом, те перенаправления, в которых этот номер указан как единственный, будут доступны к редактированию.

Важно: по умолчанию, в модуле телефонии ИКС, действует правило - при ручной переадресации входящего звонка на внутренний номер другого абонента, если нажать *, то переадресация будет прервана.

Очереди

На данной вкладке отображаются очереди телефонии. Очереди предназначены для удержания вызовов, пока какой либо номер не ответит или источник не положит трубку. Также вкладка содержит строку поиска и функциональные кнопки (добавить, удалить, редактировать, воспроизвести), активирующиеся при выборе перенаправления.

Правила Перенаправления **Очереди**

Добавить Удалить Редактировать ▶ Воспроизвести [■] Поиск... [↻]

↻ Тусня в ответе
Очередь

Телефонные номера: Тусня
Стратегия: Звонить всем
Таймаут: 15 сек.
Время выхода из очереди: 60 сек.
Проиграть сообщение: Abonent unavailable now.mp3

Удалить Редактировать

Для добавления очереди необходимо нажать кнопку «Добавить», откроется диалоговое окно, где будет предложено указать обязательные параметры: название очереди и телефонные номера, на которые будет производиться вызов. В качестве телефонных номеров также можно указать группу номеров, тогда вызов будет перенаправлен номерам, которые находятся в этой группе.

Добавление очереди

Название *

Телефонные номера *

Стратегия

Таймаут

 сек.

Время выхода из очереди

 сек.

Не звонить, если номер занят

Поле «Стратегия» предназначено для указания распределения вызовов в очереди:

- *Звонить всем.* Вызов происходит всему списку указанных номеров одновременно.
- *Звонить по очереди.* Вызов начинается с первого указанного номера, и при неответе происходит вызов следующему номеру.
- *С наименьшей нагрузкой.* Обзвон начинается с номера, принявшего меньше всего вызовов.
- *Случайно.* Телефонные номера будут перебираться в случайном порядке.

Поле «Таймаут» указывает, в течение какого промежутка времени (в секундах), будет вызываться телефон пользователя, прежде чем будет считаться, что он не ответил.

Поле «Время выхода из очереди» предназначено для указания времени, по истечении которого звонок попадёт обратно в исходный список правил и будет обрабатываться следующим правилом.

Проиграть сообщение

[Загрузить](#) [✕](#) [▶ Воспроизвести](#) [■](#) [🗑 Удалить мелодию](#)

Описание *

Abonent unavailable now.mp3

Оповещать в очереди

О номере в очереди ▾

Каждые *

60 [^](#) [v](#) сек.

Выйти из очереди при нажатии

[^](#) [v](#)

В набор правил *

▾

[Добавить](#)

[Отмена](#)

Флаг «Проиграть сообщение» активирует функциональные кнопки для загрузки, воспроизведения и удаления мелодии ожидания, а также поле «Описание» (по умолчанию в это поле после загрузки файла будет подставлено его название).

Поле «Оповещать в очереди» предназначено для выбора оповещений о статусе абонента в очереди. Возможен выбор оповещений о времени ожидания и/или номере в очереди, а также отключение оповещений. Если выбрано, о чем оповещать абонента при ожидании, становится активно поле для указания частоты оповещений.

Флаг «Выйти из очереди при нажатии» активирует два поля: указание комбинации цифр для выхода и набор правил, в который необходимо выйти. При этом звонок перейдет к первому правилу в указанном наборе правил.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: https://doc.a-real.ru/doku.php?id=ics70:asterisk_rules

Last update: **2019/11/10 19:25**



Монитор звонков

Модуль «Монитор звонков» расположен в Меню - «Телефония».

Данный модуль отображает все входящие и исходящие телефонные переговоры в режиме on-line, проходящие через «ИКС». В основном окне модуля отображается таблица с текущими звонками, а также поле «Провайдер», предназначенное для установки фильтра отображения звонков по имени провайдера, заведенного в «ИКС».

Муми-дол > Телефония > Монитор звонков Туге Янссон 15

Внешний канал (любой) ↻

Источник	Назначение	Состояние	Перевод с	Продолжительность	Внешний канал
+7-987-654-32-10	☎ 111	Разговор		00:07:45	🌐 Муми SIP
+7-987-654-32-10	☎ 007	Разговор	☎ 111	00:06:37	🌐 Муми SIP
☎ 322	☎ 777	Разговор		00:01:43	
☎ 101	+7-123-456-78-90	Разговор		00:00:21	🌐 Муми SIP

В таблице выводится следующая информация о каждом текущем вызове:

- Источник
- Назначение
- Состояние звонка
- Номер, с которого осуществлен перевод звонка
- Продолжительность вызова
- Внешний канал, через который осуществляется данный звонок

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:phone_monitor

Last update: **2019/11/10 19:25**



Журнал звонков

Модуль «Журнал звонков» расположен в Меню - «Телефония».

В журнале звонков перечислены все входящие и исходящие звонки в систему, в том числе перенаправленные и неотвеченные.

Время	Источник	Назначение	Отвечил	Длительность	Результат
03.10.2019 08:25:42	777-777-77-77 Волшебник	800-555-92-97 Муми-дол - внешний многоканальный номер	114 Френк Снорк (Телефонные номера)	54 сек	Разговор
03.10.2019 08:26:32	777-777-77-77 Волшебник	800-555-92-97 Муми-дол - внешний многоканальный номер		4 сек	Звонок без ответа
03.10.2019 08:30:24	777-777-77-77 Волшебник	142 Муми-мама (Телефонные номера)	142 Муми-мама (Телефонные номера)	15 мин 29 сек	Разговор
03.10.2019 08:44:01	777-777-77-77 Волшебник	2	115 Муми-троль (Телефонные номера)	1 мин 53 сек	Разговор

Параметры

В левой части окна расположены поля для задания параметров выборки звонков.

Детализация звонков

Группировка *

По дням ✕

Источник

Телефонные номера ✕

Назначение

+79876543210 ✕

Ответил

(любой) ✕

Результат

Разговор ✕

Время с по

08:00 17:00

Показать

Флаг «Детализация звонков» предназначен для просмотра всех звонков за период. При установке этого флага поле «Группировка» становится неактивным.

Поле «Группировка» предназначено для формирования отчета по времени (по месяцам, дням или часам), источникам или назначениям. Возможен выбор только одного значения для группировки записей.

Поля «Источник», «Назначение» и «Ответил» предназначены для выбора записей, соответствующие столбцы которых подходят под заданные значения. Возможно выбрать номер или группу номеров, заведенных в ИКС либо указать номер вручную.

Поле «Результат» предназначено для фильтрации записей по типу звонка: «разговор», «звонок без ответа», «линия занята» и «ошибка соединения».

Поля «Время с» и «по» предназначены для указания временного промежутка для фильтрации записей.

Воспроизведение

Если в [Настройках Телефонии](#) проставлен флаг «Записывать звонки» и длительность разговора составляет более 5 секунд, то при выделении строки таблицы активируются кнопки «Воспроизвести» и «Скачать». Файл аудиозаписи представлен в формате .mp3

▶ Воспроизвести ■ Скачать ⬆ Экспорт ▾

Назначение	Отвечил	Длительность	Результат
☎ 800-555-92-97 Муми-дол - внешний многоканальный номер		4 сек	Звонок без ответа
☎ 142 Муми-мама (Телефонные номера)	☎ 142 Муми-мама (Телефонные номера)	15 мин 29 сек	Разговор
2	☎ 115 Муми-троль (Телефонные номера)	1 мин 53 сек	Разговор

Экспорт

Полученные в результате фильтрации данные, можно экспортировать в файл (.csv, .txt, .xls) для дальнейшей распечатки. При выборе одного из форматов, будет открыто новое диалоговое окно «Настройки», в котором будет предложено уточнить как экспортировать таблицу («Экспортировать все страницы»). Также на данной вкладке предлагается выбрать временной интервал отображения отчета: «Сегодня» (отобразятся звонки за текущий день), «Неделя» (отобразятся звонки за текущую неделю с понедельника по воскресенье), «Месяц» (отобразятся звонки за текущий месяц с первого по последний день), «Другой период» (необходимо указать период).

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:phone_log

Last update: **2019/11/10 19:25**



Система

Модуль «Система» расположен в Меню «Обслуживание». Данный модуль предназначена для того, чтобы можно было: ввести название организации, которое будет отображаться в веб-интерфейсе; ввести доменное имя системы; произвести удаление данных; просмотреть текущие задачи в «ИКС» (создание резервной копии, импорт пользователей и т.д.). Модуль «Система» имеет четыре вкладки: «Система», «Удаление данных», «Журнал», «Задачи».

Система

The screenshot shows the 'Система' configuration page. At the top, there is a navigation bar with 'ИКС > Система' on the left, a user profile 'Администратор' in the center, and a notification icon with '20' on the right. Below the navigation bar, there are four tabs: 'Система' (active), 'Удаление данных', 'Журнал', and 'Задачи'. The main content area contains a form with the following elements: a text input field for 'Название организации' containing 'ИКС'; a text input field for 'Имя системы *' containing 'testics.local'; a checked checkbox labeled 'Разрешить ИКС отправлять анонимную статистику'; a green 'Сохранить' button; a grey 'Обновить' button; and a blue 'Мастер начальной настройки системы' button with a pencil icon.

Вкладка «Система». На данной вкладке расположены поля для ввода данных: «**Название организации**» (будет отображаться в веб-интерфейсе «ИКС») и «**Имя системы**» (hostname), стоит отметить, что при изменении данного имени необходимо создать соответствующую запись в [DNS-сервере](#), иначе сервер телефонии, почты и Jabber-сервер не будут функционировать. Флаг «**Разрешить ИКС отправлять анонимную статистику**» доступен, если на ИКС приобретена лицензия больше, чем на 8 пользователей. Если он отмечен, то с ИКС будет собираться анонимная статистика.

При нажатии кнопки «**Мастер начальной настройки системы**» будет открыто новое диалоговое окно. В котором будет предложено ввести поэтапно: название организации, имя системы (hostname), а также изменить логин и пароль для входа в веб-интерфейс программы первого (по времени) Пользователя «ИКС» с ролью «Администратор».

