|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ |
|  | Генеральный директор |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.И. Баранов |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г. |

**Менеджер сервера**

программного комплекса

«Омега К100»

Руководство системного программиста

ЛИСТ УТВЕРЖДЕНИЯ

АСТФ.468367.004 - ЛУ

|  |  |
| --- | --- |
| *Подп. и дата* |  |
| *Инв. № дубл.* |  |
| *Взам. Инв №* |  |
| *Подп. и дата* |  |
| *Инв. № подл.* |  |

|  |  |
| --- | --- |
|  | Руководитель подразделения  А.С. Глазунов  Руководитель разработки  А.Н. Зюзин  Ответственный исполнитель  Р. Н. Ермаков |
| |  |  | | --- | --- | | *Подп. и дата* |  | | *Инв. № дубл.* |  | | *Взам. Инв №* |  | | *Подп. и дата* |  | | *Инв. № подл.* |  | |

2021

УТВЕРЖДЕН

АСТФ.468367.004-ЛУ

**Менеджер сервера**

программного комплекса

«Омега К100»

Руководство системного программиста

АСТФ.468367.004

|  |  |
| --- | --- |
| *Подп. и дата* |  |
| *Инв. № дубл.* |  |
| *Взам. Инв №* |  |
| *Подп. и дата* |  |
| *Инв. № подл.* |  |

Листов 66

2021

Аннотация

Настоящий документ является руководством системного программиста – администратора программы «Менеджер сервера» АСТФ.468367.004 (далее – программа или менеджер сервера), являющейся частью программного комплекса «Сервер системы «Омега К100», входящего в состав системы радиосвязи ОМЕГА реального времени (АСТФ.464514.004), разработанной группой компаний «АСТРАКОМ».

Руководство системного программиста (АСТФ.468367.004) содержит сведения для проверки, обеспечения функционирования и настройки системы на условия конкретного применения.

Структурно документ состоит из шести разделов.

В первом разделе указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих её работу, а также требования к персоналу.

Во втором разделе приведены сведения о структуре программы и её составных частях.

В третьем разделе приведено описание действий по настройке программы для условий конкретного применения.

В четвертом разделе приведено описание способов проверки, позволяющих дать общее заключение о работоспособности программы (контрольные примеры, методы прогона, результаты).

В пятом разделе указаны дополнительные возможности программы.

В шестом разделе указаны тексты сообщений, выдаваемых в ходе выполнения настройки, проверки программы, а также в ходе работы программы, описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

Содержание

[1. Общие сведения о программе 5](#_Toc72413747)

[1.1. Наименование программы 5](#_Toc72413748)

[1.2. Назначение программы 5](#_Toc72413749)

[1.3. Функции программы 5](#_Toc72413750)

[1.4. Системные требования 6](#_Toc72413751)

[1.5. Требования к персоналу (системному программисту) 6](#_Toc72413752)

[2. Структура программы 8](#_Toc72413753)

[2.1. Сведения о структуре 8](#_Toc72413754)

[2.2. Сведения о составных частях программы 9](#_Toc72413755)

[2.3. Сведения о связях с другими программами 9](#_Toc72413756)

[2.4. Особенности программы 9](#_Toc72413757)

[2.4.1. Приоритеты вызовов 9](#_Toc72413758)

[3. Настройка программы 11](#_Toc72413759)

[3.1. Настройка сети и системы безопасности для обеспечения устойчивой работы 11](#_Toc72413760)

[3.2. Установка программы «Менеджер сервера» 11](#_Toc72413761)

[3.3. Конфигурация запуска сервера 12](#_Toc72413762)

[3.4. Настройка учетных записей диспетчеров 16](#_Toc72413763)

[3.5. Настройки клиентского приложения 19](#_Toc72413764)

[3.5.1. Настройки интерфейса 19](#_Toc72413765)

[3.5.2. Определение настроек по умолчанию 21](#_Toc72413766)

[3.6. Сети серверов ОМЕГА 22](#_Toc72413767)

[3.6.1. Абоненты сети 24](#_Toc72413768)

[3.6.2. Группы сети 26](#_Toc72413769)

[3.6.3. Диспетчеры сети 27](#_Toc72413770)

[3.6.4. Устройства сети 28](#_Toc72413771)

[3.6.5. Статусы устройств 28](#_Toc72413772)

[3.6.6. Аварийные профили 29](#_Toc72413773)

[3.6.7. Разрешения абонентов 30](#_Toc72413774)

[3.6.8. Разрешения диспетчера 32](#_Toc72413775)

[3.6.9. Параметры режима присутствия 32](#_Toc72413776)

[3.7. Журнал событий 33](#_Toc72413777)

[3.8. Лицензии 34](#_Toc72413778)

[3.8.1. Идентификатор оборудования 35](#_Toc72413779)

[3.8.2. Активация лицензионного ключевого файла 36](#_Toc72413780)

[3.9. Настройка DMR 37](#_Toc72413781)

[3.9.1. Excera AIS-DMR 38](#_Toc72413782)

[3.9.2. Hytera DMR 41](#_Toc72413783)

[3.9.3. Kirisun DMR 48](#_Toc72413784)

[3.9.4. Групповая ассоциация 55](#_Toc72413785)

[3.9.5. Назначение DMR-идентификатора (Virtual Radio ID) 55](#_Toc72413786)

[3.9.6. Подписчики DMR 56](#_Toc72413787)

[3.10. Порты, используемые сервером ОМЕГА 56](#_Toc72413788)

[3.10.1. Серверные порты 56](#_Toc72413789)

[3.10.2. Сетевые порты 57](#_Toc72413790)

[4. Проверка программы 59](#_Toc72413791)

[4.1. Настройка сети для проведения тестирования 59](#_Toc72413792)

[4.2. Описание способов проверки 59](#_Toc72413793)

[4.3. Проверка целостности 59](#_Toc72413794)

[4.4. Методы прогона 60](#_Toc72413795)

[5. Дополнительные возможности 61](#_Toc72413796)

[5.1. Резервирование сервера 61](#_Toc72413797)

[5.1.1. Особенности резервирования 61](#_Toc72413798)

[5.1.2. Настройки резервирования 61](#_Toc72413799)

[5.1.3. Настройка режима Резервный сервер 62](#_Toc72413800)

[5.1.4. Настройка режима Основной 62](#_Toc72413801)

[5.2. Удаленный мониторинг 63](#_Toc72413802)

[5.3. Шифрование трафика 64](#_Toc72413803)

[5.4. Телефонная связь 64](#_Toc72413804)

[5.5. Поддержка от разработчика 66](#_Toc72413805)

[6. Сообщения системному программисту 67](#_Toc72413806)

[Перечень сокращений 68](#_Toc72413807)

[Лист регистрации изменений 69](#_Toc72413808)

# Общие сведения о программе

## Наименование программы

Полное наименование программного изделия: «Менеджер сервера «Омега К100» программного сервера (АСТФ.468367.004).

Краткое наименование программного изделия: «Менеджер сервера».

## Назначение программы

Сервер системы, входящий в состав системы радиосвязи ОМЕГА реального времени (АСТФ.468367.004) построен на основе технологии PoC.

Технология PoC реализует клиент-серверную архитектуру. В состав системы входят следующие элементы: основной и резервный сервера PoC, диспетчерское автоматизированное рабочее место PoC, терминальные устройства PoC (смартфоны, планшеты и т.д.), устройства сопряжения (шлюзы) PoC. Транспортом для системы оперативной радиосвязи на базе технологии PoC является выделенная или публичная сеть 3G/4G, а также Wi-Fi сегменты.

Сервер PoC состоит из оборудования (аппаратной части) сервера и специализированного программного обеспечения сервера. Сервер PoC управляет работой абонентов и взаимодействует с устройствами сопряжения PoC через программное приложение «Менеджер сервера».

На базе Сервера PoC реализованы функции Администратора сети и Диспетчера. Программное приложение «Менеджер сервера» отвечает за функции Администратора, а именно:

* Администратор сети PoC прописывает абонентов, имеющих доступ в систему и формирует группы абонентов (Каналы в системе PoC).
* Администратор отвечает за необходимые обновления информации об абонентах системы.

## Функции программы

Программа «Менеджер сервера» реализует следующие функции:

* регистрации абонентов,
* коммутации вызовов,
* записи переговоров,
* предоставляет возможности GPS-отслеживания для определения местоположения участников связи.
* предоставляет возможности удаленного мониторинга, позволяя захватывать голос и видео с клиентских устройств, отображать их в диспетчерской консоли и записывать на сервере;
* готовит для диспетчера обновления клиентских приложений;
* предоставляет возможности создать резервный сервер, который может использоваться в случае сбоя или чрезмерного трафика на основном сервере.

## Системные требования

Системные требования программы «Менеджер сервера»:

* процессор: **CPU Core i5**;
* ОЗУ: RAM 8 ГБ;
* жесткий диск: **HDD 500 ГБ**;
* ОС: ASTRA Linux 3.2.0 и выше.

СУБД PostgreSQL необходим для хранения всех данных сервера и входит в установочный пакет программы.

Требования к сетевой пропускной способности представлены в таблице 1.

Таблица 1 – Требования к пропускной способности сети

|  |  |
| --- | --- |
| Тип данных | Ширина канала, кбит/с |
| Голосовые вызовы PTT: |  |
| Узкополосный (8 кГц) | 16 |
| Широкополосный (16 кГц) | 24 |
| Сверхширокополосный (24 кГц) | 32 |
| Полный диапазон (Full Band) (48 кГц) | 56 |
| Видео звонки PTT | 512 |

## Требования к персоналу (системному программисту)

Системный программист должен иметь минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

* задача поддержания работоспособности технических средств;
* задача установки (инсталляции) и поддержания работоспособности общего программного обеспечения;
* задача установки (инсталляции) и поддержания работоспособности системы радиосвязи ОМЕГА.

# Структура программы

## Сведения о структуре

Состав системы радиосвязи ОМЕГА (АСТФ.464514.004), управляемой сервером «Омега К100» (рис. 1) состоит из:

1. сервера программного комплекса «ОМЕГА К100» (АСТФ.468367.004);
2. диспетчерской консоли со специализированным программным обеспечением «ОМЕГА К400» (АСТФ.468369.004);
3. технологических шлюзов для коммутации сервера PoC с классическими системами профессиональной радиосвязи – концентраторами «ОМЕГА К500» (АСТФ.468354.004);
4. абонентского оборудования (терминалы, клиентские приложения «ОМЕГА К600Т» (АСТФ.464514.006))

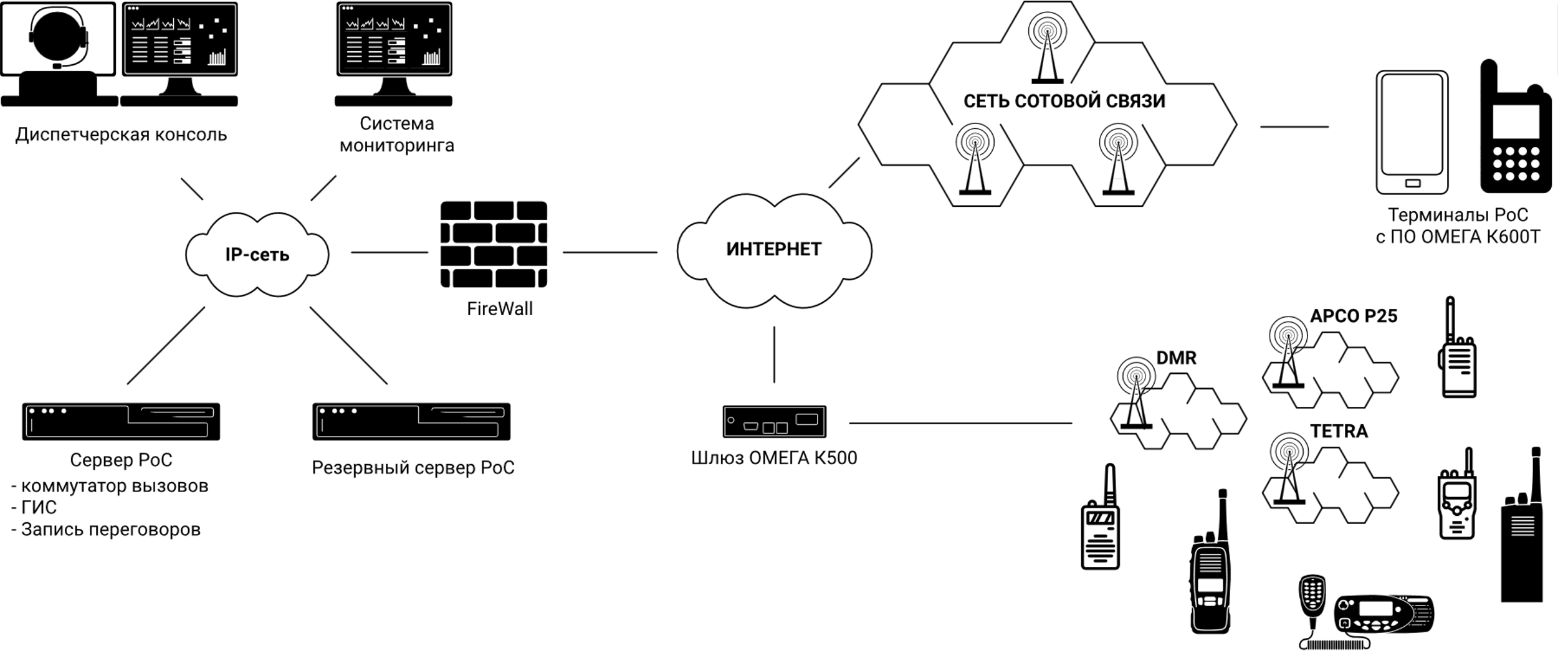


Рисунок 1 – Структура системы радиосвязи ОМЕГА

Сервер системы, входящий в состав системы радиосвязи ОМЕГА посредством приложения «Менеджер сервера «Омега К100»», взаимодействует со всеми структурами системы радиосвязи ОМЕГА по схеме, представленной на рисунке 2.

Специализированное программное обеспечение сервера – представляет собой совокупность баз данных (абонентов и настроек), прикладных сервисов и интерфейса управления. Основной и резервный Сервер реализует 100% аппаратное и программное резервирование по схеме 1+1.