Удаление данных

Система **Удаление данных** Журнал Задачи

Ручное удаление данных

Автоматически удалять:

Логи статистики	квота (сейчас занято 81К)
<input type="text" value="никогда"/>	<input type="text" value="0"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб
Логи детализированной статистики	квота (сейчас занято 291К)
<input type="text" value="старше недели"/>	<input type="text" value="64"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб
Записи звонков	квота (сейчас занято 2К)
<input type="text" value="старше 3 месяцев"/>	<input type="text" value="128"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб
Логи системы	квота (сейчас занято 782К)
<input type="text" value="старше года"/>	<input type="text" value="256"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Мб

Сохранить

Обновить

Вкладка «Удаление данных». Позволяет удалить различные логи (данные содержащиеся на «ИКС») и записи звонков в автоматическом режиме или в ручном режиме.

Ручное удаление данных

Удалить с по

- Логи статистики
- Логи детализированной статистики
- Записи звонков
- Логи системы

Ручной режим. Для ручного удаления данных необходимо нажать «Ручное удаление данных», при этом откроется новое диалоговое окно, в котором будет предложено указать границы временного периода и выбрать данные, которые необходимо удалить (логи статистики, логи

детализированной статистики, записи звонков, логи системы). После нажатия кнопки «**Ок**» выбранные данные будут безвозвратно удалены.

Автоматический режим. Позволяет задать временные рамки или квоту (в Мб) при которой «ИКС» будет удалять хранящиеся данные (логи статистики, логи детализированной статистики, записи звонков, логи системы). Если заданы временные рамки и квота, то удаление данных будет происходить в зависимости от параметра, который будет достигнут ранее. 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.

Под логами статистики понимаются данные собранные из детализированной статистики и объединенные по различным признакам для уменьшения занимаемого места на жестком диске и оптимизации времени составления отчетов. Стоит отметить, что данные логи не содержат: данные по ip, данные по http, данные ленты поисковиков и данные активности пользователей. При удалении логов статистики их можно восстановить по соответствующим логам детализированной статистики.

Под логами детализированной статистики понимается вся собранная «ИКС» статистика с Пользователей без каких-либо объединений и группировок. При удалении детализированной статистики данные будут безвозвратно удалены.

Под записями звонков понимаются записи телефонных звонков, совершенные с помощью сервера телефонии в ИКС.

Под логами системы понимаются данные [системного журнала](#) и данные отображаемые во вкладках «События» и «Журнал» всех модулей «ИКС».

Журнал

04.10.2019 - 04.10.2019

Сегодня

Неделя

Месяц

Другой период ▾



 Экспорт  Удалить логи

Поиск... 

↓↑
auto clean stat started 11:25:59
auto clean system logs started 11:25:59
auto clean phone logs started 11:25:59
auto clean system logs finished 11:25:59
auto clean phone logs finished 11:25:59
auto clean stat finished 11:25:59

« < Стр 1 из 1 > »

Показаны записи 1 - 6 из 6

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «Система» 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) - 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**».

Журнал

04.10.2019 - 04.10.2019

Сегодня

Неделя

Месяц

Другой период ▾



 Экспорт

Удалить логи

Поиск...



auto clean stat started

11:25:59

auto clean system logs started

11:25:59

auto clean phone logs started

11:25:59

auto clean system logs finished

11:25:59

auto clean phone logs finished

11:25:59

auto clean stat finished

11:25:59

« < Стр 1 из 1 > »

Показаны записи 1 - 6 из 6

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «Система» 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) - 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**».

Задачи

ИКС > Система > Задачи

Администратор 563

Система Удаление данных Журнал **Задачи**

local

backup.jobMake 39%

Created: 04.10.2019, 12:27:27
Started: 04.10.2019, 12:27:27

Cancel

Вкладка «Задачи». Отображает выполняющиеся асинхронные процессы в «ИКС», а также процент выполнения для каждого процесса. Нажав на кнопку «**Cancel**» можно прервать выполнение соответствующего процесса. При выполнении асинхронного процесса Пользователь «ИКС» может производить различные настройки в GUI «ИКС». Асинхронными процессами являются: перенос почты, импорт пользователей, создание резервной копии и т.д.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:system>

Last update: **2019/11/10 19:25**



Все службы

Модуль «Все службы» расположен в Меню «Обслуживание». В данном модуле отображается список всех служб «ИКС», а также присутствует возможность управления ими (Включение/Выключение).

Статус службы (Включена/Выключена) сохраняется между перезагрузками, отключенная служба не будет запущенf при следующем включении питания «ИКС». Клик по названию службы откроет соответствующую страницу в «ИКС», если она доступна.

ИКС > Все службыАдминистратор 568

Название	Состояние
Application Firewall Отвечает за блокировку приложений прользователей	не настроен
Arpwatch Мониторинг соответствия между ip и mac-адресами	запущен
Captive portal Отвечает за авторизацию пользователей через веб страницу	не настроен
DHCP-сервер Отвечает за автоматическую настройку сетевых параметров локальной сети	не настроен
DLP Обеспечивает защиту от утечек информации	не настроен
DNS-сервер Служба доменных имен	запущен
DynDNS Регистрирует ip-адрес на сервере динамического DNS	не настроен

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:allservices>

Last update: **2019/11/10 19:25**



Резервные копии

Модуль «Резервные копии» расположен в Меню «Обслуживание». Данный модуль предназначен для управления, создания и удаления копий данных в «ИКС». Основное окно модуля имеет три вкладки: «Резервные копии», «Шаблоны» и «Настройки».

Резервные копии

Вкладка «**Резервные копии**». На данной вкладке представлены имеющиеся резервные копии «ИКС» и инструменты работы с ними.

The screenshot displays the 'ИКС > Резервные копии' interface. At the top, there is a navigation bar with 'Резервные копии', 'Шаблоны', and 'Настройки' tabs. Below the tabs, there are action buttons: 'Добавить' (Add), 'Удалить' (Delete), 'Загрузить' (Upload), and 'Загрузить из хранилища файлов' (Upload from file storage). A search bar and a refresh icon are also present. The main content area shows a list of backup files. The first entry is 'testics.local-2019.09.04-11.39.41-s-7.0.0.1909041000-backup' (Reserve copy (settings)). The second entry is 'testics.local-2019.09.17-11.59.45-stmcfu-7.0.0.1909041000-backup' (Reserve copy (settings, statistics, mail, call records, web resource databases, files: primary, secondary)). Details for the second backup include: Date: 17.09.2019 11:59, Size: 136.27M, Location: Основной системный раздел Mirgor, Version: 7.0.0.1909041000, and Comment: Полный бэкап. Action buttons for the second backup are 'Удалить' (Delete), 'Восстановить' (Restore), 'Скачать' (Download), and 'Скопировать на FTP' (Copy to FTP).

Чтобы создать резервную копию данных «ИКС» нужно нажать кнопку «**Добавить**». После нажатия будет открыто новое диалоговое окно, в котором будет предложено выбрать данные для резервного копирования:

- настройки «ИКС»;
- все собранные «ИКС» статистические данные;
- все почтовые сообщения, хранящиеся на «ИКС»;
- записи всех звонков телефонии;
- базы данных всех веб-ресурсов;
- папки из хранилища файлов.

Так же есть возможность добавить комментарий к создаваемому бэкапу.

Добавление резервной копии

- Настройки
- Статистика
- Почта
- Записи звонков
- Базы данных веб-ресурсов
- Файлы

- primary
- secondary

Комментарий

Добавить Отмена

После выбора нужных данных необходимо нажать кнопку **«Добавить»**. В результате будет создана резервная копия в формате <имя системы>-<дата>-<время создания>-<обозначение содержания резервной копии>-<версия «ИКС»>-backup.

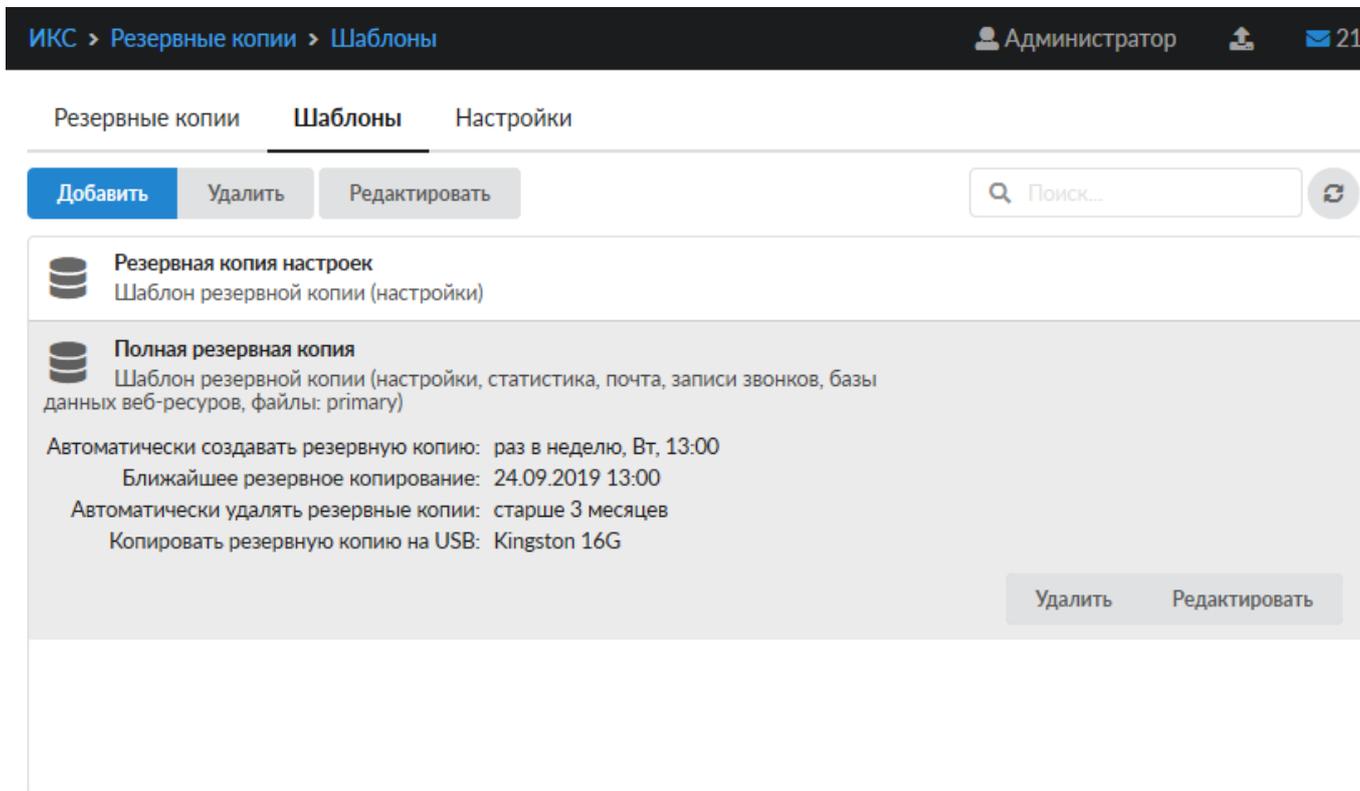
Также на данной вкладке можно удалить ранее созданные бэкапы, загрузить из сторонних источников в формате *.bin (кнопка **«Закачать»**), или загрузить из файлового хранилища «ИКС» нажав **«Загрузить из хранилища файлов»**.

При выборе резервной копии станут доступны кнопки: **«Удалить»**, **«Восстановить»**, **«Скачать»**, **«Скопировать на FTP»**. При нажатии на кнопку **«Восстановить»** «ИКС» восстановит сохраненные данные, при этом, если при сохранении резервной копии не был выбран пункт, например, «Статистика», то статистические данные, накопившиеся за промежуток времени от создания копии до ее восстановления, не будут изменены. Для сохранения резервной копии вне дискового пространства «ИКС» необходимо нажать **«Скачать»** и указать место сохранения. При нажатии на кнопку **«Скопировать на FTP»**, «ИКС» попытается скопировать резервную копию на ftp-сервер, указанный во вкладке **«Настройки»**. Результат выполнения данной операции можно посмотреть в [СИСТЕМНОМ журнале](#).

Шаблоны

Вкладка **«Шаблоны»**. Предназначена для создания резервных копий по заданному шаблону в

указанное время, а также удаление созданных ранее резервных копий и копирование на заданный ftp-ресурс и внешний носитель. В «ИКС» имеется два предустановленных шаблона: «Резервная копия настроек» (сохраняет только настройки «ИКС») и «Полная резервная копия» (сохраняет полную резервную копию «ИКС»). Для активации одного из шаблонов, необходимо указать время его срабатывания.



Для создания шаблона резервной копии необходимо нажать «**Добавить**». Будет открыто новое диалоговое окно «Добавление шаблона резервной копии». Данное окно имеет три вкладки: «Общие настройки», «Расписание» и «Копирование».

Во вкладке «**Общие настройки**» обязательным является введение названия шаблона, а также выбор одного из пунктов данных для резервного копирования (настройки «ИКС»; все собранные «ИКС» статистические данные; все почтовые сообщения, хранящиеся на «ИКС»; записи всех звонков; базы данных всех веб-ресурсов; папки из хранилища файлов).

Редактирование шаблона резервной копии

Общие настройки Расписание Копирование

Название *

- Настройки
- Статистика
- Почта
- Записи звонков
- Базы данных веб-ресурсов
- Файлы

primary	<input type="checkbox"/>
secondary	<input checked="" type="checkbox"/>

Во вкладке «**Расписание**» возможно задать время автоматического создания и удаления резервной копии. При указании времени автоматического создания возможно задать период (каждый день, раз в неделю, раз в две недели, раз в месяц), день недели и время в формате чч:мм создания резервной копии. При указании времени автоматического удаления возможно задать период (старше дня, старше недели, старше месяца, старше 3 месяцев, старше 6 месяцев, старше года) удаления резервной копии.

Редактирование шаблона резервной копии

Общие настройки **Расписание** Копирование

Автоматически создавать резервную копию

Период

раз в неделю

День недели

Пн Вт Ср Чт Пт Сб Вс

Время

13:00

Автоматически удалять резервные копии

Период

старше 3 месяцев

Сохранить Отмена

Во вкладке «**Копирование**» возможно задать съёмный носитель и настройки FTP сервера: IP адрес или доменное имя FTP сервера, порт FTP, относительный путь к папке, имя учетной записи и пароль. Данные настройки не взаимосвязаны с настройками FTP сервера во вкладке «Настройки». Таким образом, каждый шаблон может быть настроен на копирование на свой FTP сервер или флеш накопитель.

Редактирование шаблона резервной копии

Общие настройки Расписание **Копирование**

Копировать резервную копию на FTP сервер

Сервер FTP * Порт FTP *

Путь до папки с резервной копией на FTP сервере

Учетная запись Пароль

Автоматически копировать резервную копию на флеш накопитель

Выберите флеш накопитель

При необходимости шаблоны можно удалить или редактировать, выбрав необходимый шаблон и нажав на соответствующие кнопки.

Настройки

ИКС > Резервные копии > Настройки

Администратор 22

Резервные копии Шаблоны **Настройки**

Автоматически удалять ручные резервные копии

Только настройки Полная резервная копия Остальные резервные копии

старше месяца старше недели никогда

Автоматически копировать резервную копию на флеш накопитель

Выберите флеш накопитель

Kingston 16G

Копировать резервные копии на FTP сервер

Сервер FTP * Путь до папки с резервной копией на FTP сервере

Порт FTP

21

Учетная запись Пароль

Anonymous

Жесткий диск для хранения резервных копий *

Основной системный раздел Mirgor

Сохранить Обновить

Вкладка «**Настройки**». Помимо сохранения резервной копии на жесткий диск «ИКС» (блок «Жесткий диск для хранения резервных копий»), можно выбрать опцию сохранения на съемный носитель (блок «Автоматически копировать резервную копию на флеш накопитель») или удаленный FTP-сервер (блок «Копировать резервные копии на FTP сервер»), это позволит обезопасить данные резервных копий на случай разрушения жесткого диска. Во избежание переполнения жесткого диска данными (резервные копии статистики могут достигать довольно больших объемов) возможно настроить параметры автоматического удаления старых резервных копий, созданных **не** по шаблонам (блок «Автоматически удалять ручные резервные копии»), указав необходимый период.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:backup>

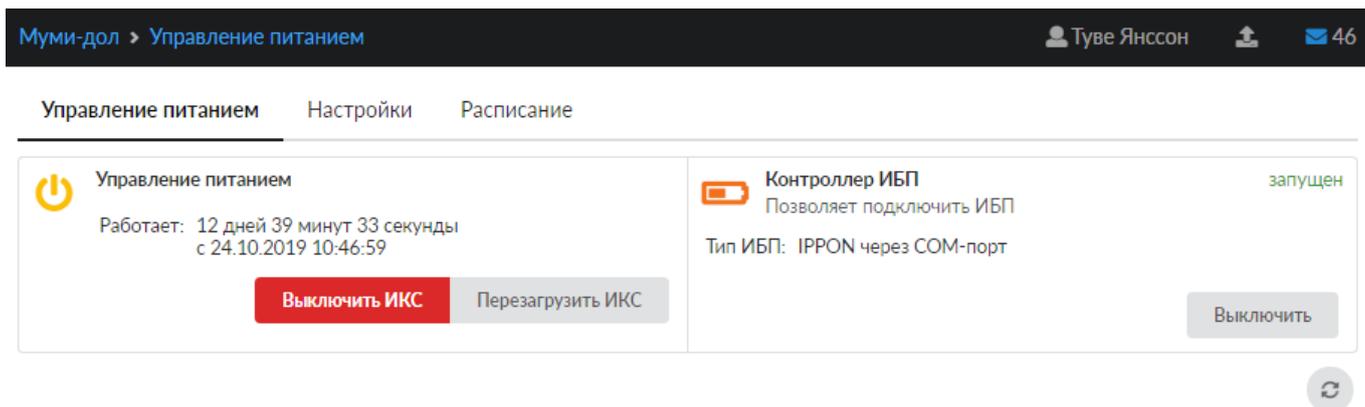
Last update: **2019/11/10 19:25**



Управление питанием

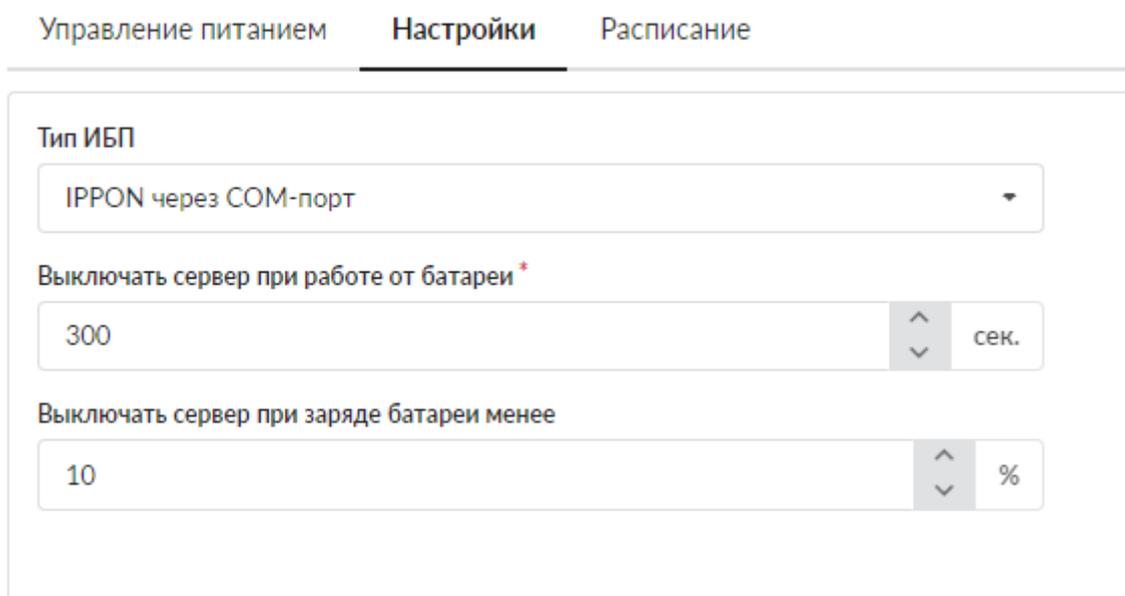
Модуль расположен в Меню – Обслуживание и имеет три вкладки: «Управлением питанием», «Настройки» и «Расписание». Данный модуль предназначен для настройки и управления источниками питания.