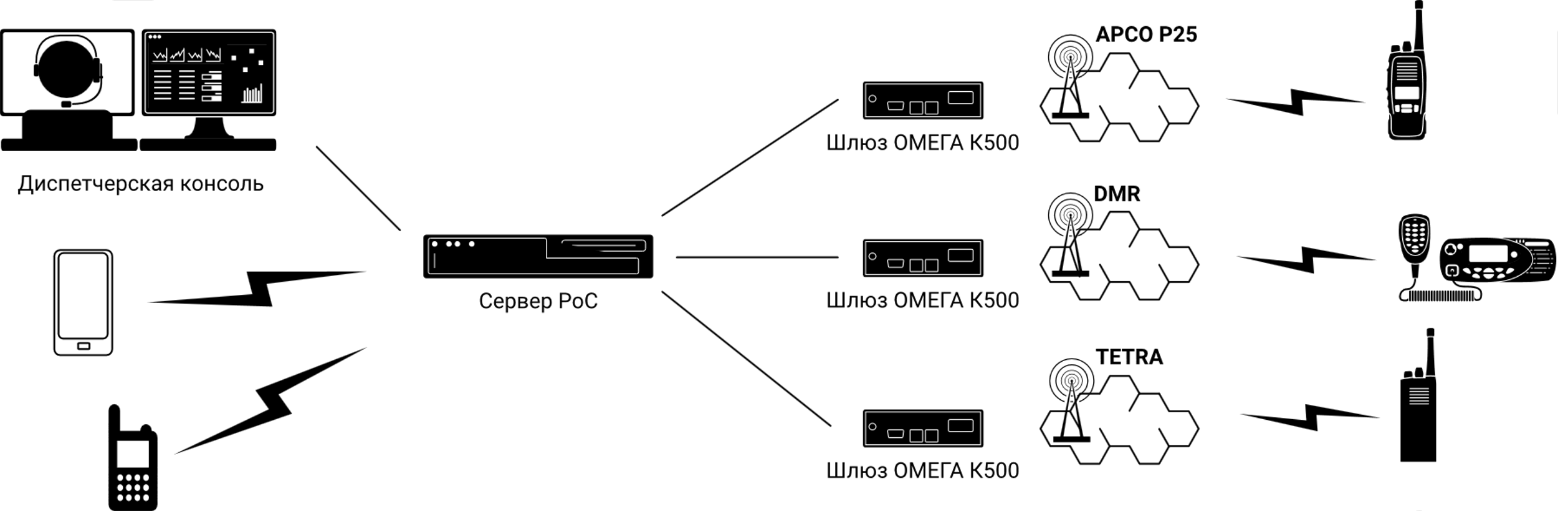


Рисунок 2 – Схема передачи сигналов между абонентами

## Сведения о составных частях программы

Пакет программы состоит из следующих основных компонентов:

* программа «Менеджер сервера «Омега К100»»;
* СУБД PostgreSQL.

## Сведения о связях с другими программами

Настройка учетных записей диспетчеров из менеджера сервера описана в подразделах 3.4, 3.6.3, 3.6.8.

Настройка клиентского приложения из менеджера сервера описана в подразделах 3.5, 3.6.1, 3.6.7. Установленные настройки отражены в клиентском приложении в том числе в файле Wfinit.cfg;

## Особенности программы

### Приоритеты вызовов

Мобильный клиент системы радиосвязи ОМЕГА - ОМЕГА К600Т (АСТФ.464514.006) может передавать или принимать только один вызов за раз. По этой причине все типы вызовов имеют приоритет, как указано в таблице 2.

Таблица 2 – Приоритеты в системе ОМЕГА

| Тип вызова | Описание |
| --- | --- |
| Экстренные вызовы | Видео или голосовые вызовы PTT в группы экстренной помощи. Вызов службы экстренной помощи – это вызовы с наивысшим приоритетом. Звонок в группы экстренной помощи останавливает все остальные типы вызовов. |
| Голосовые и видеовызовы | Обычный вызов PTT не может прерывать экстренные вызовы. Частные и групповые вызовы PTT имеют равный приоритет. |

Групповой приоритет имеет смысл только в рамках обычных групповых вызовов. Текущий групповой вызов останавливается и подключается новый групповой вызов, если новая группа имеет более высокий приоритет.

Приоритет абонента имеет смысл только в рамках текущего звонка. Абонент с более высоким приоритетом может прервать текущую передачу и начать разговор в рамках того же разговора.

# Настройка программы

Перед установкой программы необходимо убедиться в актуальности дистрибутива.

## Настройка сети и системы безопасности для обеспечения устойчивой работы

Серверный компьютер должен быть подключен к сети по кабелю, но не по Wi-Fi. Соединение Wi-Fi подходит для временного тестирования, но не для постоянного использования.

Серверный компьютер должен иметь фиксированный IP-адрес.

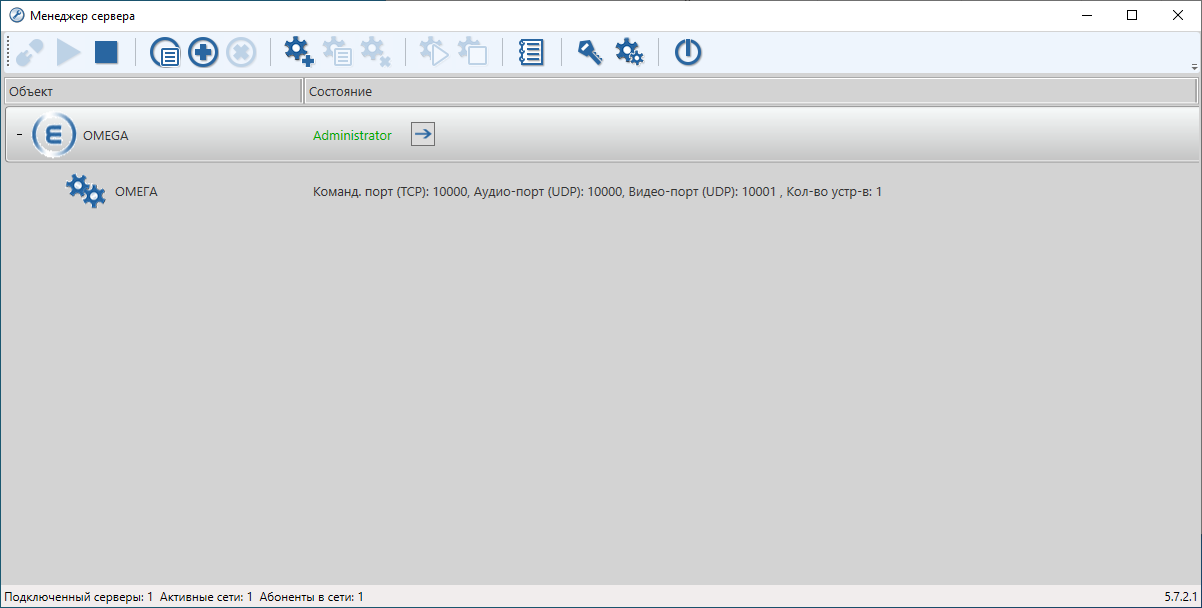
Фиксированный IP-адрес WAN необходимо получить у интернет-провайдера. Этот IP-адрес будет использоваться для подключения клиента системы ОМЕГА через Интернет. Динамический IP-адрес WAN подходит для тестов, но в реальной работе изменение IP-адреса на маршрутизаторе не позволит произвести подключение всех клиентов.

Помимо антивирусного программного обеспечения и брандмауэра, порты могут быть заблокированы сетевым оборудованием. В простых маршрутизаторах Wi-Fi брандмауэр обычно отключен по умолчанию, но в более сложных корпоративных сетях такие настройки безопасности могут применяться администраторами сети.

## Установка программы «Менеджер сервера»

Запустите установочный пакет. Обязательно соблюдайте системные требования (см. подраздел 1.4).

Программа «Менеджер сервера» реализован как сервис Linux. Когда установка будет завершена, значок ASTRACOM Server Manager станет доступен на рабочем столе для запуска утилиты настройки (рис. 3).

Рисунок 3 – Окно Менеджер сервера

По умолчанию Менеджер сервера отображает запись локального сервера, установленного на ПК. Также можно подключать / отключать удаленные серверы (для этой цели используйте кнопки Подключиться к серверу  и Отключиться от сервера ).

Для запуска / остановки локального сервера используйте кнопки Запустить локальный сервер  и Остановить локальный сервер  соответственно.

**Примечание**. Удаленные серверы не могут быть запущены / остановлены из программы «Менеджер сервера».

Чтобы изменить настройки сервера, нажмите кнопку Настройки сервера  (см. подраздел 3.4 – 3.5.3).

Чтобы настроить конфигурацию запуска сервера, нажмите кнопку Начальная конфигурация сервера  (см. подраздел 3.3).

## Конфигурация запуска сервера

Первоначальная конфигурация запуска сервера осуществляется через диалоговое окно Начальная конфигурация сервера (рис. 4, 5, 6) (запускается кнопкой Начальная конфигурация сервера  в окне Менеджер сервера – рис. 3).

**Примечание**. Изменение конфигурации запуска доступно только для локального сервера. Её нельзя изменить для серверов, подключенных удаленно.

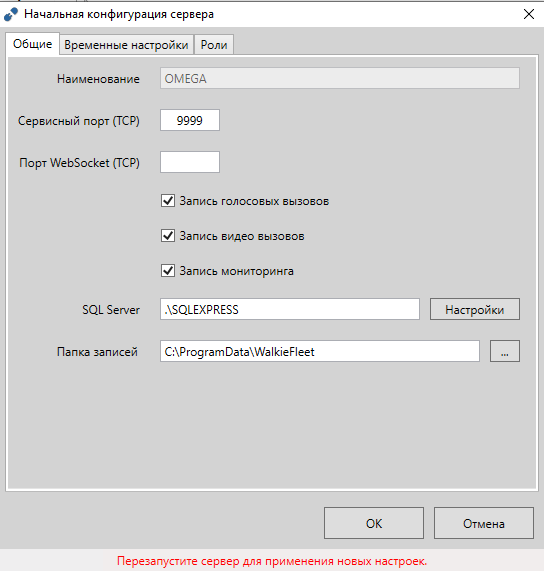


Рисунок 4 – Вкладка Общие окна настройки конфигурации сервера

В поле Сервисный порт (TCP) (рис. 4) задайте TCP-порт, используемый менеджером сервера для подключения к серверу.

В поле Порт WebSocket (TCP) (рис. 4) задайте порт TCP, используемый сторонними приложениями для подключения через API с учетной записью диспетчера.

В поле SQL Server (рис. 4) задайте путь с экземпляром SQL Server, на котором будут храниться данные сервера. По умолчанию указана ссылка на экземпляр PostgreSQL, установленный вместе с программой.

В поле Папка записей (рис. 4) задайте путь к папке, где будут храниться записи голосовых вызовов и видеозвонков.

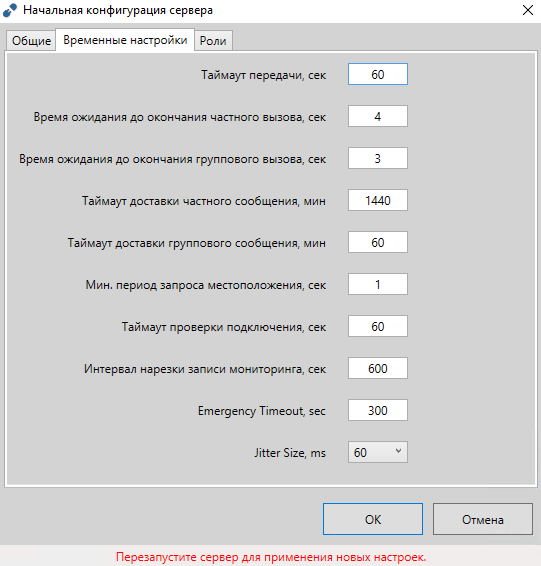


Рисунок 5 – Вкладка Временные настройки окна настройки конфигурации сервера

В поле Таймаут передачи, сек (рис. 5) задайте тайм-аут передачи в секундах. Сервер автоматически останавливает вызов, если непрерывная односторонняя передача по вызову превышает тайм-аут передачи.

В поле Время ожидания до окончания частного вызова, сек (рис. 5) задайте время ожидания частного вызова в секундах – это время ответа на частный вызов в рамках разговора после того, как вызывающая сторона отпустила PTT.

В поле Время ожидания до окончания группового вызова, сек (рис. 5) задайте время ожидания группового вызова в секундах – это время ответа на групповой вызов в рамках разговора после того, как вызывающая сторона отпустила PTT.

В поле Таймаут доставки частного сообщения, мин (рис. 5) задайте тайм-аут доставки частного сообщения в минутах – это время для продолжения доставки личного сообщения адресату.

В поле Таймаут доставки группового сообщения, мин (рис. 5) задайте тайм-аут доставки группового сообщения в минутах – это время для продолжения доставки группового сообщения членам группы.

В поле Мин. период запроса местоположения, сек (рис. 5) задайте минимально возможное время опроса для периодического обновления местоположения в секундах.

В поле Таймаут проверки подключения, сек (рис. 5) задайте период проверки доступности подключения к серверу в секундах.

В поле Интервал нарезки записи мониторинга, сек (рис. 5) задайте интервал нарезки записи мониторинга в секундах (см. подраздел 5.2). Сеанс мониторинга сохраняется набором из нескольких файлов. Интервал срезов мониторинга – это максимальная продолжительность записи для сохранения в одном файле.

В поле Emergency Timeout (рис. 5) задайте временной интервал подачи аварийного сигнала в секундах в случае, когда ни один из получателей аварийного сигнала не подтверждает аварийную ситуацию.

В поле Jitter size (рис. 5) задайте фазовое дрожание цифрового сигнала голосового потока на принимающем устройстве в миллисекундах. В умеренных сетевых условиях более высокий значение этой величины делает воспроизведение голоса более плавным, но добавляет дополнительную задержку в разговоре.

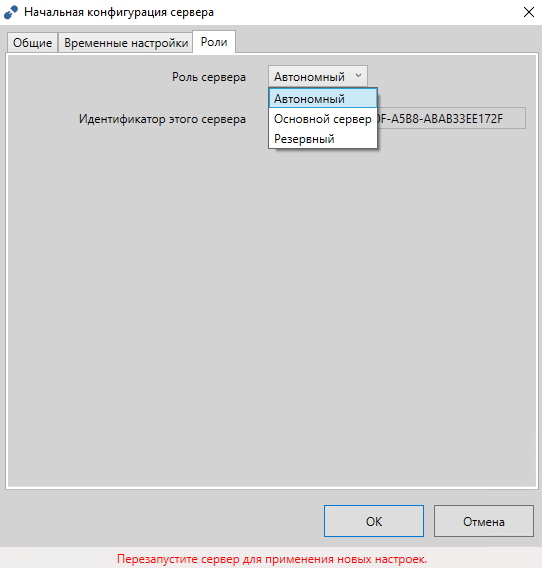


Рисунок 6 – Вкладка Роли окна настройки конфигурации сервера

Вкладка Роли (рис. 6) позволяет выбрать режим работы сервера и настроить резервирование. Настройка резервного сервера описана в подразделе 5.1.

**Внимание!** Перезагрузите сервер после изменения настроек.

## Настройка учетных записей диспетчеров

Учетные записи диспетчеров настраиваются на вкладке Диспетчеры диалогового окна Настройки сервера (рис. 7) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

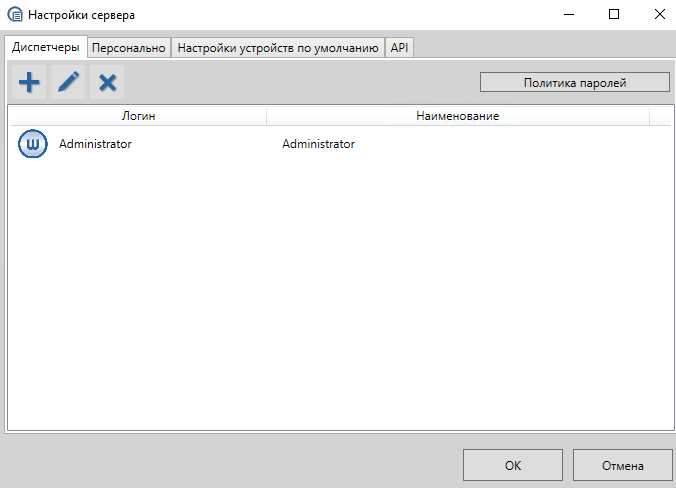


Рисунок 7 – Вкладка Диспетчеры с учётными записями диспетчеров

Учетные записи диспетчера используются для подключения к серверу из диспетчерской консоли ОМЕГА K400 (Astracom Console).

**Примечание.** Диспетчер, подключенный через ОМЕГА K400 (Astracom Console), может одновременно управлять несколькими сетями. Доступные диспетчеру сети назначаются в окне Изменить диспетчера (рис. 8) и отображаются в свойствах учетной записи диспетчера.

Добавление нового диспетчера в список или внесение изменений в настройки уже существующего из списка, отображаемого на вкладке Диспетчеры реализуется через диалоговое окно Изменить диспетчера (рис. 8) (нажмите кнопку  в окне Настройки сервера на вкладке Диспетчеры для добавления диспетчера и кнопку  для редактирования настроек выбранного диспетчера – рис. 7). Чтобы удалить выбранного из списка диспетчера, нажмите кнопку .

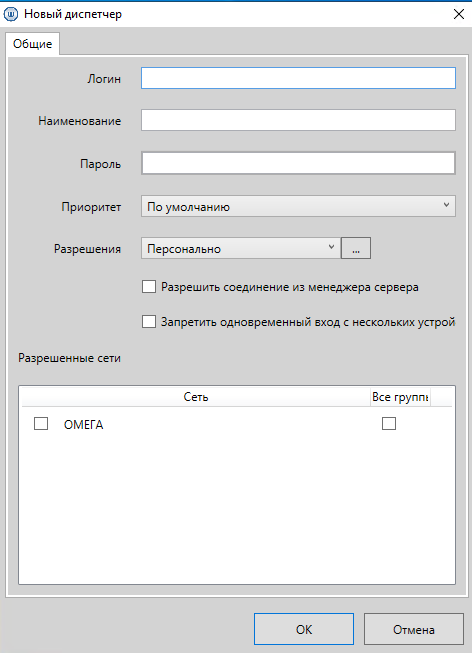


Рисунок 8 – Окно добавления диспетчера

В поле Логин (рис. 8) задайте логин диспетчера, используемый для входа на сервер.

В поле Наименование (рис. 8) задайте имя диспетчера, отображаемое в интерфейсе клиентского приложения.

В поле Пароль (рис. 8) задайте пароль диспетчера, используемый для входа на сервер.

В поле Приоритет (рис. 8) выберите приоритет диспетчера. Приоритет имеет смысл только в рамках текущего группового вызова PTT. Группа с более высоким приоритетом может прервать текущую передачу и начать разговор в рамках того же группового разговора (см. подраздел 2.4.1).

В поле Разрешения (рис. 8) выберите разрешения диспетчера. Разрешения могут быть унаследованы от разрешений, определенных в настройках сети, или установлены на пользовательское значение. Пользовательские разрешения применимы ко всем сетям, назначенным учетной записи диспетчера.

Установите «флажок» напротив Разрешить соединение из менеджера сервера (рис. 8), чтобы разрешить использование этой учетной записи для аутентификации в Менеджере сервера.

Установите «флажок» напротив Запретить одновременных вход с нескольких устройств (рис. 8), чтобы ограничить использование этой учетной записи для входа с разных компьютеров одновременно.

В списке Разрешенные сети (рис. 8) выберите сети, доступные диспетчеру. Установите Все группы, когда все группы, определенные в сети, должны быть доступны диспетчеру. В противном случае назначьте диспетчеру нужные группы в окне настроек сети (см. подраздел 3.6).

## Настройки клиентского приложения

### Настройки интерфейса

Настройки интерфейса абонентов сети расположены на вкладке Персонально диалогового окна Настройки сервера (рис. 9) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

Пользовательские настройки применяются при подключении клиента к серверу и сохраняются в файлах настроек.

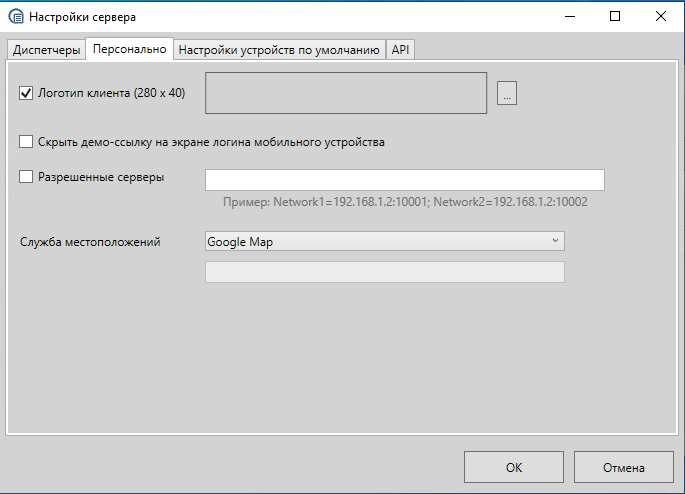


Рисунок 9 – Вкладка Персонально настроек абонента

Установите «флажок» напротив Логотип клиента (рис. 9) и загрузите изображение в формате PNG, чтобы заданное изображение демонстрировалось на экране клиентского приложения при входе в систему и в окне О программе.

Установите «флажок» напротив Скрыть демо-ссылку на экране логина мобильного устройства (рис. 9), чтобы скрыть ссылку на сайт разработчика на экране клиентского приложения при входе в систему.

Установите «флажок» напротив Разрешенные серверы (рис. 9) и перечислите в формате Network1 = ХХХ.ХХХ.Х.ХХ:Порт; адреса серверов, из списка которых абонент сможет выбирать при подключении. При подключении абоненту нельзя вводить адрес сервера вручную. Адрес сервера можно будет выбрать только из заданного здесь списка.

Пример списка серверов: Network1 = 192.168.1.10: 10001; Network2 = 192.168.1.10: 10002;

В поле Служба местоположений (рис. 9) выберите сервис определения местоположения для использования по умолчанию на устройствах абонентов.

Пользовательские настройки сохраняются на клиентском устройстве во внешних файлах:

Место расположения файла конфигурации на устройстве Android: ../files/custom.cfg

Место расположения файла логотипа на устройстве Android: ../files/customLogo.png

Файлы клиентских настроек могут быть предварительно загружены на устройства Android для применения настроек перед первым входом в систему.

### Определение настроек по умолчанию

Настройки по умолчанию для клиентского приложения расположены на вкладке Настройки устройств по умолчанию диалогового окна Настройки сервера (рис. 10) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

Параметры по умолчанию, определенные сервером, позволяют автоматически применять настройки определенных устройств абонентов при их входе на сервер.

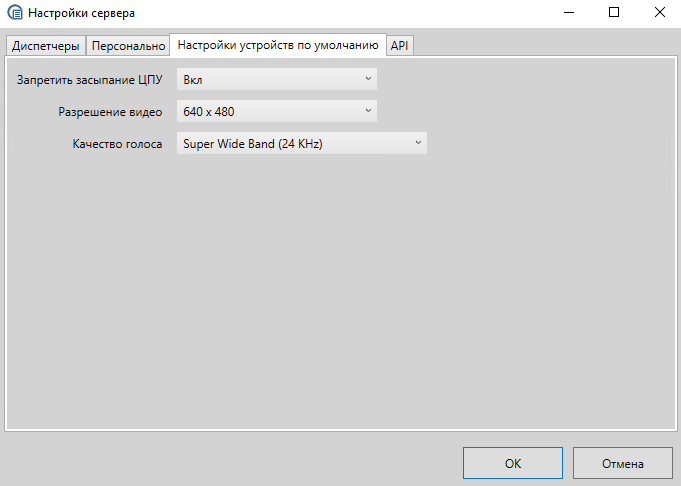


Рисунок 10 – Вкладка Настройки устройств по умолчанию настройки клиентских приложений по умолчанию

В поле Запретить засыпание ЦПУ (рис. 10) выберите Вкл для предотвращения перехода пользовательского устройства в «спящий» режим. При этом устройство абонента будет потреблять больше энергии при одновременном повышении скорости отклика клиентского приложения.

В поле Разрешение видео (рис. 10) выберите разрешение экрана для видеозвонков.

В поле Качество голоса (рис. 10) выберите частоту дискретизации для кодирования голоса. Более высокая частота дискретизации обеспечивает лучшее качество голоса, но требует более высокой пропускной способности сети для передачи (см. подраздел 1.4 о системных требованиях для получения более подробной информации).

## Сети серверов ОМЕГА

Сервер может управлять неограниченным количеством отдельных сетей. Каждая сеть изолирована от других сетей и имеет собственный набор метаданных (пользователи, группы, статусы и т.д.). Возможность использования нескольких сетей позволяет обрабатывать независимые объекты с одного сервера. Например, разные сети могут быть созданы для разных независимых компаний или отделов.

Выберите сервер из списка в окне Менеджер сервера (рис. 3). Для запуска / остановки локального сервера используйте кнопки Запустить локальный сервер  и Остановить локальный сервер  соответственно. Убедитесь, что выбранный сервер запущен. (Когда сервер запущен, значок слева должен вращаться.)

Чтобы добавить новую сеть, нажмите кнопку Новая сеть . Для удаления сети используйте кнопку . С помощью диалогового окна Новая сеть задаются настройки новой сети (рис. 11).

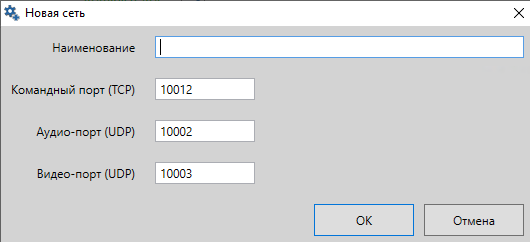


Рисунок 11 – Окно создания сети

В поле Наименование (рис. 11) задайте название сети.

В поле Командный порт (TCP) (рис. 11) задайте TCP-порт, используемый клиентами для подключения к серверу для передачи сигналов и общего обмена данными.

В поле Аудио-порт (UDP) (рис. 11) задайте порт UDP для передачи аудиопотоков.

В поле Видео-порт (UDP) (рис. 11) задайте UDP-порт для передачи видеопотоков.

Сети, созданные для сервера, отображаются в списке под записью сервера (рис. 12).

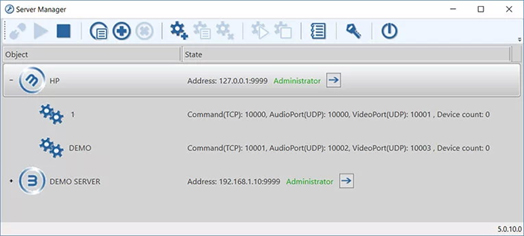


Рисунок 12 – Окно Менеджер сервера со списком сетей

Для запуска / остановки выбранной сети используйте кнопки Запустить сеть  и Остановить сеть  соответственно. Когда сеть запущена, значок шестеренки должен вращаться.

Дважды щелкните наименование сети в списке или используйте кнопку Настройки сети  , чтобы выполнить настройки сети (рис. 13).

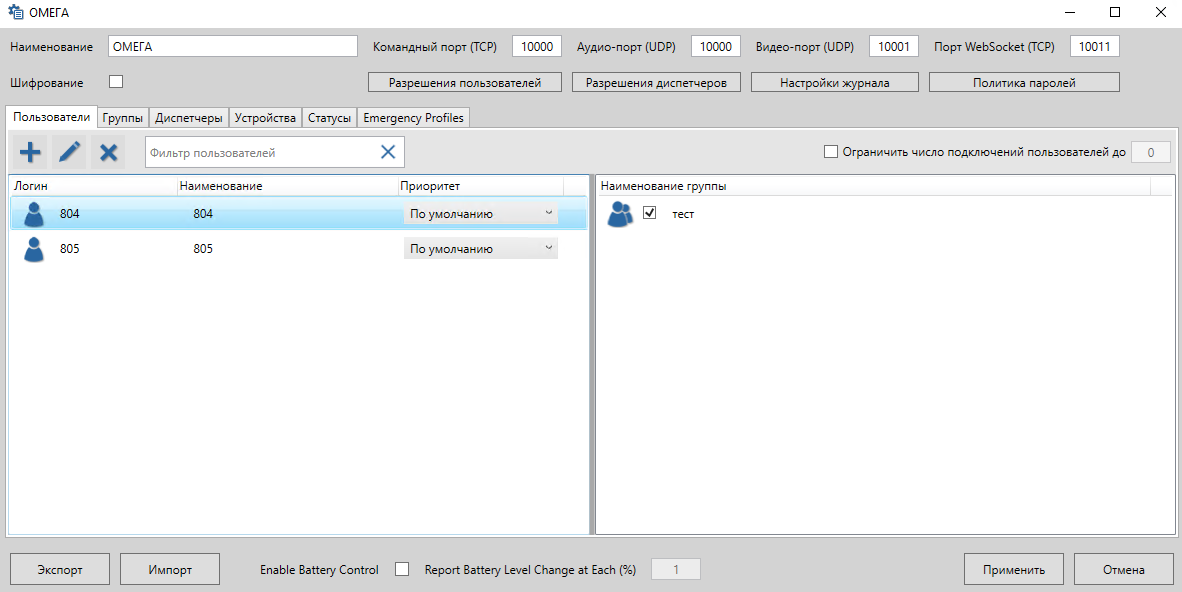


Рисунок 13 – Вкладка Пользователи с настройками сети

Установите «флажок» напротив Ограничить число подключений пользователей до (рис. 3, чтобы ограничить количество разрешенных подключений мобильных абонентов к сети числом, указанным в окне справа.

В поле Порт WebSocket (TCP) (рис. 13) задайте порт TCP, используемый сторонними приложениями для подключения через API с учетной записью абонента.

### Абоненты сети

Абоненты сети – это учетные записи, используемые для подключения к серверу из клиентского приложения ОМЕГА.

В окне Настройки сети (рис. 13) на вкладке Пользователи нажмите кнопку , чтобы добавить новую учетную запись; кнопку , чтобы отредактировать существующую; кнопку , чтобы удалить учётную запись. Настройка учётной записи происходит через диалоговое окно Изменить пользователя (рис. 14).

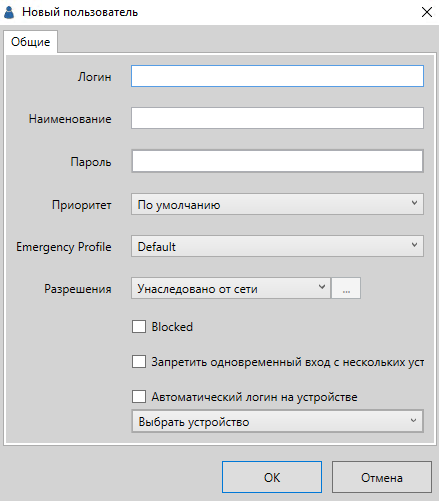


Рисунок 14 – Окно добавления нового абонента

В поле Логин (рис. 14) задайте имя абонента, используемое для входа на сервер.

В поле Наименование (рис. 14) задайте имя абонента, отображаемое в интерфейсе клиентского приложения.

В поле Пароль (рис. 14) задайте пароль абонента, используемый для входа на сервер.

В поле Приоритет (рис. 14) выберите приоритет абонента. Приоритет имеет смысл только в рамках текущего группового вызова PTT. Абонент с более высоким приоритетом может прервать текущую передачу и начать разговор в рамках того же группового разговора (см. подраздел 2.4.1).