Управление питанием



На данной вкладке расположено два раздела: «Управление питанием» и «Контроллер ИБП». В первом отображается время работы «ИКС» от сети питания, а также кнопки «Выключить ИКС» и «Перезагрузить ИКС», нажав одну из них, произойдет соответствующее действие. Во втором блоке отображается информация о подключенном ИБП и кнопка «Включить/Выключить», отвечающая за включение/отключение контроллера взаимодействующего с ИБП.

Настройки



Вкладка позволяет задать настройки контроллеру для взаимодействия с источником бесперебойного питания (ИБП). Контроллер «ИКС» может работать с ИБП фирм IPPON и APC по COM-порту или по USB-порту. В качестве настроек возможно задать порог времени работы (в

секундах) от ИБП или порог остаточного заряда (в процентах) батареи. При достижении одного из параметров, «ИКС» перейдет в режим завершения работы и выключится.

Стоит отметить, для того чтобы «ИКС» автоматически включился при восстановлении электропитания, необходимо настроить BIOS материнской платы. (Опция «After power failure»: «Last State» или аналогичная.)

Расписание

Управление питанием Настройки **Расписание**

Перезагрузка

в указанные дату и время

в указанные дни и время

Выключение

в указанные дату и время

в указанные дни и время

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

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:power>

Last update: **2019/11/10 19:25**



ИКС > Жесткие диски Администратор 10

Добавить

Раздел	Имя	Название	Объем	Используется	Свободно	Статус
Раздел Mirror						
Раздел Stripe						
е жесткие диски						
<input type="checkbox"/> Основной системный раздел Mirror			15 Г	3.91 Г	10.6 Г	Ок
<input type="checkbox"/> Основной жесткий диск VMware Virtual disk 1.0	da0p4		15.19 Г			Ок
<input type="checkbox"/> Раздел Mirror Раздел 1 - mirror			3.75 Г	451 К	3.62 Г	
<input type="checkbox"/> Жесткий диск VMware Virtual disk 1.0	da1		4 Г			Ок
<input type="checkbox"/> Раздел Stripe Раздел 2 - stripe			15.5 Г	132 К	15 Г	
<input type="checkbox"/> Жесткий диск VMware Virtual disk 1.0	da2		16 Г			Ок

При перемещении жесткого диска в «**Раздел Mirror**», будет создан RAID 1. Для добавления в раздел второго и более диска, добавляемый диск должен быть такого же или большего размера, чем первый добавленный в раздел диск. Объемом всего раздела будет считаться объем первого (т.е. меньшего по размеру) добавленного диска.

Добавление раздела Mirror

Название *	Описание
<input type="text" value="Раздел 1"/>	<input type="text" value="mirror"/>

При перемещении жесткого диска в «**Раздел Stripe**», будет создан RAID 0. При добавлении диска в **раздел Stripe**, будет выдано предупреждение, что **вынуть диски из раздела возможно только при удалении всего раздела**. Ограничений по размеру добавляемых дисков нет.

Добавление раздела Stripe

Название *	Описание
<input type="text" value="Раздел 2"/>	<input type="text" value="stripe"/>

Важно! При перемещении жесткого диска в раздел, содержимое перемещаемого

диска будет отформатировано.

Разделы так же можно редактировать с помощью соответствующей кнопки на странице или с помощью двойного нажатия левой кнопки мыши по имени раздела. Для перемещения жестких дисков между разделами используется способ DnD (drag-and-drop). Минимальный размер жесткого диска 64 МБ.

Для каждого раздела в модуле «Файловый сервер» - «[Хранилище файлов](#)» в **Корневой папке** появится папка с именем, аналогичным имени созданного раздела. Эти папки можно выбирать при создании файловых ресурсов ([Веб](#), [FTP](#), [Сетевое окружение](#)).

Подключенные жесткие диски «ИКС» может использовать для своей работы. Например, возможно настроить хранение почтовых писем в выбранном разделе (Меню – Почта – Настройки – [вкладка «Настройки»](#) - поле «Жесткий диск для хранения почты»); или сохранение резервных копий «ИКС» (Меню – Обслуживание – Резервные копии - [вкладка «Настройки»](#) - поле «Жесткий диск для хранения резервных копий»).

Удаление разделов и дисков

Удалить диск из раздела можно перетащив диск в «**Неиспользуемые жесткие диски**» либо нажав кнопку «**Удалить**» (кроме раздела типа Stripe). Удалить разделы можно нажав кнопку «**Удалить**», при этом если удаляемый раздел выбран в Настойках [Почты](#) или [Резервных копий](#), будет выдана соответствующая ошибка.

Разделы «**Неиспользуемые жесткие диски**» и «**Основной раздел**», а также «**Основной жесткий диск**» в «Основном разделе», удалить нельзя.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:hdd>

Last update: **2019/11/10 19:25**



Время и дата

Модуль «Время и дата» расположен в Меню – Обслуживание. Данный модуль предназначен для работы со временем и датой в «ИКС», а также содержит следующие вкладки: «Время и дата», «Сервер времени», «Временные промежутки» и «Журнал».

Время и дата

ИКС > Время и дата > Время и дата Администратор   8

Время и дата Сервер времени Временные промежутки Журнал

Дата *  Время *

Временная зона

Сервера для синхронизации NTP-сервера

× × × ×

× × × ×

Автоматически создавать разрешающее правило для доступа к серверу времени

Доступ к NTP-серверу

Вкладка «Время и дата». На данной вкладке обязательными полями являются «**Дата**» и «**Время**». Если сервер времени выключен, то можно задать необходимые значения времени и даты. Поле «**Временная зона**» предназначено для указания текущей временной зоны. Поле «**Сервера для синхронизации NTP-сервера**» содержит предустановленные URL пулов NTP-серверов. В данное поле возможно указывать ip-адреса NTP-серверов или иных пулов. Встроенный NTP-сервер в «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 в межсетевом экране на доступ от локальных и DMZ сетей на порт **ntp (123)**.

Сервер времени

ИКС > [Время и дата](#) Администратор 8

[Время и дата](#) **Сервер времени** [Временные промежутки](#) [Журнал](#)

Сервер времени запущен
Отвечает за синхронизацию системного времени

Сервер синхронизации: hnapel.xs4all.nl
Уровень точности сервера: 2

[Выключить](#)

Журнал

11:17:13
basedate set to 2018-08-07
11:17:13

gps base set to 2018-08-12 (week 2014)
11:17:13

restrict default: KOD does nothing without LIMITED.
11:17:13

restrict ::: KOD does nothing without LIMITED.
11:17:13

switching logging to file /var/log/ntp.log
11:17:13

Отображает текущее состояние сервера времени (NTP-сервера «ИКС»). А именно, URL NTP-сервера с которым синхронизирован «ИКС» (0.0.0.0 означает, что сервера NTP не доступны), а также уровень точности данной синхронизации (1 – максимальная точность, 16 – сервера не доступны). Кнопка «**Выключить**»/«**Включить**» для останова или запуска сервера времени. Также на данной вкладке представлен журнал сервера времени за текущую дату.

Временные промежутки

ИКС > [Время и дата](#) > **Временные промежутки** Администратор 9

[Время и дата](#) [Сервер времени](#) **Временные промежутки** [Журнал](#)

[Добавить](#) [Удалить](#) [Редактировать](#)

Обеденное время
Временной промежуток

Время: Пн-Пт 12:00-13:00

[Удалить](#) [Редактировать](#)

Позволяет задать временные промежутки по дням недели и времени «с... по...». На данной вкладке отображаются созданные временные промежутки. Временные промежутки можно

добавлять, удалять и редактировать нажав на соответствующие кнопки. Созданные временные промежутки возможно будет применить в различных модулях «ИКС», где необходимо задавать время действия.

Название *
Новый временной промежуток

Дни недели *
 Пн Вт Ср Чт Пт Сб Вс

Время с * 12:00 до * 13:00

Добавить Отмена

При добавлении временного промежутка будет открыто новое диалоговое окно, в котором необходимо: задать **название**, указать **дни недели**, а так же **время действия** данного временного промежутка. Все поля являются обязательными.

Журнал

ИКС > Время и дата > Журнал

Администратор

Время и дата Сервер времени Временные промежутки Журнал

10.10.2019 - 10.10.2019 Сегодня Неделя Месяц Другой период

Экспорт Удалить логи Поиск...

ntpд 4.2.8p12-a (1): Starting
11:17:13

Command line: /usr/sbin/ntpd -p /var/run/ntpd.pid
11:17:13

proto: precision = 0.090 usec (-23)
11:17:13

basedate set to 2018-08-07
11:17:13

gps base set to 2018-08-12 (week 2014)
11:17:13

restrict default: KOD does nothing without LIMITED.
11:17:13

Стр 1 из 1

Показаны записи 1 - 8 из 8

Отображает сводка 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**».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:date>

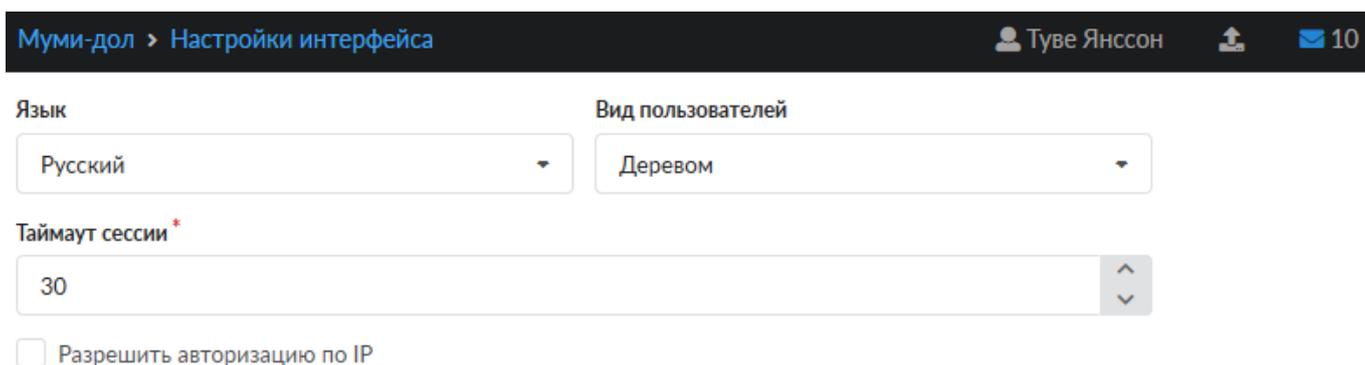
Last update: **2019/11/10 19:25**



Настройки интерфейса

Модуль «Настройки интерфейса» расположен в Меню – Обслуживание. Данный модуль предоставляет возможность настройки некоторых параметров web-интерфейса.