В поле Emergency Profile (рис. 14) выберите аварийный профиль абонента.

В поле Разрешения (рис. 14) выберите разрешения абонента. Разрешения могут быть унаследованы от разрешений абонента, определенных в настройках сети, или установлены индивидуально.

Установите «флажок» напротив Blocked (рис. 14), чтобы заблокировать абонента.

Установите «флажок» напротив Запретить одновременный вход с нескольких устройств (рис. 14), чтобы ограничить использование этой учетной записи для входа с разных устройств одновременно.

Установите «флажок» напротив Автоматический логин на устройстве (рис. 14) и назначьте конкретное устройство учетной записи абонента для автоматического входа в систему (устройство автоматически входит на сервер без проверки пароля).

### Группы сети

Группы сети используются в функциях, поддерживающих групповые операции (обмен текстовыми сообщениями, вызовы PTT, запросы местоположения и т.д.). К каждой группе могут присоединиться неограниченное количество абонентов.

В окне Настройки сети (рис. 15) на вкладке Группы нажмите кнопку , чтобы добавить новую группу; кнопку , чтобы отредактировать существующую; кнопку , чтобы удалить группу.

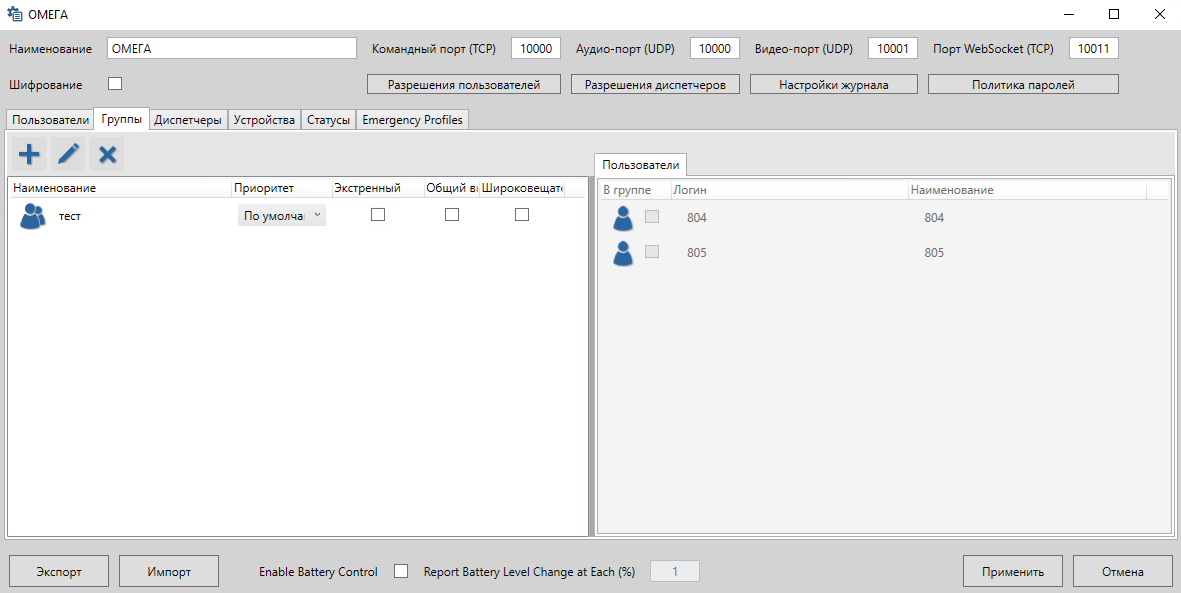


Рисунок 15 – Вкладка Группы с группами абонентов

Настройка группы происходит через диалоговое окно Изменить группу (рис. 16).

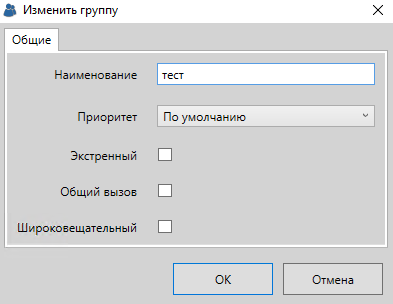


Рисунок 16 – Окно изменения группы абонентов

В поле Наименования (рис. 16) задайте название группы, отображаемое в интерфейсе клиентского приложения.

В поле Приоритет (рис. 16) выберите групповой приоритет. Приоритет имеет смысл только в рамках обычных групповых вызовов. Текущий групповой вызов прерывается и подключается новый групповой вызов, если новая группа имеет более высокий приоритет (см. подраздел 2.4.1).

Установите «флажок» напротив Экстренный (рис. 16), чтобы отметить группу как аварийную (см. подраздел 3.6.6).

Установите «флажок» напротив Общий вызов (рис. 16), для того чтобы общий вызов мог быть инициирован только абонентам, входящими в группу, но передан всем онлайн-абонентам в сети, даже если они не являются членами группы.

Установите «флажок» напротив Широковещательный (рис. 16), чтобы разрешить широковещательную рассылку – односторонний групповой вызов, на который нельзя ответить.

Чтобы добавить абонентов в группу на вкладке Группы (рис. 15) в окне Настройки сети, выберите группу и установите флажки для соответствующих абонентов или на вкладке Пользователи (рис. 13) выберите абонента и установите флажки напротив групп, куда он будет включён.

### Диспетчеры сети

Диспетчеры сети – это учетные записи, используемые для подключения к серверу из приложения ОМЕГА K400 (Astracom Console).

В окне Настройки сети на вкладке Диспетчеры нажмите кнопку , чтобы добавить новую учетную запись; кнопку , чтобы отредактировать существующую; кнопку , чтобы удалить учётную запись. Настройка учётной запись происходит через диалоговое окно Изменить диспетчера.

Чтобы диспетчеры имели возможность создавать задания для обновления клиентского приложения, файлы APK, содержащие версии, должны быть помещены в папку ..\OtapPackages на сервере.

### Устройства сети

Устройства сети – это список устройств абонентов, которые хотя бы однажды были подключены к серверу. Устройства нельзя добавлять вручную. Они автоматически добавляются в кэш после успешного входа в систему с определенного устройства. Перечень устройств отображается в окне Настройки сети (рис. 17) на вкладке Устройства.

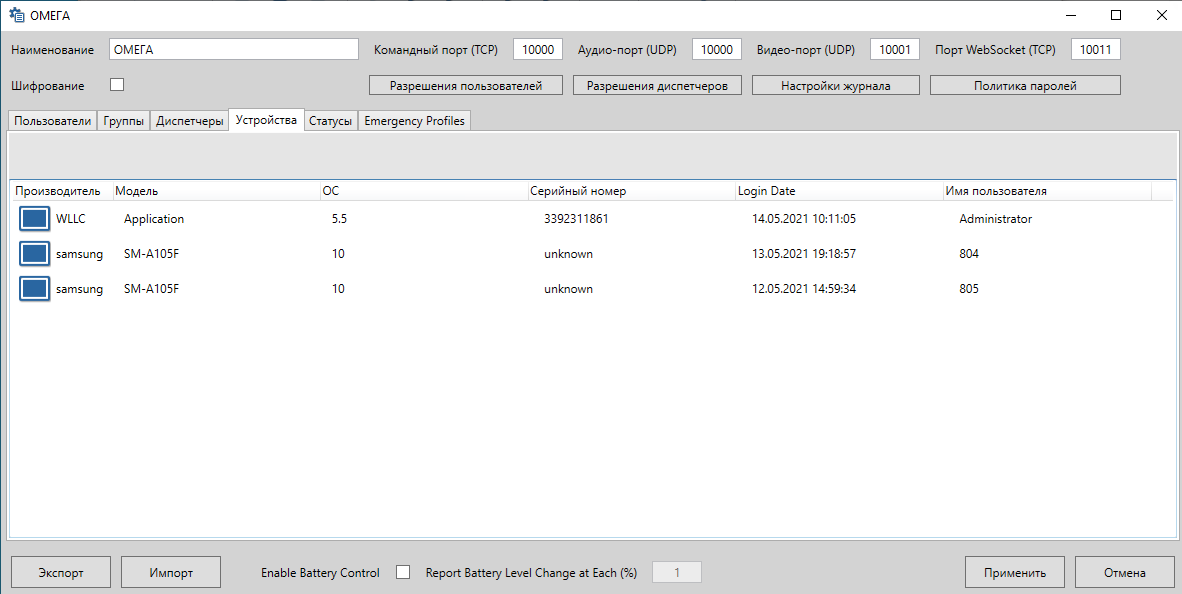


Рисунок 17 – Вкладка Устройства с перечнем клиентских устройств

### Статусы устройств

Статус устройств – это атрибут, который может быть применен к конкретному устройству в клиентском приложении, отражающем текущую активность абонента: свободен, занят, дежурный и т.д. Каждый статус отмечен цветом для удобства использования.

В окне Настройки сети на вкладке Статусы нажмите кнопку , чтобы добавить новый статус; кнопку , чтобы отредактировать существующий; кнопку , чтобы удалить статус.

Настройка статуса происходит через диалоговое окно Новый статус (рис. 18).

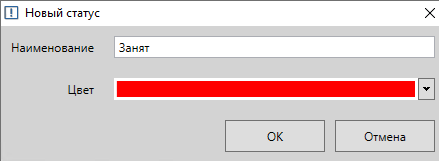


Рисунок 18 – Окно создания статуса

В диалоговом окне Новый статус (рис. 18) задайте наименование статуса и цвет его условного обозначения.

### Аварийные профили

Аварийный профиль – это набор свойств, определяющих поведение аварийного сигнала. Аварийный профиль устанавливается для абонента / группы абонентов либо в окне Менеджер сервера → Настройки сети → Изменить пользователя (рис. 14) / Изменить группу (рис. 16), либо в диспетчерской консоли.

По умолчанию каждому абоненту / группе назначается профиль Default.

В окне Настройки сети на вкладке Emergency Profiles нажмите кнопку , чтобы добавить новый профиль для использования в различных чрезвычайных ситуациях; кнопку , чтобы отредактировать существующий профиль; кнопку , чтобы удалить профиль. Настройка профиля происходит через диалоговое окно Edit Profile (рис. 19).

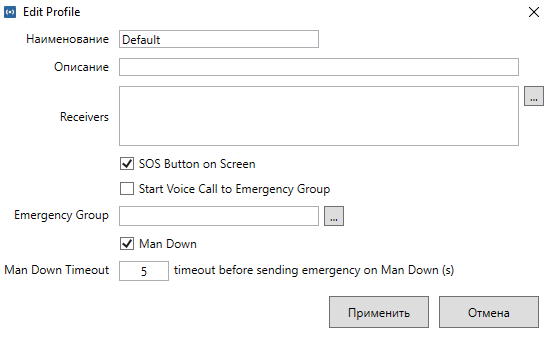


Рисунок 19 – Окно изменения профилей

В поле Наименование (рис. 19) задайте название профиля.

В поле Описание (рис. 19) задайте описание профиля.

В поле Receivers (рис. 19) составьте (через запятую) список диспетчеров, абонентов или групп, получающих экстренное уведомление.

Установите «флажок» напротив SOS Button on Screen (рис. 19), чтобы кнопка SOS отображалась на экране мобильного устройства абонента.

Установите «флажок» напротив Start Voice Call to Emergency Group (рис. 19) и назначьте Emergency Group, чтобы сопровождать сигнал экстренной помощи голосовым вызовом выбранной группы экстренной помощи.

Установите «флажок» напротив Man Down (рис. 19), чтобы при падении устройства инициировался аварийный сигнал.

**Примечание**. Данная функция поддерживается только на устройствах с акселерометром.

В поле Man Down Timeout (рис. 19) задайте время задержки для отправки аварийного сигнала Man Down после падения устройства.

Аварийный сигнал всегда сопровождается запросом местоположения устройства, пославшего этот сигнал.

### Разрешения абонентов

Разрешения абонентов определяют функциональные возможности, доступные абонентам сети. Для этого в окне Настройки сети (рис. 13) нажмите кнопку Разрешения пользователей, чтобы открыть окно определения полномочий Разрешения пользователей (рис. 20).

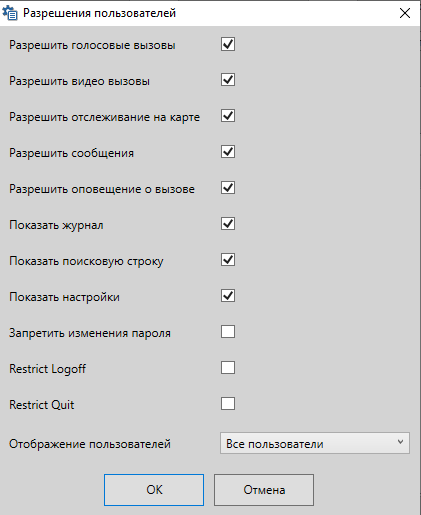


Рисунок 20 – Окно настроек полномочий абонента

Перечень допустимых полномочий абонента:

Разрешить голосовые вызовы – Разрешить посылать голосовые вызовы PTT;

Разрешить видео вызовы – Разрешить посылать видеовызовы PTT;

Разрешить отслеживания на карте – Разрешить отслеживание местоположения;

Разрешить сообщения – Разрешить посылать сообщения;

Разрешить оповещения о вызове – Разрешить посылать сигнал предупреждения при вызове;

Показать журнал – Разрешить просмотр журнала событий (см. подраздел 3.6.9);

Показать поисковую строку – Разрешить доступ к окну поиска;

Показать настройки – Разрешить просмотр настроек;

Запретить изменение пароля – Ограничить изменение пароля;

Отображение пользователей – Включить режим присутствия для выбранного сообщества (см. подраздел 3.6.9).

### Разрешения диспетчера

Разрешения диспетчеров определяют функциональность, доступную диспетчерам сети.

Для этого в окне Настройки сети (рис. 13) нажмите кнопку Разрешения диспетчеров, чтобы открыть окно определения полномочий диспетчера Разрешения диспетчеров (рис. 21).

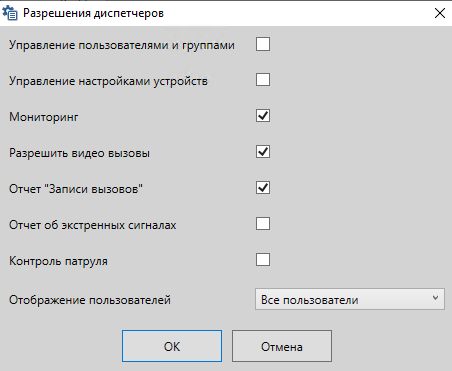


Рисунок 21 – Окно настроек полномочий диспетчера

Перечень допустимых полномочий для диспетчера:

Управление пользователями и группами – Разрешить управление абонентами и группами;

Управление настройками устройств – Разрешить управление настройками устройств;

Мониторинг– Разрешить удалённый мониторинг (см. подраздел 5.2);

Отчёт “Записи вызовов” – Разрешить вести отчет о записи разговоров;

Отображение пользователей – Включить режим присутствия для выбранного сообщества (см. подраздел 3.6.9).

**Примечание**. Чтобы получить доступ к функциям OTAP в диспетчерской консоли, необходимо включить режим присутствия.

### Параметры режима присутствия

Пункт Отображение пользователей определяет видимость абонентов и диспетчеров в клиентском приложении и диспетчерской консоли. Режим присутствия назначается отдельно для мобильных устройств (через диалоговое окно Разрешения пользователей – рис. 20) и диспетчерских консолей (через диалоговое окно Разрешения диспетчеров – рис. 21).

Допустимые значения параметра Отображение пользователей:

Все пользователи – все абоненты сети, перечисленные в интерфейсе приложения.

Только члены групп – только абоненты, входящие в те же группы, что и абонент, вошедший в систему.

Только группы – только доступные группы (приложение не будет показывать ни абонентов сети, ни диспетчеров).

Только группы и диспетчеры – помимо списка групп, абонент сможет видеть диспетчеров, вошедших в сеть.

## Журнал событий

Журнал событий представляет собой список событий, проходящих через сервер.

Настройки журнала событий расположены в окне Журнал событий (рис. 22) (запускается кнопкой Журнал событий  в окне Менеджер сервера – рис. 3).

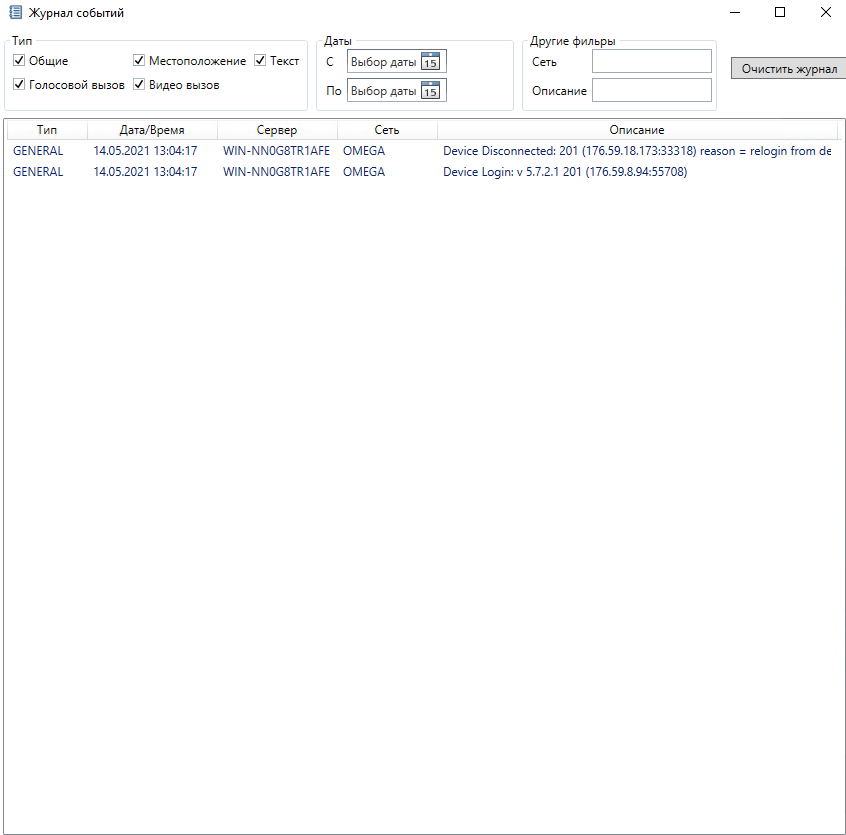


Рисунок 22 – Окно журнала событий

Настройки журнала определяют количество дней для хранения журнала событий и тип записей голосовых и видеозвонков для хранения. В окне Журнал событий (рис. 22) также можно просмотреть события с помощью фильтра и удалить ненужные.

## Лицензии

Перечень лицензий расположен на вкладке Лицензии (рис. 23) (запускается кнопкой Лицензии  в окне Менеджер сервера – рис. 3).

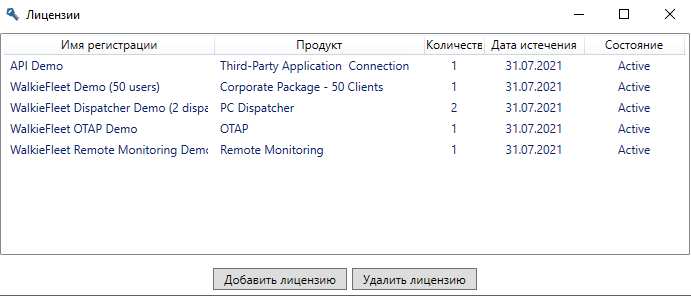


Рисунок 23 – Окно лицензий

Сервер активируется с помощью лицензионного ключа, предоставленного производителем. Лицензионный ключ представляет из себя зашифрованный файл с расширением WFL.

Существует два вида лицензионных ключей: демонстрационный и постоянный. Демо-ключ предоставляется для демонстрационных целей и ограничен сроком действия. Постоянный ключ выдается при покупке и не имеет ограничения по дате.

Срок бесплатного обновления ограничен одним годом после покупки. Чтобы продлить период обновления, необходимо приобрести годовую подписку.

### Идентификатор оборудования

Для постоянных лицензий требуется идентификатор оборудования, полученный на компьютере, на котором запущен менеджер сервера. Идентификатор оборудования, встроенный в лицензионный ключ, предотвращает незаконную установку программы.

Порядок генерации идентификатора оборудования

* Чтобы получить инструмент создания идентификатора оборудования обратитесь к разработчику системы радиосвязи ОМЕГА (группа компаний «АСТРАКОМ»).
* Разархивируйте архив и запустите FleetHID.exe на компьютере, на котором установлен сервер.
* Нажмите кнопку Get Hardware ID.

Идентификатор оборудования должен отобразиться в текстовом поле (рис. 24).

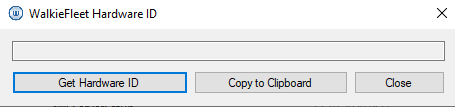


Рисунок 24 – Окно с идентификатором оборудования Hardware ID

### Активация лицензионного ключевого файла

Лицензионные ключи поставляются в файлах с расширением WFL.

Порядок активации лицензионного ключа

Откройте Менеджер сервера (рис. 25). Нажмите кнопку Лицензии  (рис. 26).

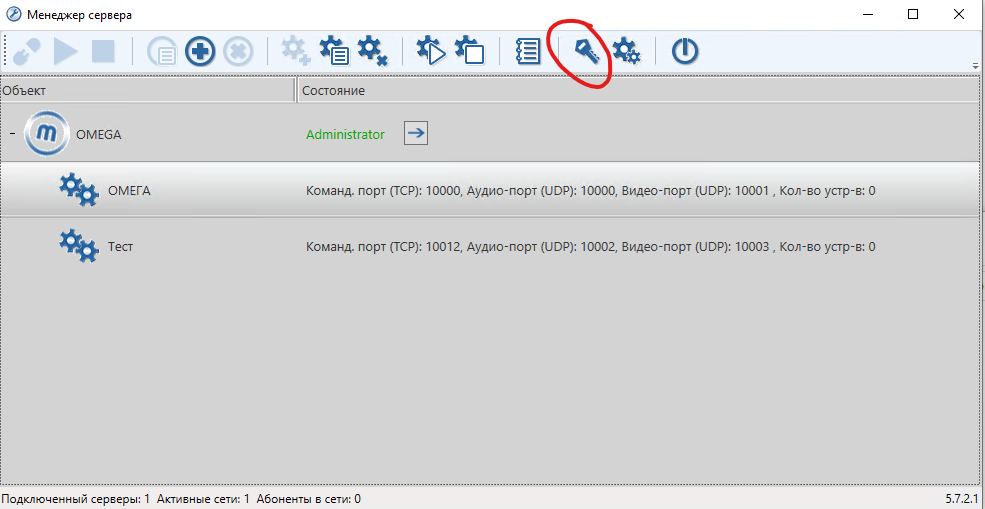


Рисунок 25 – Окно Менеджер сервера для перехода к окну Лицензии

В диалоговом окне Лицензии (рис. 26) нажмите кнопку Добавить лицензию и выберите файл лицензионного ключа.

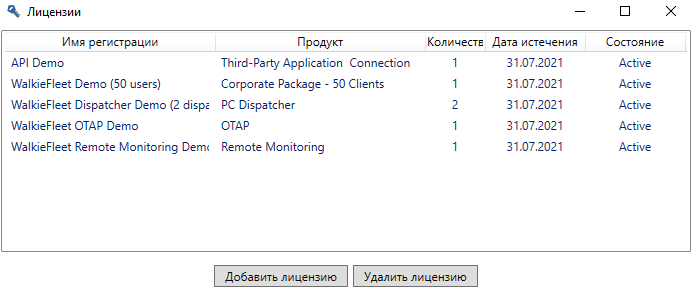


Рисунок 26 – Окно лицензий для добавления лицензионного ключа

Запись о лицензии должна отображаться в списке (рис. 25). Убедитесь, что добавленная лицензия активна (Состояние = Active).

## Настройка DMR

DMR (Digital Mobile Radio) – новый стандарт профессиональной радиосвязи, разработанный Европейским институтом телекоммуникационных стандартов (ETSI), как единый общеевропейский стандарт цифровой радиосвязи.

Существует три разновидности стандарта DMR:

DMR Tier I – простейший вариант технологии, ориентированный на работу в нелицензируемом диапазоне 446 МГц. Ввиду своей ограниченности не получил распространения.

DMR Tier II – стандарт конвенциональной связи, охватывающий лицензируемые частоты от 66 до 960 МГц и позволяющий на одном частотном канале 12,5 кГц выделить два логических канала.

DMR Tier III – стандарт транкинговой связи в диапазонах 66-960 МГц с двухслотовым TDMA в канале 12,5 кГц и поддержкой пакетной передачи данных, в том числе по протоколам IPv4 и IPv6.

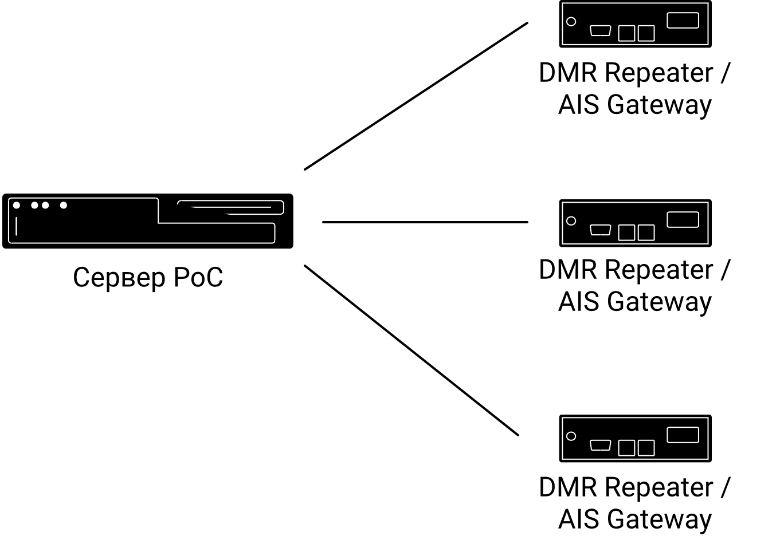


Рисунок 27 – Схема подключения сервера к DMR

### Excera AIS-DMR

Сети Excera DMR контролируются сервером по протоколу AIS (рис. 27).

Интерфейс приложения DMR (AIS) – это соединение на основе SIP для передачи голоса и данных по радиосети DMR Tier II и Tier III.

Функциональные возможности Excera DMR:

* сервер может подключать несколько сетей Excera DMR через шлюз AIS,
* частные и групповые голосовые вызовы между абонентами ОМЕГА и DMR,
* отслеживание местоположения,
* обмен текстовыми сообщениями,
* сигнал предупреждения,
* проверка радио.

**Примечание**. Для подключения к системе Excera DMR требуется лицензия Excera DMR.

Сервер ОМЕГА может подключать несколько шлюзов Excera AIS, встроенных в ретрансляторы, для управления абонентами DMR.

Все настройки подключения Excera DMR выполняются на вкладке DMR диалогового окна Настройки сервера (рис. 28) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

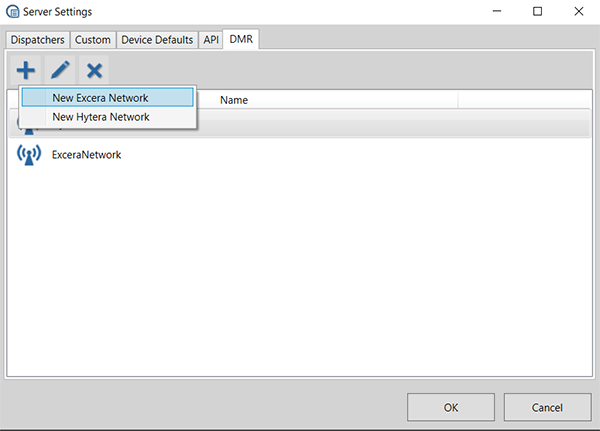


Рисунок 28 – Подключение сети Excera DMR в Менеджер сервера

Подключение Excera DMR

Добавление новой сети или внесение изменений в настройки уже существующей из списка, отображаемого на вкладке DMR реализуется через диалоговое окно DMR Network (рис. 28) (нажмите кнопку  в окне Настройки сервера на вкладке DMR для добавления сети и кнопку  для редактирования настроек выбранной сети – рис. 29, 30). Чтобы удалить выбранную из списка сеть, нажмите кнопку .

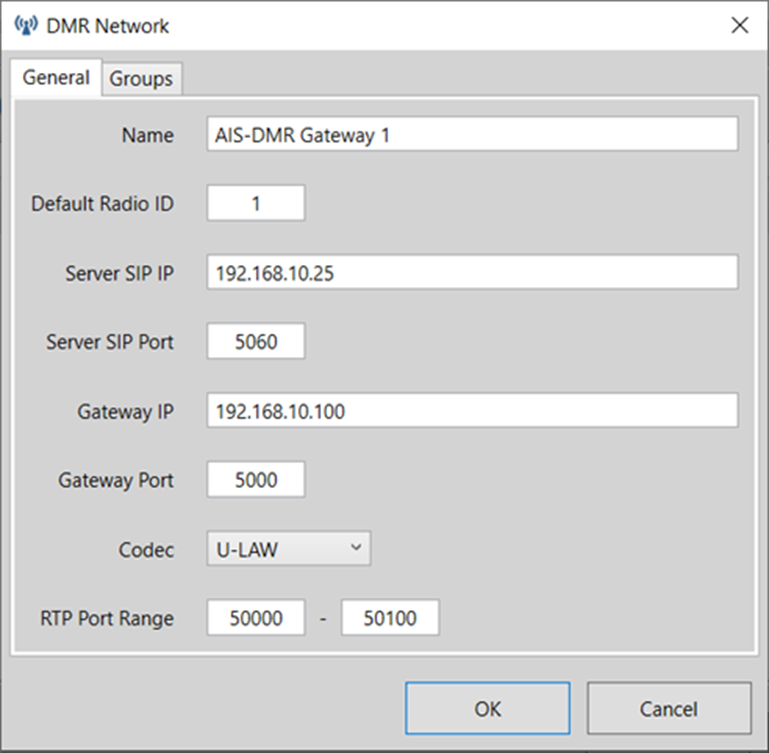


Рисунок 29 – Вкладка General окна подключения DMR Network

В поле Name (рис. 29) задайте имя сети.

В поле Default Radio ID (рис. 29) задайте номер, используемый по умолчанию для идентификации действий, выполняемых из ОМЕГА в систему DMR. Этот номер используется, если никакой другой идентификатор (Virtual Radio ID) не назначен диспетчеру или абоненту ОМЕГА, звонящему абонентам DMR.