Общие настройки



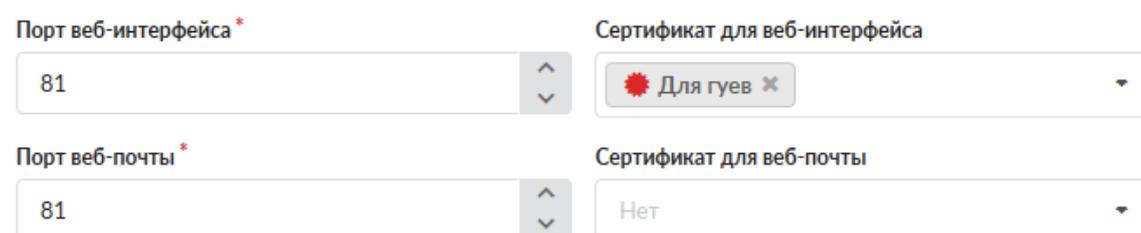
Поле «Язык» - предоставляет возможность выбора языка отображения web-интерфейса (русский или английский).

Поле «Вид пользователей» - позволяет задать вид отображения Пользователей в модуле «Пользователи». Отображение может быть представлено деревом или списком.

Поле «Таймаут сессии» - позволяет задать время таймаута. Таймаут сессии определяет время бездействия Пользователя «ИКС» в web-интерфейсе, по окончании которого Пользователь будет отключен (разлогинен) от web-интерфейса. Стоит отметить, что если web-интерфейс открыт на странице с динамическим содержимым, то таймаут сессии не наступит.

Флаг «Разрешать авторизацию по IP» - позволяет всем Пользователям, заведенным на «ИКС» с указанным IP-адресом, проходить авторизацию и аутентификацию без введения логина и пароля.

Порты и сертификаты



Поле «Порт веб-интерфейса» - позволяет задать порт, на котором работает web-интерфейс «ИКС». По умолчанию это 81 порт.

Поле «Сертификат для веб-интерфейса» - так как веб-интерфейс «ИКС» работает только по протоколу https, то для доступ к веб-интерфейсу необходимо иметь [сертификат](#). По умолчанию, «ИКС» создает само подписанный сертификат «Autogenerated GUI...». Так как сертификат является само подписанным, все интернет браузеры будут считать его не достоверным. Для того чтобы зайти в веб-интерфейс «ИКС», необходимо добавить данный сертификат в интернет браузер.

Поле «Порт веб-почты» - позволяет задать порт, на котором работает веб-интерфейс почты «ИКС» (Roundcube). По умолчанию это 81 порт, но для доступа к веб-интерфейсу почты «ИКС» необходимо ввести в адресной строке «/rc/», после указания порта. Или при авторизации в веб-интерфейсе «ИКС» перейти по ссылке «Веб-почта». При изменении номера порта по умолчанию, доступ к веб-интерфейсу почты станет в формате <ip-адрес «ИКС»>:<вновь заданный порт>. Стоит отметить, что при изменении порта по умолчанию необходимо чтобы был указан сертификат в поле «Сертификат для веб-почты», так как веб-интерфейс почты «ИКС» доступен по протоколу https. Если был задан 80 порт, то при обращении к веб-почте необходимо, либо указывать явный прокси в браузере, либо использовать [прозрачный прокси](#) в «ИКС», но в поле «Исключения для прозрачного прокси» указать IP-адрес «ИКС».

Поле «Сертификат для веб-почты» - аналогично полю «Сертификат для веб-интерфейса». Само подписанный сертификат имеет имя «Autogenerated MailServer...». Данное поле может быть не заполненным, если значение полей «Порт веб-интерфейса» и «Порт веб-почты» совпадают.

Ссылки в окне авторизации

Ссылки в окне авторизации

- | | |
|---|---|
| <input type="checkbox"/> Скрывать ссылку на веб-почту | <input type="checkbox"/> Скрывать ссылку на Captive portal |
| <input type="checkbox"/> Скрывать ссылку на Iphone | <input type="checkbox"/> Скрывать ссылку на программу авторизации |

Флаг «Скрывать ссылку на веб-почту в окне авторизации» - позволяет скрывать ссылку «Веб-почта» в окне авторизации «ИКС».

Флаг «Скрывать ссылку на программу авторизации в окне авторизации» - позволяет скрывать ссылку «Программа авторизации», по которой можно скачать программу xauth, в окне авторизации «ИКС».

Для того, чтобы внесенные изменения применились необходимо нажать кнопку «Сохранить».

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:guisetup>

Last update: **2019/11/10 19:25**



Мониторинг

Модуль «Мониторинг» находится в Меню «Обслуживание». Данный модуль предназначен для просмотра статистики 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.

Модуль «Мониторинг» имеет три вкладки: «Графики», «Мониторинг состояния системы» и «Журнал».

Графики

The screenshot shows the 'Мониторинг' (Monitoring) interface. At the top, there is a breadcrumb 'Муми-дол > Мониторинг' and user information 'Тыве Янссон' with a notification icon showing '10'. Below the breadcrumb are three tabs: 'Графики' (selected), 'Мониторинг состояния системы', and 'Журнал'. Under the 'Графики' tab, there are three buttons: 'Добавить' (highlighted in blue), 'Удалить', and 'Редактировать', along with a refresh icon. A list of monitoring metrics is shown on the left, with 'Загрузка дисков' (Disk Load) selected. The main area displays a graph titled 'Загрузка дисков за последний час' (Disk Load for the last hour). The graph shows a red area chart of disk usage percentage over time from 14:30 to 15:20. Below the graph, statistics for 'da0' are provided: '61%' (current), 'макс: 61%' (max), 'сред: 12%' (avg), and 'мин: 4%' (min). A second graph title 'Загрузка дисков за последние 6 часов' is visible at the bottom of the chart area.

Вкладка «Графики». В левой части данной вкладки отображается список доступных показателей. На каждый из выбранных пунктов в правой части окна строится несколько графиков, различных по временному интервалу: за последний час, 6 часов, день, неделю, и т.д.

При необходимости вы можете добавить собственные графики для проверки доступности указанных хостов, нажав кнопку «Добавить» → «Пинг».

Мониторинг состояния системы

 **Мониторинг состояния системы** запущен
Строит графики состояния системы

Выключить

Журнал ↓↑ ↻

started
15:19:36

config loaded
15:19:36

Вкладка «Мониторинг состояния системы». На данной вкладке отображается состояние службы, кнопка «Выключить» (или «Включить» если служба выключена) и последние сообщения в журнале.

Журнал

Графики **Мониторинг состояния системы** **Журнал**

01.11.2019 - 30.11.2019 Сегодня Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи 🔍

↓↑

started
05.11.2019 15:43:13

config loaded
05.11.2019 15:43:13

started
15:19:36

Вкладка «Журнал». На данной вкладке находится сводка всех системных сообщений от службы. 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) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**»

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:graphs>

Last update: **2019/11/10 19:25**



Журнал и уведомления

Системный журнал

Системный журнал Настройки уведомлений Уведомления на почту Уведомления на Jabber Уведомления в Telegram Сл >

18.09.2019 - 18.09.2019 Сегодня Неделя Месяц Другой период ▾ ↻

↑ Экспорт Системный журнал ▾ Все сообщения ▾ Поиск... 🔍

↓ ↑

Тестовый период истекает через 7 дней
00:00:10

Пользователь Администратор вошел в систему с адреса 192.168.17.30
14:31:29

« < Стр 1 из 1 > » Показаны записи 1 - 2 из 2

В модуле «системный журнал» отображаются сообщения о действиях пользователей, изменениях в статусах сервисов и ошибках системы.

Сообщения можно фильтровать по категориям и дате. В случае необходимости отображения конкретного журнала одного из модулей, необходимо выбрать данный модуль из выпадающего списка. А также возможно указать дополнительный фильтр, если это возможно, по выбранному модулю.

Кроме того, можно фильтровать сообщения по содержанию. Для этого 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

Системный журнал **Настройки уведомлений** Уведомления на почту Уведомления на Jabber Уведомления в Telegram С >

Отправлять уведомления

Посылать уведомление

сразу

Уведомлять о всех событиях

Уведомлять о следующих событиях:

- События системы
- События сервисов
- Ошибки
- Другие события

Дублировать syslog сообщения

Сервер syslog

Порт

Вкладка «Настройки уведомлений» позволяет настроить уведомления о состоянии системы. Поставив флаг в поле «Отправлять уведомления» активируется меню настроек отправления уведомления. В поле «Посылать уведомления» можно указать период доставки сообщения. Также можно выбрать одно из двух полей «Уведомлять о всех событиях системы» или «Уведомлять о следующих событиях системы». Выбрав последнее поле можно настроить о каких именно событиях нужно получать уведомления. Можно выбрать поля: «События системы», «События сервисов», «Ошибки» и «Другие события». Поле «Дублировать syslog сообщения». Поставив флаг в это поле можно настроить получение логов на внешний ресурс, заполнив соответствующие поля «Сервер syslog» и «Порт». Для того, чтобы внесенные изменения применились нужно нажать кнопку «Сохранить» или «Обновить».