**Примечание**. Идентификатор радо по умолчанию должен быть уникальным среди всех идентификаторов, назначенных абонентским устройствам DMR.

В поле Server SIP IP (рис. 29) задайте IP-адрес, используемый сервером для подключения к шлюзу AIS.

В поле Server SIP Port (рис. 29) задайте порт UDP, используемый сервером для подключения к шлюзу AIS.

В поле Gateway IP (рис. 29) задайте IP-адрес шлюза AIS.

В поле Gateway Port (рис. 29) задайте порт, используемый шлюзом AIS для приема SIP-подключений.

В поле Codec (рис. 29) выберите кодек, реализованный в шлюзе AIS.

В полях RTP Port Range (рис. 29) задайте диапазон портов UDP, используемых сервером для приема голосовых данных от шлюза AIS.

На вкладке Группы (рис. 34) представлен список групп, доступных серверу для голосовой связи через шлюз AIS.

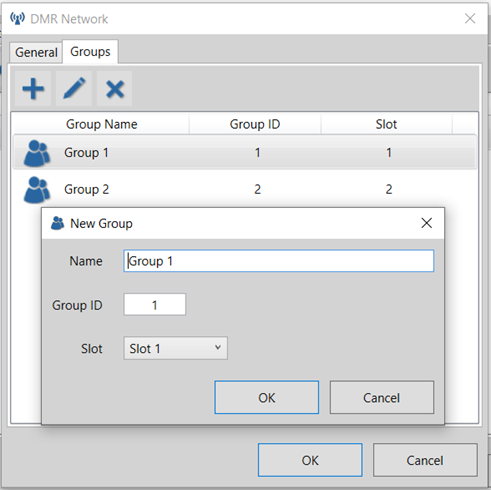


Рисунок 30 – Вкладка Группы окна подключения DMR Network

В поле Name (рис. 30) задайте имя группы.

В поле Group ID (рис. 30) задайте ID группы, как он определен в системе DMR.

В поле Slot (рис. 30) выберите номер слота.

### Hytera DMR

Сети Hytera DMR управляются сервером через IP-соединение с ретрансляторами с помощью протокола Hytera DMR Application Protocol. Сервер ОМЕГА не использует библиотеки Hytera SDK, что позволяет реализовать 64-битную службу и повысить гибкость (рис. 27).

Функциональные возможности Hytera DMR:

* сервер может подключать несколько сетей Hytera DMR через шлюз AIS,
* частные и групповые голосовые вызовы между абонентами ОМЕГА и DMR,
* отслеживание местоположения,
* обмен текстовыми сообщениями,
* сигнал предупреждения,
* проверка радио.

**Примечание**. Для подключения к системе Hytera DMR требуется лицензия Hytera DMR.

Сервер может одновременно подключать несколько сетей Hytera.

Все настройки подключения Hytera DMR выполняются на вкладке DMR диалогового окна Настройки сервера (рис. 31) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

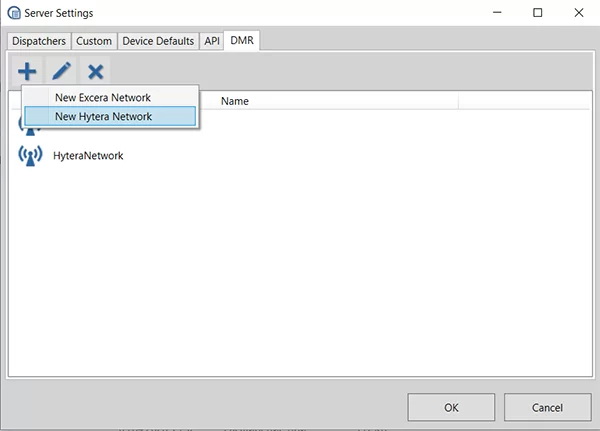


Рисунок 31 – Подключение сети Hytera DMR в Менеджер сервера

Подключение Hytera DMR

Добавление новой сети или внесение изменений в настройки уже существующей из списка, отображаемого на вкладке DMR реализуется через диалоговое окно DMR Network (рис. 28) (нажмите кнопку  в окне Настройки сервера на вкладке DMR для добавления сети и кнопку  для редактирования настроек выбранной сети – рис. 32, 33). Чтобы удалить выбранную из списка сеть, нажмите кнопку .

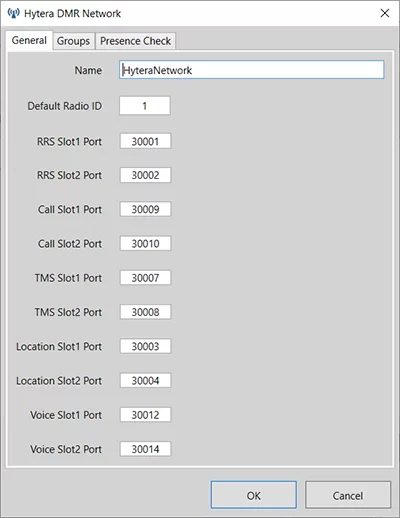


Рисунок 32 – Вкладка General окна подключения Hytera DMR

В поле Name (рис. 32) задайте имя сети.

В поле Default Radio ID (рис. 32) задайте идентификатор подключенного главного ретранслятора Hytera. Этот номер используется, если никакой другой идентификатор (Virtual Radio ID) не назначен диспетчеру или абоненту ОМЕГА, звонящему абонентам DMR.

**Примечание**. Идентификатор по умолчанию должен быть уникальным среди всех идентификаторов, назначенных абонентским устройствам DMR.

В полях RRS Slot1 Port ... Voice Slot2 (рис. 32) задайте номера портов, они должны иметь те же значения, что и в подключенном главном ретрансляторе Hytera.

На вкладке Группы (рис. 30) представлен список групп, доступных серверу для голосовой связи через соединение DMR.

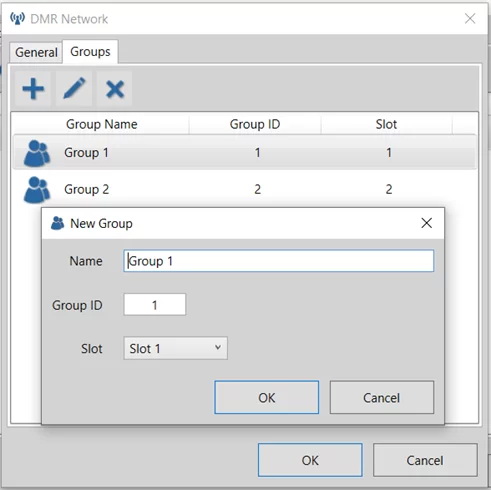


Рисунок 33 – Вкладка Группы окна подключения Hytera DMR

В поле Name (рис. 33) задайте имя группы.

В поле Group ID (рис. 33) задайте ID группы, как он определен в системе DMR.

В поле Slot (рис. 33) выберите номер слота.

На вкладке Presence Check (рис. 34) включите проверку присутствия, чтобы отслеживать состояние абонента DMR онлайн / офлайн.

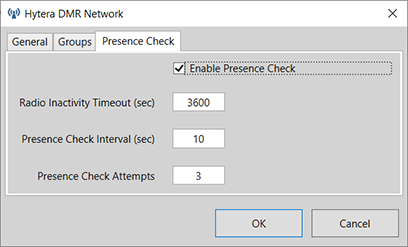


Рисунок 34 – Вкладка Presence Check окна подключения Hytera DMR

Установите «флажок» напротив Enable Presence Check и задайте значение в секундах в поле Radio Inactivity Timeout (рис. 34) для проверки радиостанции. Проверка запускается, если радиостанция бездействует в течение указанного промежутка времени.

В поле Presence Check Interval (рис. 34) задайте минимальный временной интервал между проверками радиостанции. Чтобы устранить зависание радиоканала, сервер не отправляет проверки радиосвязи чаще, чем указано в Presence Check Interval.

В поле Presence Check Attempts (рис. 34) задайте количество попыток отправить проверку радиосвязи на определенную радиостанцию. В случае отсутствия ответа сервер прекращает проверку наличия радиостанции в сети и предполагает, что она находится в автономном режиме.

Для работы Hytera DMR необходимо проверить настройки сети в операционной системе ретранслятора (рис. 35 – 38).

Настройка ретранслятора

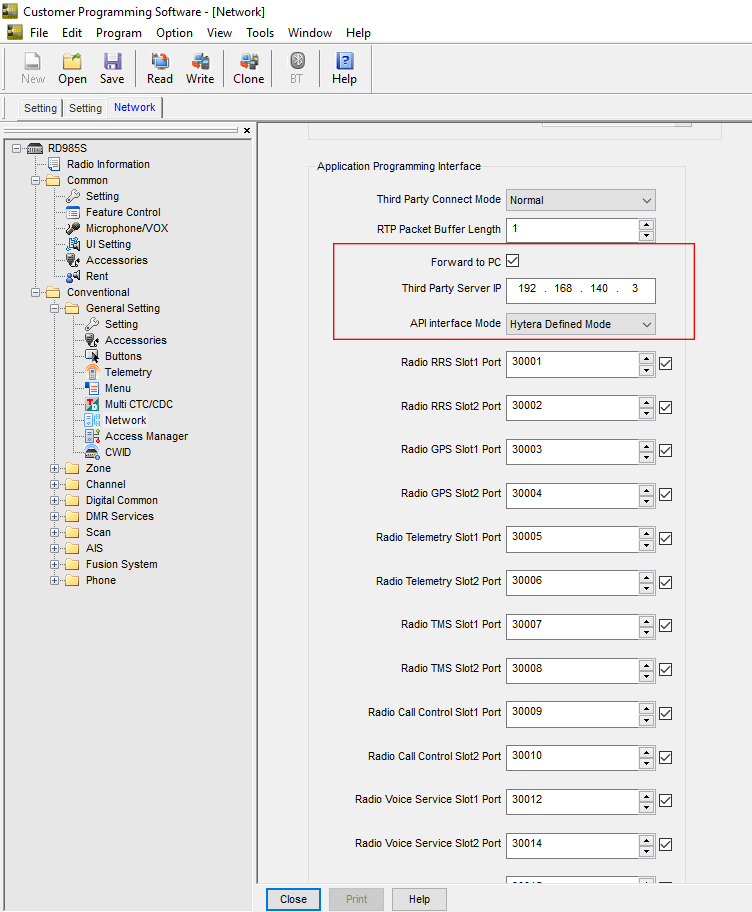


Рисунок 35 – Настройка ретранслятора

Должна быть включена опция Forward to PC (рис. 35).

В поле Third Part Server IP (рис. 35) должен быть IP-адрес сервера.

В поле API Interface Mode (рис. 35) установите режим, определенный Hytera.

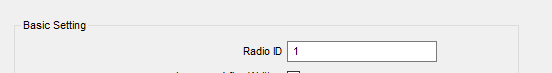


Рисунок 36 – Настройка ретранслятора

Radio ID (рис. 36) должен совпадать с Default Radio ID, установленным в свойствах подключения Hytera DMR.

Настройка Hytera Radio

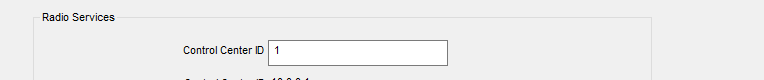


Рисунок 37 – Настройка ретранслятора

Control Center ID (рис.37) должен совпадать с Default Radio ID, установленным в свойствах подключения Hytera DMR.

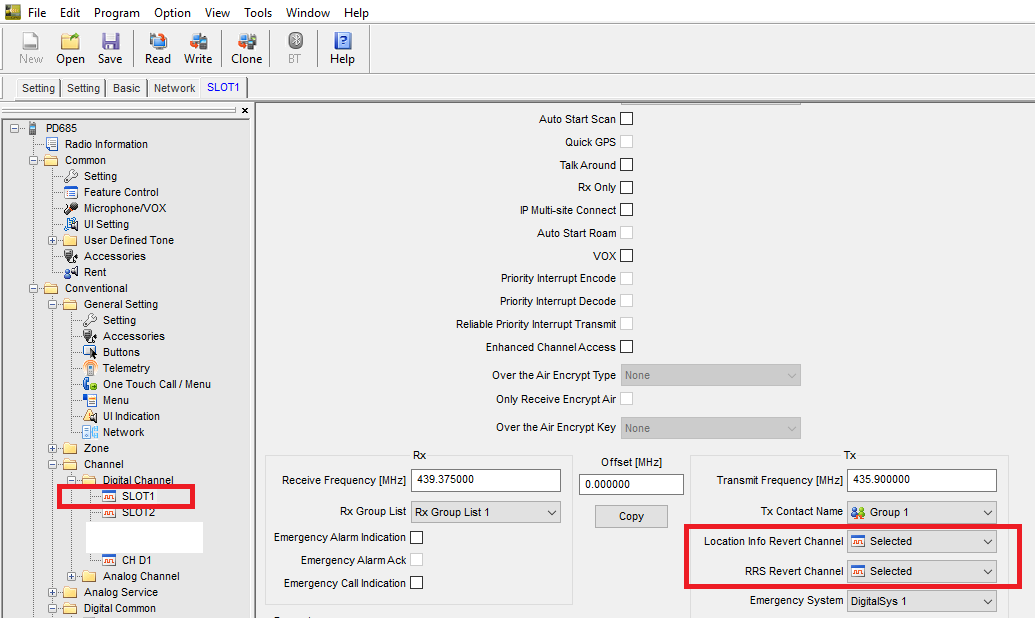


Рисунок 38 – Настройка ретранслятора

Для правильной работы Hytera DMR необходимо установить параметрам Location Info и RRS Revert Channel (рис. 38) значение Selected.

### Kirisun DMR

Сети Kirisun DMR контролируются сервером по протоколу AIS (рис. 27).

Интерфейс приложения DMR (AIS) – это соединение на основе SIP для передачи голоса и данных по радиосети DMR Tier II и Tier III.

Функциональные возможности Kirisun DMR:

* сервер может подключать несколько сетей Kirisun DMR через шлюз AIS,
* частные и групповые голосовые вызовы между абонентами ОМЕГА и DMR,
* отслеживание местоположения,
* обмен текстовыми сообщениями,
* сигнал предупреждения,
* проверка радио.

**Примечание**. Для подключения к системе Kirisun DMR требуется лицензия Kirisun DMR.

Сервер может подключать несколько шлюзов Kirisun AIS, встроенных в ретрансляторы, для управления абонентами DMR.

Все настройки подключения Kirisun DMR выполняются на вкладке DMR диалогового окна Настройки сервера (рис. 39) (запускается кнопкой Настройки сервера  в окне Менеджер сервера – рис. 3).

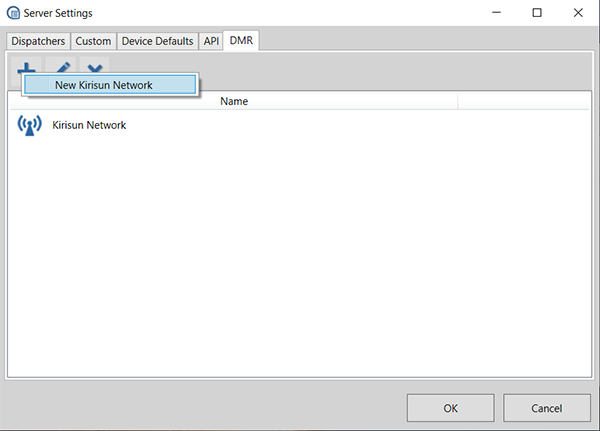


Рисунок 39 – Подключение сети Kirisun DMR в Менеджер сервера

Подключение Kirisun DMR

Добавление новой сети или внесение изменений в настройки уже существующей из списка, отображаемого на вкладке DMR реализуется через диалоговое окно Kirisun DMR Network (рис. 39) (нажмите кнопку  в окне Настройки сервера на вкладке DMR для добавления сети и кнопку  для редактирования настроек выбранной сети – рис. 40, 41, 42). Чтобы удалить выбранную из списка сеть, нажмите кнопку .

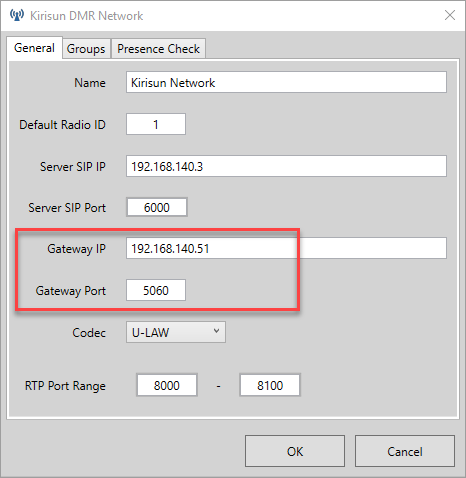


Рисунок 40 – Вкладка General окна подключения Kirisun DMR Network

В поле Name (рис. 40) задайте имя сети.

В поле Default Radio ID (рис. 40) задайте номер, используемый по умолчанию для идентификации действий, выполняемых из ОМЕГА в систему DMR. Этот номер используется, если никакой другой идентификатор (Virtual Radio ID) не назначен диспетчеру или абоненту ОМЕГА, звонящему абонентам DMR.

**Примечание**. Идентификатор радо по умолчанию должен быть уникальным среди всех идентификаторов, назначенных абонентским устройствам DMR.

В поле Server SIP IP (рис. 40) задайте IP-адрес, используемый сервером для подключения к шлюзу AIS.

В поле Server SIP Port (рис. 40) задайте порт UDP, используемый сервером для подключения к шлюзу AIS.

В поле Gateway IP (рис. 40) задайте IP-адрес шлюза AIS.

В поле Gateway Port (рис. 40) задайте порт, используемый шлюзом AIS для приема SIP-подключений.

В поле Codec (рис. 40) выберите кодек, реализованный в шлюзе AIS.

В полях RTP Port Range (рис. 40) задайте диапазон портов UDP, используемых сервером для приема голосовых данных от шлюза AIS.

На вкладке Группы (рис. 41) представлен список групп, доступных серверу для голосовой связи через шлюз AIS.

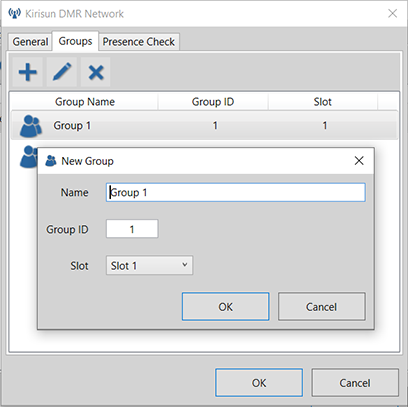


Рисунок 41 – Вкладка Группы окна подключения Kirisun DMR Network

В поле Name (рис. 41) задайте имя группы.

В поле Group ID (рис. 41) задайте ID группы, как он определен в системе DMR.

В поле Slot (рис. 41) выберите номер слота.

На вкладке Presence Check (рис. 41) включите проверку присутствия, чтобы отслеживать состояние абонента DMR онлайн / офлайн.

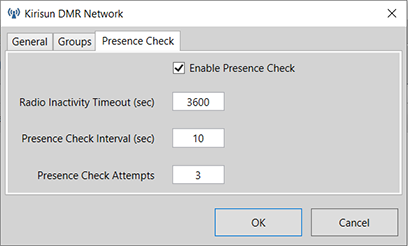


Рисунок 42 – Вкладка Presence Check окна подключения Kirisun DMR Network

Установите «флажок» напротив Enable Presence Check и задайте значение в секундах в поле Radio Inactivity Timeout (рис. 42) для проверки радиостанции. Проверка запускается, если радиостанция бездействует в течение указанного промежутка времени.

В поле Presence Check Interval (рис. 42) задайте минимальный временной интервал между проверками радиостанции. Чтобы устранить зависание радиоканала, сервер не отправляет проверки радиосвязи чаще, чем указано в Presence Check Interval.

В поле Presence Check Attempts (рис. 42) задайте количество попыток отправить проверку радиосвязи на определенную радиостанцию. В случае отсутствия ответа сервер прекращает проверку наличия радиостанции в сети и предполагает, что она находится в автономном режиме.

Настройка ретранслятора

Локальный IP-адрес ретранслятора должен соответствовать настройке IP-адреса шлюза в свойствах подключения Kirisun DMR в Менеджер сервера (рис. 43).



Рисунок 43 – Настройка ретранслятора

Порт прослушивания ретранслятора должен соответствовать настройке порта шлюза в свойствах подключения Kirisun DMR в Менеджер сервера (рис. 44).

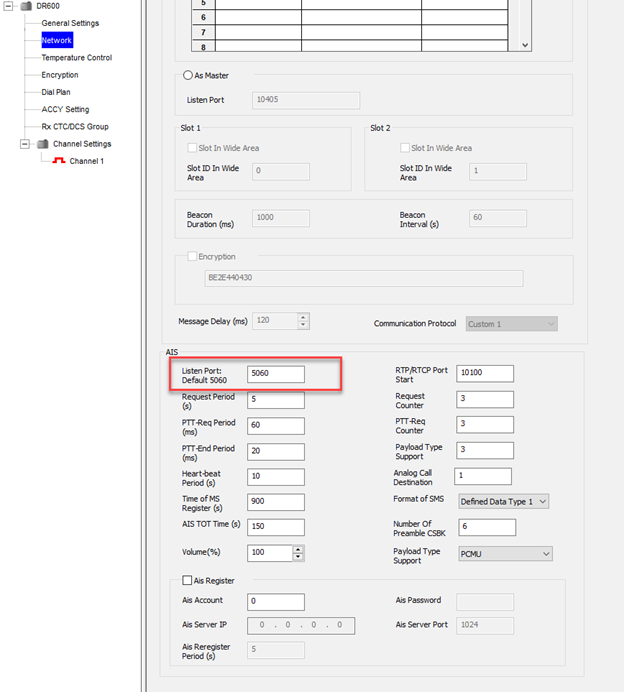


Рисунок 44 – Настройка ретранслятора

Для правильной работы службы присутствия (состояние радио On-line / Off-line) необходимо выполнить настройки на радиотерминале Kirisun (рис. 45).

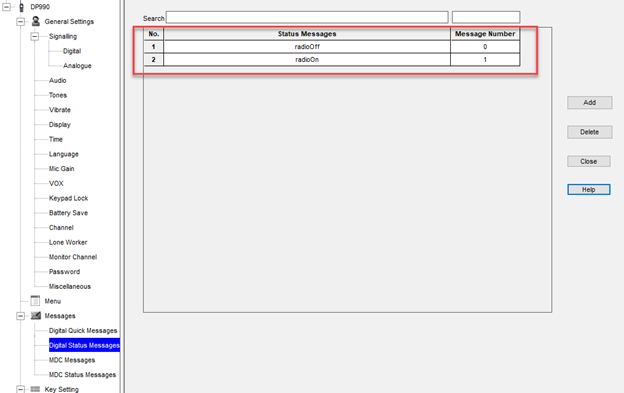


Рисунок 45 – Настройка ретранслятора

Определите статусные сообщения для событий Radio On и Radio Off (рис. 46).

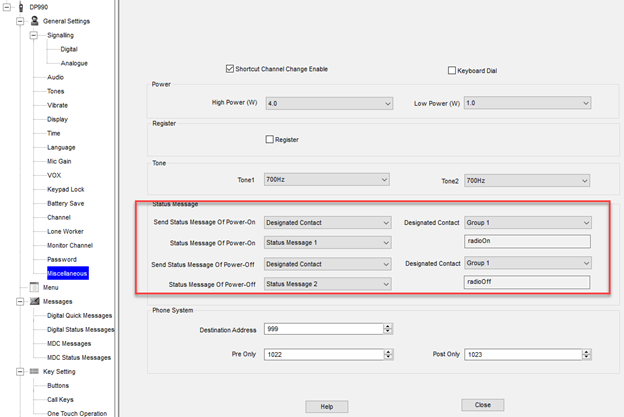


Рисунок 46 – Настройка ретранслятора

### Групповая ассоциация

Группа DMR становится доступной в сети ОМЕГА, когда она связана с определенной группой ОМЕГА.

Откройте окно Настройки сети (см. подраздел 3.6) и добавьте или откройте свойства группы, которая будет связана с группой DMR (рис. 47).

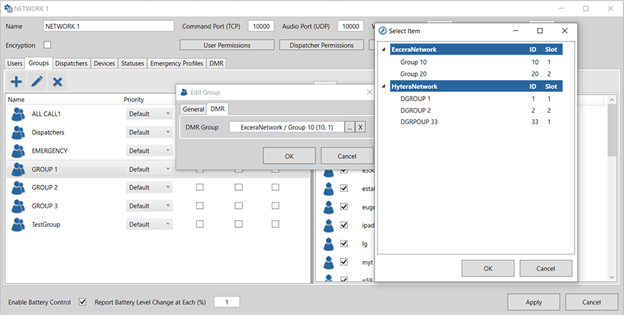


Рисунок 47 – Настройка групповой ассоциации

Перейдите на вкладку DMR и выберите соответствующую группу DMR.

### Назначение DMR-идентификатора (Virtual Radio ID)

Абоненту ОМЕГА может быть назначен Virtual Radio ID, являющийся его идентификатором в сети DMR.

Virtual Radio ID назначается в окне свойств абонента, на вкладке DMR (рис. 48).

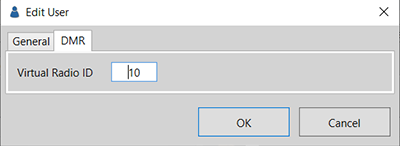


Рисунок 48 – Окно назначения Virtual Radio ID для абонента

Диспетчеру ОМЕГА можно назначить Virtual Radio ID, представляющий один в сети DMR.

Virtual Radio ID назначается в окне свойств диспетчера, на вкладке DMR (рис. 49).

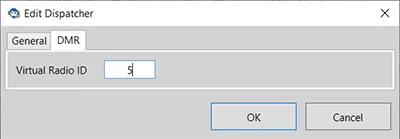


Рисунок 49 – Окно назначения Virtual Radio ID для диспетчера

### Подписчики DMR

Абоненты DMR могут появляться в списке абонентов мобильного клиента и диспетчерского приложения с определенными именами. Управление списком абонентов DMR осуществляется на вкладке DMR в окне Настройки сети (рис. 50).

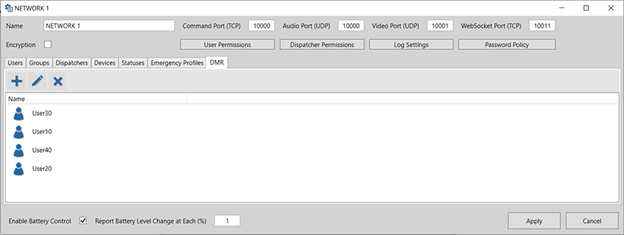


Рисунок 50 – Список абонентов DMR

## Порты, используемые сервером ОМЕГА

Сервером используются следующие типы портов:

* серверные порты, определенные в окне Начальная конфигурация сервера (см. подраздел 3.3);
* сетевые порты, определенные в окне Настройки сети (см. подраздел 3.6).

### Серверные порты

Серверные порты характеризуются следующими настройками в окне Начальная конфигурация сервера (рис. 51). Запускается кнопкой Начальная конфигурация сервера  в окне Менеджер сервера (рис. 3).

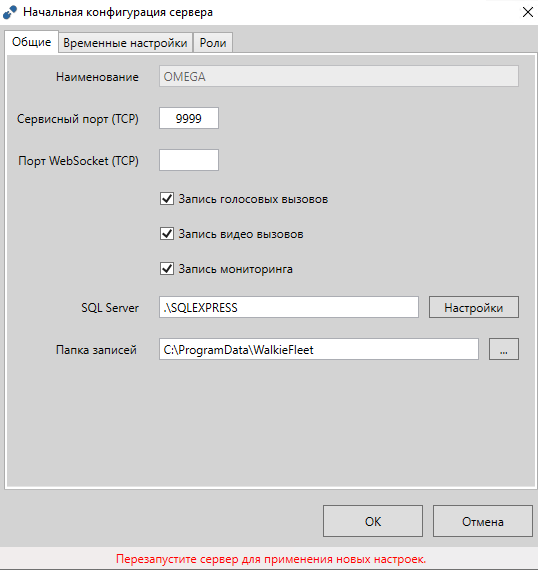


Рисунок 51 – Окно настройки серверного порта

В поле Сервисный порт (TCP) (рис. 51) задайте TCP-порт, используемый для подключения диспетчера, приложения Менеджер сервера и Резервного сервера. По умолчанию: 9999.

В поле Порт WebSocket (TCP) (рис. 51) задайте порт TCP, используемый сторонним диспетчерским приложением. Значения по умолчанию нет.

### Сетевые порты

Сетевые порты отображаются в окне Настройки сети (рис. 52). Запускается кнопкой Настройки сети  в окне Менеджер сервера (рис. 3).

Каждая сеть занимает 3 или 4 порта.

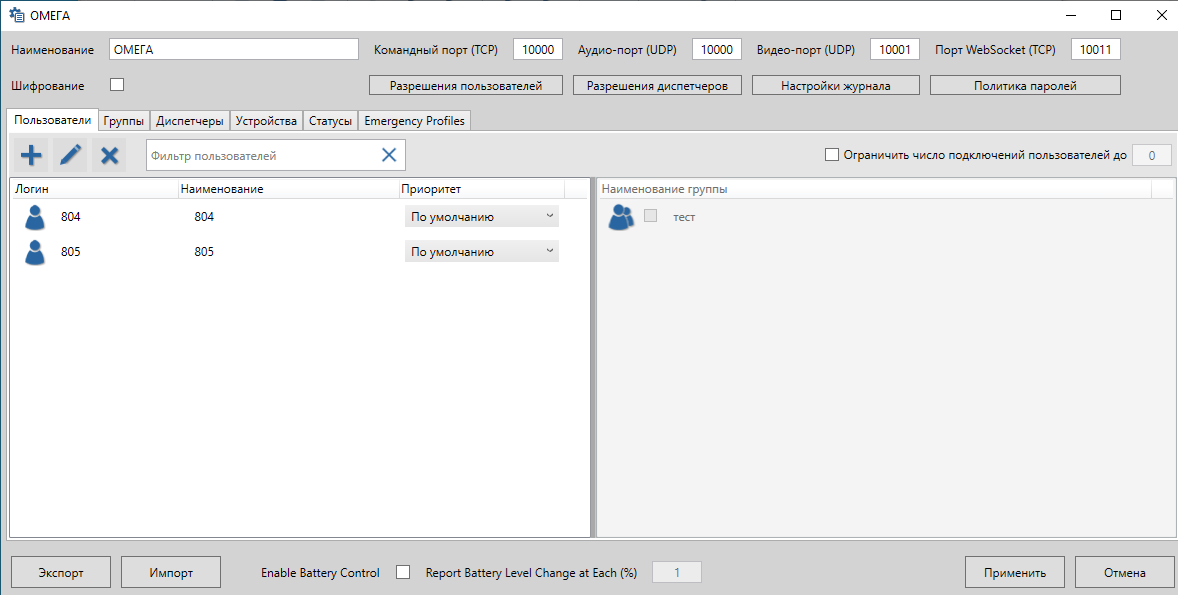


Рисунок 52 – Окно Настройки сети с отображением сетевых портов

В поле Командный порт (рис. 52) задайте TCP-порт, используемый для подключения мобильного клиента. По умолчанию для первой сети: 10000.