Уведомления на почту

Системный журнал Настройки уведомлений Уведомления на почту **Уведомления на Jabber** Уведомления в Telegram Служба уведомлений Журнал

Соединение установлено

Jabber-аккаунты для уведомлений

postmaster@test.ics ✕

Использовать Jabber-сервер ИКС

Учетная запись * Пароль *

poster@test.ics ✕

Использовать указанный Jabber-сервер

Jabber-сервер * Порт *

5222

Имя учетной записи * Пароль *

Ресурс

(icsJabberBot)

Использовать SSL

Не проверять SSL сертификат

Сохранить Обновить

Вкладка «Уведомления на почту» позволяет настроить отправку уведомлений посредством email. Она содержит следующие параметры:

«Почтовые ящики для уведомлений» - позволяет выбрать один или несколько ящиков, созданных в почтовом сервере ИКС либо прописать вручную внешние почтовые адреса.

Переключатель между почтовым сервером ИКС и внешним SMTP-сервером. В первом случае достаточно выбрать адрес отправителя из почтовых адресов, созданных в почтовом сервере ИКС. Во втором необходимо заполнить поля «SMTP-сервер», «Порт» и «Адрес отправителя».

Затем указываются логин и пароль для указанного ящика отправителя.

Флажок «Использовать SSL» используется для указания, что передача данных осуществляется по защищенному протоколу.

После сохранения настроек ИКС устанавливает проверочное соединение с введенными параметрами. Если соединение прошло успешно, то спустя несколько секунд статус подключения изменится на «Соединение установлено».

Уведомления на Jabber

Системный журнал Настройки уведомлений Уведомления на почту **Уведомления на Jabber** Уведомления в Telegram Служба уведомлений Журнал

Соединение установлено

Jabber-аккаунты для уведомлений

postmaster@test.ics ✕

Использовать Jabber-сервер ИКС

Учетная запись* Пароль*

poster@test.ics ✕

Использовать указанный Jabber-сервер

Jabber-сервер* Порт*

5222

Имя учетной записи* Пароль*

Ресурс

{ics.JabberBot}

Использовать SSL

Не проверять SSL сертификат

Сохранить Обновить

Вкладка «Уведомления на jabber» позволяет настроить отправку уведомлений посредством протокола XMPP (jabber). Она содержит следующие параметры:

«Jabber-аккаунты для уведомлений» - позволяет выбрать один или несколько аккаунтов, созданных в jabber-сервере ИКС либо прописать вручную внешние аккаунты.

Переключатель между jabber-сервером ИКС и внешним XMPP-сервером. В первом случае достаточно выбрать аккаунт отправителя из созданных в ИКС. Во втором необходимо заполнить поля «Jabber-сервер» и «Порт».

Затем указываются логин и пароль для указанного аккаунта.

Флаг «Использовать SSL» создает xmpps-подключение (в jabber-сервер ИКС не поддерживается).

Флаг «Не проверять SSL-сертификат» позволяет работать с самоподписанными сертификатами, используя starttls.

Если настройки верны, то после сохранения статус подключения изменится на «Соединение установлено».

Уведомления в Telegram

Системный журнал Настройки уведомлений Уведомления на почту Уведомления на Jabber **Уведомления в Telegram** Служба уведомлений Журнал

Соединение установлено

Telegram-аккаунты для уведомлений

Test ✕

Токен *

34344354388:Fdfkdklk5jcnvSlaklk56lkAAssdg

Использовать прокси

Сервер * Порт *

192.168.10.255 1080

Логин Пароль

admin

Сохранить Обновить

Вкладка «Уведомления в Telegram» позволяет настроить отправку уведомлений посредством предварительно созданного бота в мессенджере Telegram.

Чтобы создать нового бота, необходимо найти в мессенджере пользователя @BotFather, нажать Start и действовать далее согласно инструкции.

Вкладка содержит следующие параметры:

«Telegram-аккаунты для уведомлений» - позволяет прописать один или несколько пользовательских telegram-аккаунтов. Аккаунты указываются без начального символа @.

«Токен» - указывается токен, полученный в результате создания бота.

Флаг «Использовать прокси» позволяет указать внешний прокси-сервер для отправки сообщений. После включения флага необходимо заполнить поля «Сервер», «Порт», «Логин» и «Пароль».

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 telegram-аккаунтов.

Служба уведомлений

Вкладка содержит текущий статус службы. Если не создано ни одного агента отправки, служба находится в состоянии «не настроен». Также в этой вкладке находится кнопка «Выключить» (или «Включить» если служба выключена) и последние записи в журнале.

Журнал

Вкладка «Журнал» отображает сводку всех системных сообщений модуля «Служба уведомлений» с указанием даты и времени. Журнал разделен на страницы, кнопками

«вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы.

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».

Важно. Кнопка «Удалить логи» удаляет все логи, которые ведутся модулем «Служба уведомлений».

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:syslog>

Last update: **2019/11/10 19:25**



Техподдержка

Модуль «Техподдержка» находится в меню «Обслуживание». Данный модуль предназначен для предоставления доступа к ИКС сотруднику технической поддержки «А-реал Консалтинг». Это может быть полезно для получения помощи по настройке ИКС или устранения каких-либо возникающих проблем в тех случаях, когда ИКС находится за межсетевым экраном, который запрещает входящие соединения, или в серой сети за NAT-устройством (модем, роутер). Модуль «Техподдержка» имеет две вкладки: «Техподдержка» и «Настройки».

Подключение

Муми-дол > Техподдержка Туве Янссон 67

Техподдержка Журнал

Техподдержка запущен

Подключается к техподдержке по ssh

Подключен к dev.a-real.ru:20281 Выключить

Журнал ↓↑ ↻

Disconnected
00:00:01

Connecting to dev.a-real.ru:20281...
15:06:05

Connected
15:06:07

На первой вкладке модуля отображается состояние службы, кнопка «Выключить» (или «Включить» если служба выключена), а также последние сообщения журнала. После старта модуля, в сводке под названием службы отобразится порт подключения (обычно это порт 20xxx), для удаленного подключения необходимо сообщить номер порта сотруднику технической поддержки.

Журнал

Техподдержка **Журнал**

01.11.2019 - 30.11.2019 Сегодня Неделя Месяц Другой период ▾ ↻

↑ Экспорт Удалить логи Поиск... 🔍

↓↑

- Connecting to dev.a-real.ru:20311...
05.11.2019 10:37:43
- Connected
05.11.2019 10:37:43
- Disconnected
05.11.2019 10:40:17
- Connecting to dev.a-real.ru:20041...
05.11.2019 10:40:17

В закладке «Журнал» находится сводка всех системных сообщений от службы «Техподдержка». 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) - 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**», или удалить логи за определенный период времени с помощью кнопки «**Удалить логи**»

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:support>

Last update: **2019/11/10 19:25**



Обновления

Описание модуля

Модуль «Обновления» расположен в Меню «Обслуживание». В данном модуле отображается доступность и готовность к установке обновления «ИКС», также здесь отображается история версий «ИКС» (Changelog). Из неё возможно узнать, какие новые функции появились в «ИКС», какие недочеты были исправлены, а также об изменении функционирование модулей.

Муни-дол > Обновления Тыве Янссон  14 

 Доступно обновление 7.0.0.1911011838 (726.14М) Загрузить

История изменений

Версия 6.1.1 от 28 мая 2019

Сеть

-  В контент-фильтр добавлена обработка страниц, сжатых brotli
-  Устранена проблема доступа к интернету при мас авторизации пользователей
-  Исправлена проблема в работе правил прокси с группами SkyDNS категорий
-  Исправлено удалённое управление ИКС
-  Исправлена работа LetsEncrypt

Веб-интерфейс

Установка обновлений

Если для «ИКС» доступно обновление, то напротив Меню «Обслуживание» загорится красный кружок, а напротив модуля «Обновления» отобразиться номер доступной версии. В самом же модуле «Обновления» появится кнопка «Загрузить». При нажатии на кнопку «Загрузить» начнется загрузка обновления. Стоит отметить, что при не достаточном месте на жестком диске (менее двукратного объема обновления), кнопка «Загрузить» будет не доступна, а в статусе красным цветом будет написано «недостаточно места на диске». Процесс загрузки можно прекратить нажав, появившуюся кнопку «Остановить загрузку». После загрузки обновления появится кнопка «Установить», которую необходимо нажать для начала установки.

При установке обновления, сервер остановит все сетевые службы, затем выполнит установку новых компонентов и попросит выполнить перезагрузку.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=ics70:update>

Last update: **2019/11/10 19:25**



О программе

В модуле «о программе» отображается информация о текущей версии ИКС, информация о лицензии, а также контактная информация технической поддержки. Кроме того, в этом модуле всегда можно освежить воспоминания о лицензионном соглашении.

Муми-дол > О программе Туге Янссон   9

О программе Лицензионное соглашение



Версия: 7.0.0.1909201710
Серийный номер 4610-1BD4-208B-A596-B66B-9EF9-ACEA-B9E1

Тестовый период истекает через 1 день

В системе 9 пользователей

[Получить лицензию](#)

Техническая поддержка:
Телефон: 8 495 240-92-96
Сайт: <http://xserver.a-real.ru>

[Задать вопрос](#)

© 2003-2019 А-Реал Консалтинг
Программный комплекс Интернет Контроль Сервер и логотип Интернет Контроль Сервер являются торговыми марками ООО «А-Реал Консалтинг». Все права защищены.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: <https://doc.a-real.ru/doku.php?id=ics70:about>

Last update: **2019/11/10 19:25**



Активация сервера

Процесс активации системы осуществляется в модуле «О программе». Активацию сервера Вы можете осуществить после того, как купили лицензию по программу, либо планируете использовать ИКС Lite.

При каждой переустановке программы серийный номер и хэш генерируются заново!

В модуле «О программе» нажмите кнопку Активация и откроется окно с вашими персональными данными.

Активация

Имя
Туве Янссон

Организация
Муми-дол

ИНН *
123456789

E-mail *
writer@mumi.ru

Телефон *
777-777-77-77

Количество пользователей
9000

Неограниченное количество пользователей

Разрешить ИКС отправлять анонимную статистику

Для активации необходимо заполнить соответствующие поля. Если число пользователей указано 8 или меньше, то вы можете активировать версию ИКС Lite, нажав соответствующую кнопку.

Автоматическая активация

После приобретения лицензии на программу вы можете активировать систему в автоматическом режиме. Для этого после заполнения регистрационных данных нажмите кнопку «Активировать ИКС». Ваш запрос на активацию будет отправлен в отдел продаж. В течение 1-2 рабочих дней ИКС активируют, и вы на почту получите уведомление об успешной активации лицензии. После этого нужно будет нажать кнопку «Получить лицензию».

Ручная активация

В некоторых случаях (отсутствие интернет-подключения например) автоматическую активацию выполнить не удастся. В этом случае нужно использовать ручную активацию. В

модуле «О программе» будет доступна кнопка «Ручная активация», а также будет показан серийный номер установки. Нажав на кнопку «Ручная активация», вы увидите окно с двумя полями:

Ручная активация

Данные для активации

```
MI+300yTE1Zx3sIRVZJa4R0G0CvVvXJTF60vD599LvwQyF5qzR5tCZ7uNDYUCIb9QIKCKZWcH/b0eVWu9+G030  
xHxMDqcDetPkhWHZq4VSOBAkmE1OikCmdQPpwaY6kvKM6Dvr38Pfqpx448cPiREYpRkJell9ULvVMRhG  
XuSNWfDwE8K3rbbwvLruaSECrLU9XHSmyVV5YhPwTwM6fEQHNX1Xvw3Q8PNdiQNdyE3sD0/JONo+ESq  
PPIme3Xp/IPRP0KhYA8RbrYF1+QI2z6QCZ2KMmeT9gbB0AWVNtdIEqkrq3Sj8MFYT22A611iMysqLbv+ea7n  
X2c4mwZSvmP+gPgs3YA1M3A==
```

Лицензия *

Данные верхнего поля, а также серийный номер необходимо отправить вашему менеджеру с указанием названия организации, ИНН. В ответном сообщении вам будет отправлен лицензионный ключ. Содержимое этого ключа необходимо вставить в поле «Лицензия» и нажать «Сохранить».

После этого активация ИКС будет завершена.

Если вы приобретаете дополнительные лицензии, то после того, как ваш персональный менеджер сообщит о внесении нужного количества пользователей в реестр, нажмите кнопку «Переактивация», и лицензия будет обновлена.

From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:activation>

Last update: **2019/11/15 13:45**



Константы

Правила набора (Dialplan)

Начиная с версии 7.0.0 добавлена возможность корректировать/обрабатывать все called number в SIP Trunk провайдера. Так как некоторые SIP провайдеры отходят от стандартной записи (например, один провайдер присылал номер начинающийся с решетки), то такой номер не мог быть обработан правилами установленными на «ИКС». Соответственно для решения данной ситуации необходимо было добавить возможность использования символа решетки в начале номера.

Константа **asterisk.rulepattern** позволяет задать список возможных символов с которых начинается номер. По умолчанию, значение - **[0-9+*#]**.

Настройка кэша ZFS

Начиная с версии 6.1.0 изменено искусственное ограничение размера кэша ZFS (Zettabyte File System) в «ИКС». Теперь FreeBSD резервирует половину оперативной памяти для ядра и прикладных программ. Вторая половина оперативной памяти используется для кэша ZFS (ARC - Adaptive Replacement Cache).

ARC имеет очень низкий приоритет для запросов к памяти. Если приложение запрашивает оперативную память, а система не имеет достаточно свободной памяти, ядро системы уменьшает ARC, предоставляя приложению запрошенную им память. Процесс возвращения оперативной памяти кэша в систему не является мгновенным; он может занять несколько секунд и система начнёт “подтормаживать”.

Для возможности изменения параметров ARC, необходимо перейти в <IP-адрес ИКС>:<порт web-интерфейса>/#/const. В данной вкладке доступны следующие параметры настройки ARC:

- `vfs.zfs.arc_max`
- `vfs.zfs.arc_meta_limit`
- `vfs.zfs.arc_min`
- `vfs.zfs.prefetch_disable`

Параметр **vfs.zfs.arc_max** - позволяет установить максимальный размер ARC, указывается в мегабайтах. Пустое поле означает, что «ИКС» использует размер по умолчанию (<объём ОЗУ>/2). Если необходимо изменить размер ARC, то необходимо исходить из следующих рекомендаций:

- На каждый терабайт ПЗУ необходимо использовать 1 Гб ARC.
- Максимальный размер ARC не должен превышать <объём ОЗУ> - 1Гб.

Параметр **vfs.zfs.arc_meta_limit** - отвечает за размер части ARC, затраченной на хранение метаданных, указывается в мегабайтах. Пустое поле означает, что установлен размер по умолчанию (`vfs.zfs.arc_max / 4`) от первоначального определения `arc_max`. Если параметр `vfs.zfs.arc_max` был изменен, рекомендуется изменить данный параметр на новое значение `vfs.zfs.arc_max` деленное на 4. Стоит отметить, что если в «ИКС» создано много каталогов с большим количеством файлов (например: много почтовых ящиков с большим количеством

писем) и система “подтормаживает”, то рекомендуется установить параметр `vfs.zfs.arc_meta_limit` равным `vfs.zfs.arc_max/2`.

Параметр **`vfs.zfs.arc_min`** – отвечает за минимальный размер ARC, указывается в мегабайтах. Пустое поле означает, что установлен размер по умолчанию (`vfs.zfs.arc_meta_limit/2`). Если параметр `vfs.zfs.arc_max` был изменен, рекомендуется изменить данный параметр на новое значение равное `vfs.zfs.arc_meta_limit` деленное на 2.

В ZFS реализован механизм предварительной загрузки файлов и называется `zfetch`. Данный механизм анализирует шаблоны чтения файлов и пытается предсказать результаты следующего чтения для сокращения времени отклика приложений. В некоторых случаях, `zfetch` может интенсивно нагружать процессор и иметь предел масштабируемости. Для того чтобы отключит `zfetch`, необходимо указать значение параметра **`vfs.zfs.prefetch_disable`** равным 1.

Для вступления в силу произведенных настроек, необходимо произвести перезагрузку «ИКС».

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
<https://doc.a-real.ru/doku.php?id=ics70:const>

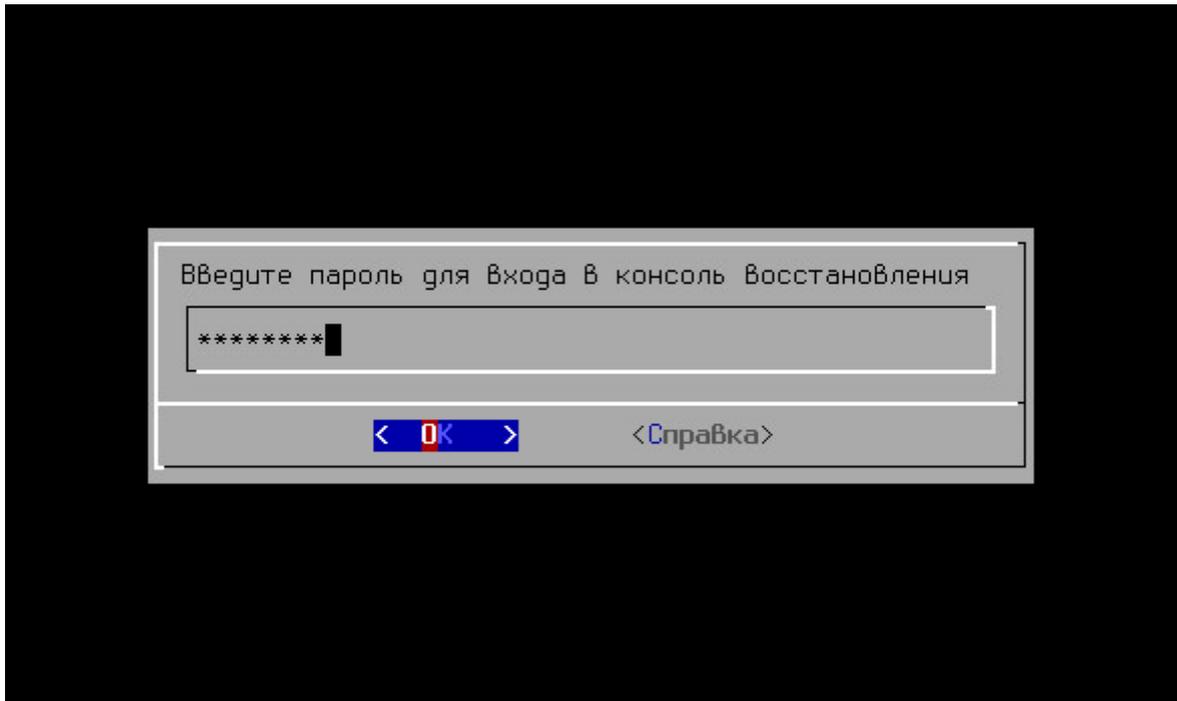
Last update: **2019/11/10 19:25**



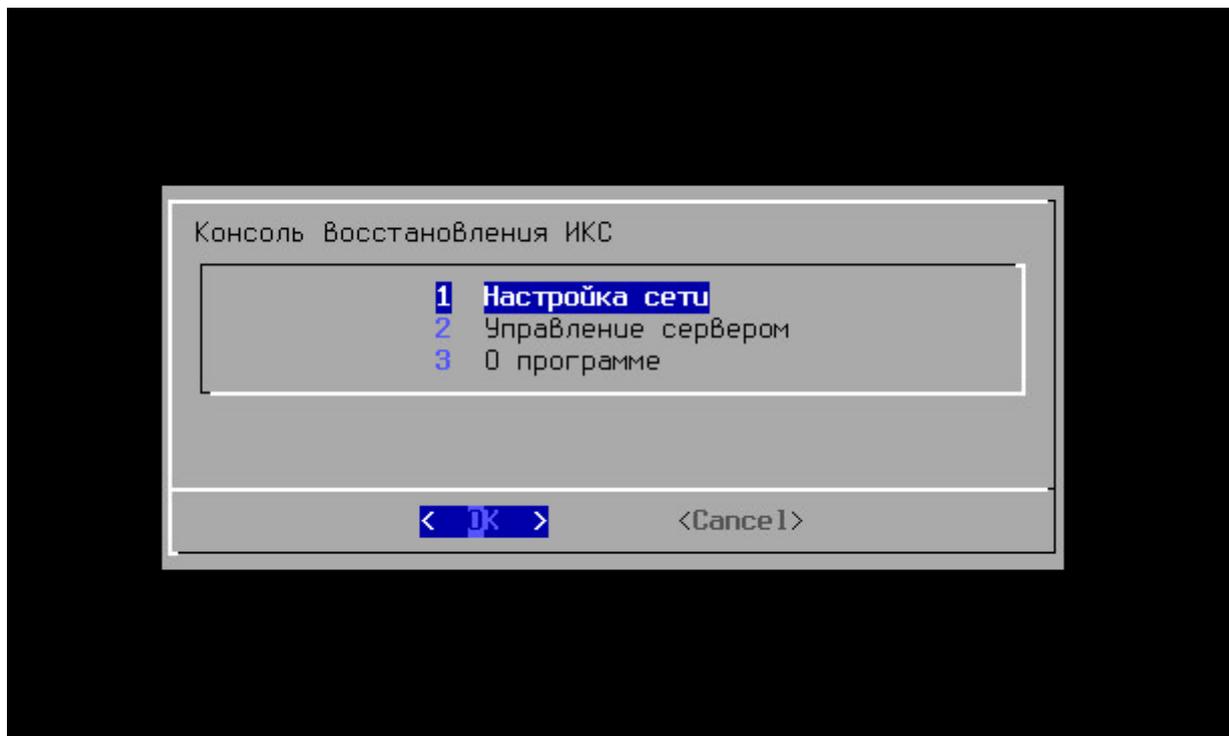
Консоль восстановления

Консоль восстановления - это служебный интерфейс ИКС, работающий в текстовом режиме. Для того, чтобы воспользоваться средствами консоли существуют два способа:

- подключите к ИКС монитор и клавиатуру
- воспользуйтесь любым ssh-клиентом (например Putty) и подключитесь на 22 порт ИКС (в этом случае в разделе [Межсетевой экран](#) → Настройки должен быть разрешен доступ по SSH с хоста, с которого производится подключение), введите логин **recshell**, пароль **recovery** (по умолчанию)

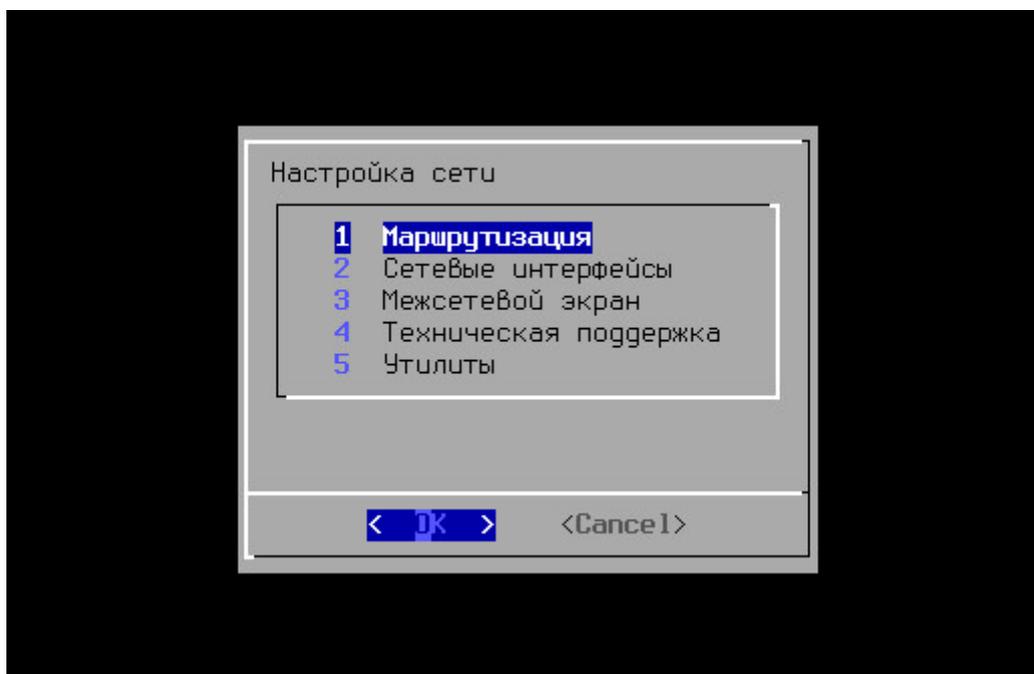


Вы увидите предложение ввести пароль. По умолчанию пароль **recovery**, вы можете изменить его в настройках консоли.



Настройка сети

Раздел консоли «Настройка сети» содержит следующие пункты меню:



- **Маршрутизация.** Вы можете просмотреть текущую таблицу маршрутизации, удалить какой-либо из маршрутов либо добавить новый.
- **Сетевые интерфейсы.** Проверка и корректировка сетевых интерфейсов ИКС. Вы можете 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.
- **Межсетевой экран.** В случае, если ИКС по каким-либо причинам блокирует доступ к веб-

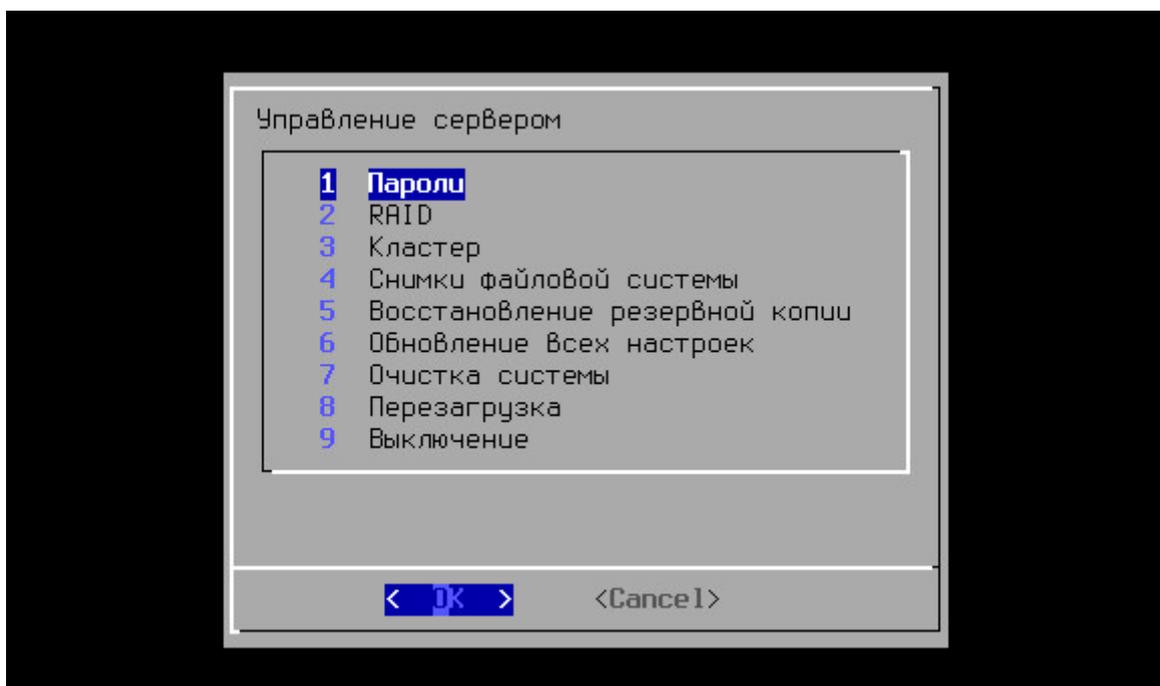
интерфейсу, вы можете временно отключить межсетевой экран до устранения причины блокировки. Помните, что вместе с ним отключается и сервис NAT, то есть пропадет доступ во внешнюю сеть у пользователей ИКС.

- **Техническая поддержка.** Позволяет запустить службу технической поддержки в случае возникновения неисправностей.
- **Утилиты (Ping и Tracе).** Позволяют проверить доступность локального или удаленного хоста.

Важно: данный раздел консоли восстановления является вспомогательным инструментом для диагностики неисправностей ИКС. Все изменения, произведенные в нем, будут сброшены при любом изменении в веб-интерфейсе ИКС или после перезагрузки.

Управление сервером

Раздел консоли «Управление сервером» содержит следующие пункты меню:



- **Пароли.** Смена пароля на аккаунт администратора и на вход в консоль восстановления. **Внимание! Будьте осторожны при смене пароля консоли восстановления по умолчанию. Если вы его забудете, восстановить его без удаленного вмешательства службы технической поддержки будет невозможно!**
- **RAID.** Добавление дисков в зеркальный массив.
- **Снимки файловой системы.** Позволяет создать снимок текущего состояния файловой системы и откатиться на него при необходимости.
- **Восстановление резервной копии.** Открывает список созданных ранее резервных копий и позволяет восстановить одну из них.
- **Обновление всех настроек.** Обновление конфигурации ИКС.
- **Очистка системы.** Позволяет очистить диск от системных логов, статистики, обновлений и резервных копий.
- **Перезагрузка.**

- **Выключение.**

О программе

Версия: 7.0.0.1910231218
Серийный номер: D135-453F-3F44-CD5E-F311-1B5C-1C67-8168

Тестовый период истекает через 22 дня
В системе 13 пользователей

Техническая поддержка:
Телефон: 8 495 240-92-96
Сайт: <http://xserver.a-real.ru>

© 2003-2019 А-Реал Консалтинг
Программный комплекс Интернет Контроль Сервер и логотип Интернет Контроль Сервер являются торговыми марками ООО «А-Реал Консалтинг». Все права защищены.



From:
<https://doc.a-real.ru/> - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=ics70:recovery_console

Last update: **2019/11/10 19:25**