В поле Аудио-порт (рис. 52) задайте UDP-порт, используемый для передачи голосового потока. По умолчанию для первой сети: 10000.

В поле Видео-порт (рис. 52) задайте UDP-порт, используемый для передачи видеопотока. По умолчанию для первой сети: 10001.

В поле Порт WebSocket  (рис. 52) задайте TCP-порт, используемый сторонним клиентским приложением. Значения по умолчанию нет.

# Проверка программы

## Настройка сети для проведения тестирования

Для первоначальных тестов рекомендуется подключить серверный компьютер и устройства Android к одной локальной сети. В простейшем случае они должны быть подключены к одному маршрутизатору Wi-Fi.

**Внимание!** Соединение Wi-Fi подходит для временного тестирования, но не для постоянного использования. Динамический IP-адрес WAN подходит для тестов, но в реальной работе изменение IP-адреса на маршрутизаторе не позволит произвести подключение всех клиентов.

Выполните переадресацию портов NAT на маршрутизаторе между IP-адресом маршрутизатора в глобальной сети WAN и IP-адресом в локальной сети сервера LAN. Информацию о перенаправляемых портах можно найти в настройки сети программы (см. подраздел 3.6).

Убедитесь, что порты, необходимые для работы, не заблокированы антивирусом. В случае, если клиент не может подключиться к серверу, временно отключите антивирусное программное обеспечение, чтобы проверить, не мешает ли оно работе.

Помимо антивирусного программного обеспечения и брандмауэра, порты могут быть заблокированы сетевым оборудованием.

## Описание способов проверки

Проверка программы выполняется посредством проверки целостности приложения и тестирования его качественных (функциональных) характеристик.

Выполнение целостности осуществляется посредством проверки целостности дистрибутивного носителя и проверки соответствия установленных файлов дистрибутиву.

Тестирование качественных (функциональных) характеристик осуществляется посредством прогона программы.

## Проверка целостности

На данном этапе проверяется состав дистрибутива программы и наличие сбоев при установке программы.

Проверка считается пройденной успешно, если:

* носитель с дистрибутивом имеет инвентарный / заводской номер, совпадающий с номером на его этикетке;
* носитель дистрибутива не имеет внешних повреждений и читается на оборудовании пользователя;
* носитель с дистрибутивом содержит файлы, указанные на его этикетке;
* установка программы «Менеджер сервера» прошла в штатном режиме.

При возникновении проблем на любом этапе проверки, свяжитесь с поставщиком программного обеспечения.

## Методы прогона

Для прогона программы требуется настроить работу диспетчеров и абонентов сети согласно разделу 3. Установка и настройка диспетчерского приложения описана в документе «Консоль диспетчера ОМЕГА K400. Руководство оператора» АСТФ.468369.004. Установка и настройка клиентского приложения описана в документе «Инструкция по установке и эксплуатации программного обеспечения ОМЕГА К600Т».

Прогон считается пройденным успешно, если удалось настроить связь между всеми участниками системы радиосвязи ОМЕГА, управляемой сервером (рис. 1), и все функции, заявленные в подразделе 1.3, работают в штатном режиме.

При возникновении проблем на любом этапе прогона, свяжитесь с поставщиком программного обеспечения.

# Дополнительные возможности

## Резервирование сервера

Сервер может работать в трёх режимах:

1. Автономный – единый сервер, работающий без резервирования.
2. Основной – основной сервер, предполагающий возможность переключения на резервный сервер.
3. Резервный – резервный сервер, работающий в случае отсутствия администрирования.

### Особенности резервирования

* Резервирование позволяет использовать только один сервер резервного копирования.
* Для обеспечения резервирования требуется лицензия на сервер резервного копирования.
* Все метаданные (сети, абоненты, группы) автоматически копируются с основного на резервный сервер, но не наоборот.
* Журнал событий и записи не синхронизируются между основным и резервным серверами.

Все сети, абоненты и группы автоматически реплицируются с главного на резервный сервер. Все клиенты автоматически переводятся на резервный сервер в случае отказа главного.

### Настройки резервирования

Остановите сервер и откройте окно Начальная конфигурация сервера вкладку Роли (рис. 53).

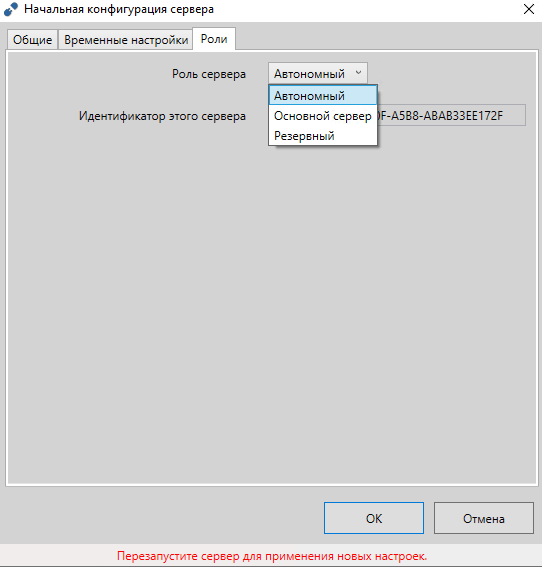


Рисунок 53 – Окно Начальная конфигурация сервера вкладка Роли

### Настройка режима Резервный сервер

Используйте значение, указанное в поле Идентификатор этого сервера (рис. 53) для определения сервера резервного копирования.

Укажите адрес резервного сервера (IP:port). IP – IP-адрес или имя хоста сервера резервного копирования. Port – служебный TCP-порт, указанный на вкладке Общие в окне Начальная конфигурация сервера.

**Внимание!** Перезагрузите сервер после изменения настроек.

### Настройка режима Основной

Используйте значение, указанное в поле Идентификатор этого сервера (рис. 53) для определения основного сервера.

Укажите адрес основного сервера (IP:port). IP – IP-адрес или имя хоста основного сервера. Port – служебный TCP-порт, указанный на вкладке Общие в окне Начальная конфигурация сервера.

Укажите задержку активации резервного сервера в секундах – тайм-аут для переключения клиентов на резервный сервер в случае недоступности основного сервера на вкладке Временные настройки в окне Начальная конфигурация сервера.

**Внимание!** Перезагрузите сервер после изменения настроек.

## Удаленный мониторинг

Удаленный мониторинг позволяет захватывать голос и видео с клиентских устройств, отображать их на консоли диспетчера и записывать на сервере. Удаленный мониторинг активируется лицензионным ключом. Разработчик предоставляет пробную демоверсию или постоянную.

**Примечание.** В некоторых странах скрытое наблюдение запрещено или ограничено законодательно. В связи с этим в мобильном клиенте имеется настройка, которая позволяет вывести на экран визуальное отслеживание, уведомляющее о подключении удаленного мониторинга. Тем не менее, перед использованием удалённого мониторинга убедитесь, что реализации этой функции удовлетворяет местным законам.

Включение удаленного мониторинга

Активируйте лицензию на удаленный мониторинг с помощью окна Менеджер сервера → Лицензии (см. подраздел 3.8).

Чтобы разрешить удаленный мониторинг для диспетчеров, в приложении Менеджер сервера откройте окно Настройки сети (рис. 13) (используйте кнопку ), нажмите кнопку Разрешения диспетчеров (рис. 21) и установите «флажок» напротив поля Мониторинг (см. подраздел 3.6.8).

Чтобы разрешить удаленный мониторинг на мобильном устройстве, в клиентском приложении откройте окно Настройки и установите «флажок» напротив поля Разрешить удалённый мониторинг.

Запуск / остановка мониторинга какого-либо устройства осуществляется диспетчером. Все голосовые и видеозвонки записываются на сервере. Каждый голосовой разговор записывается в mp3 файл. Видеозвонки записываются в формате MKV. Сервер продолжает мониторинг устройств, даже если консольное приложение закрыто. Удаленный мониторинг останавливается только тогда, когда с консоли отправляется команда Остановить Monitoring.

**Примечание.** Записи мониторинга автоматически разбиваются на файлы фиксированной продолжительности. По умолчанию интервал среза составляет 10 минут. Интервал мониторинга среза можно изменить в приложении Менеджер сервера → Начальная конфигурация сервера → вкладка Временные настройки.

## Шифрование трафика

Система ОМЕГА реализует дополнительное шифрование голосового и видео трафика между клиентом / диспетчером и сервером.

Особенности шифрования трафика

* Трафик между клиентом и сервером зашифрован по протоколу AES-256.
* Для включения шифрования трафика требуется лицензия Encryption.
* Шифрование включается / отключается в сетевых настройках сразу для всех мобильных клиентов или диспетчеров, подключенных к сети.
* Пара ключей, используемая для шифрования данных, генерируется автоматически для каждого сеанса подключения.
* Клиент или диспетчер всегда аутентифицируются на сервере по защищенному каналу TLS, даже если на сервере не включено шифрование трафика.
* Ключи шифрования доставляются клиенту или диспетчеру через защищенное соединение TLS.

## Телефонная связь

Телефонное соединение позволяет совершать звонки из IP-ATC или программных приложений на базе SIP группам или абонентам ОМЕГА по магистральному протоколу SIP.

Можно индивидуально настроить SIP-соединения для каждой сети.

**Примечание**. Для включения услуги требуется лицензия на подключение к телефонной сети.

Настройки телефонного соединения выполняются в окне Настройки сети приложения сервера Менеджер сервера (используйте кнопку , чтобы открыть окно – рис. 54).

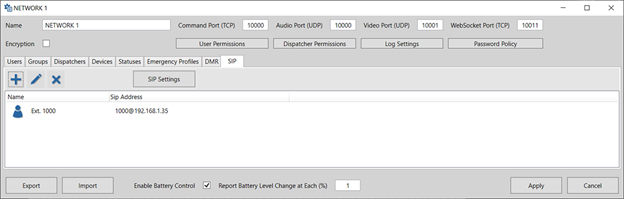


Рисунок 54 – Настройка телефонного соединения в окне Настройки сети

Список абонентов на вкладке SIP представляет контакты SIP, которые могут звонить группе или абоненту. В случае, когда телефонный вызов совершает указанный контакт, он отображается как имя абонента в соответствующих клиентских приложениях.

Настройка SIP-соединения производится в окне SIP Setting (рис. 55).

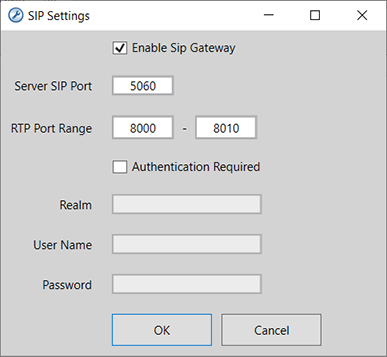


Рисунок 55 – Настройка SIP-соединения

Установите «флажок» напротив Enable SIP Gateway (рис. 55), чтобы включить шлюз SIP в сети для входящего соединения от IP-АТС или приложений программного телефона.

В поле Server SIP Port (рис. 55) задайте SIP-порт шлюза.

Установите «флажок» напротив Authentication Required (рис. 55), чтобы включить защищенное соединение со шлюзом.

Телефонный вызов абоненту или группе

IP-АТС или SIP-телефон должен установить соединение по SIP-магистрали с сервером через Server SIP Port.

SIP-имя – это имя группы без пробелов.

SIP-имя абонента – это логин абонента.

Пример группового SIP-адреса: *mygroup@192.168.1.45: 5060*

где

Mygroup – SIP-имя группы. Исходное название группы может быть «mygroup» или «my group»;

192.168.1.45 – IP-адрес сервера;

5060 – Порт SIP сервера, определенный в окне настроек SIP.

## Поддержка от разработчика

Приложение Assistant позволяет разработчику удаленно подключаться к компьютеру пользователя для оказания необходимой поддержки при установке и настройке. Чтобы получить установочный файл Assistant обратитесь к разработчику системы радиосвязи ОМЕГА (группа компаний «АСТРАКОМ»).

# Сообщения системному программисту

Программа «Менеджер сервера» не генерирует сообщений об ошибках, отличающихся от стандартных для операционной системы сервера.

Перечень сокращений

|  |  |  |
| --- | --- | --- |
| AIS | – | Интерфейс приложения DMR |
| API | – | Программный интерфейс контроллера |
| APK | – | Формат архивных исполняемых файлов-приложений для Android |
| DHCP | – | Dynamic Host Configuration Protocol – протокол динамической настройки узла |
| DMR | – | Digital Mobile Radio – стандарт профессиональной радиосвязи |
| GPS | – | Global Positioning System – система глобального позиционирования |
| IP | – | Маршрутизируемый протокол сетевого уровня |
| IP-ATC | – | Автоматическая телефонная станция на основе протокола IP |
| JPG | – | Растровый формат хранения графической информации |
| KML | – | Keyhole Markup Language – язык разметки на основе XML |
| LAN | – | Локальная сеть |
| NAT | – | Network Address Translation – протокол преобразования сетевых адресов |
| NFC | – | Технология беспроводной передачи данных малого радиуса действия |
| OTAP | – | Over-the-air programming |
| PNG | – | Растровый формат хранения графической информации |
| PoC | – | Технология для организации системы оперативной радиосвязи Push to Talk Over Cellular |
| POI | – | Point of interest – достопримечательность или другой объект, отмеченный точкой на карте |
| PPT | – | Вызовы Push to Talk |
| SDK | – | Библиотеки для разработки программного обеспечения |
| SIP | – | Session Initiation Protocol – протокол передачи данных |
| SSID | – | Service Set Identifier – идентификатор точки доступа Wi-Fi |
| TDMA | – | Time Division Multiple Access – множественный доступ с разделением по времени |
| TLS | – | Transport layer security – Протокол защиты транспортного уровня |
| TCP | – | Transmission Control Protocol – протокол передачи данных интернета |
| UDP | – | User Datagram Protocol – протокол пользовательских датаграмм |
| USB | – | Последовательный интерфейс для подключения периферийных устройств к вычислительной технике |
| WAN | – | Wide Area Network – компьютерная сеть |
| Wi-Fi | – | Технология беспроводной локальной сети |
| WFL | – | Автономный дизайн для данных процесса Workflow |
| КПП | – | Контрольно-пропускной пункт |
| ОЗУ | – | Оперативное запоминающее устройство |
| ПК | – | Персональный компьютер |

Лист регистрации изменений

|  | Номера листов (страниц) | | | | Всего листов (страниц) в докум. | № документа | Входящий № сопроводи-тельного документа и дата | Подп. | Дата |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Изм | изменен-ных | заменен-ных | новых | аннулиро-ванных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |