



# **BOND**

**Система корпоративного  
общения**

**Иструкция по развертыванию**

**Москва  
2022г.**

## **Контактная информация**

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: [office@avsw.ru](mailto:office@avsw.ru)

[www.avsw.ru/about/contacts](http://www.avsw.ru/about/contacts)

## **Авторское право**

ООО «АВ Софт»

[www.avsw.ru](http://www.avsw.ru)

© 2010-2022 ООО «АВ Софт»

## **Версия документа**

Март 30, 2022.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

## СОДЕРЖАНИЕ

1	Термины и определения .....	4
2	Сокращения.....	5
3	Общие сведения о программе .....	6
4	Системные требования .....	7
4.1	Доступ.....	8
4.2	Порты.....	8
5	Развёртывание и настройка сервера.....	9
5.1	Настройка вашего DNS-сервера.....	9
5.2	Настройка поддоменов.....	10
5.3	Настройка Ansible.....	11
5.4	Установка сервисов Бонда.....	12
5.5	SSL-сертификаты.....	12
5.6	Запуск служб .....	13
5.7	Регистрация пользователя .....	13
5.8	Пример конфигурационного файла .....	14
6	Панель администратора.....	16

## 1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	СУБД PostgreSQL	Свободная объектно-реляционная система управления базами данных (СУБД).
2.	Сервер облачного хранилища Minio	Сервер облачного хранилища, совместимый с Amazon S3, выпущенный под лицензией Apache License v2. Популярный сервер хранения объектов с открытым исходным кодом. Максимальный размер объекта составляет 5 ТБ.
3.	Протокол TURN	Предназначается для работы с симметричным NAT'ом. Использует сервер для передачи данных от клиента (как и STUN является клиент-серверным протоколом) любому количеству устройств (пиров).
4.	Android	Мобильная операционная система для смартфонов, планшетов и других устройств, разрабатываемая и выпускаемая компанией Google и конгломератом разработчиков и производителей мобильных устройств.
5.	iOS	Мобильная операционная система для смартфонов, планшетов и других устройств, разрабатываемая и выпускаемая компанией Apple.
6.	GAPPS	Набор сервисов, поставляемых компанией Google в рамках ОС Android. Одними из сервисов GAPPS является платформа распространения контента Google Play Market.

## 2 Сокращения

В настоящем документе используется перечень сокращений, представленных в таблице 2.

**Таблица 2. Сокращения и значения**

№	Сокращение	Значение
1.	СКК «BOND»	Средство корпоративной коммуникации BOND
2.	APM	Автоматизированное рабочее место
3.	ОС	Операционная система
4.	GAPPS	Google Application Services
5.	NAT	Преобразование сетевых адресов
6.	ПО	Программное обеспечение
7.	TURN	Traversal Using Relays around NAT

### 3 Общие сведения о программе

Средство корпоративной коммуникации BOND (далее – СКК «BOND») позволяет осуществлять все современные виды коммуникаций между пользователями в различных форматах. Мессенджер является клиент-серверным приложением. Структурная схема ПО СКК «BOND» представлена на рисунке 1.

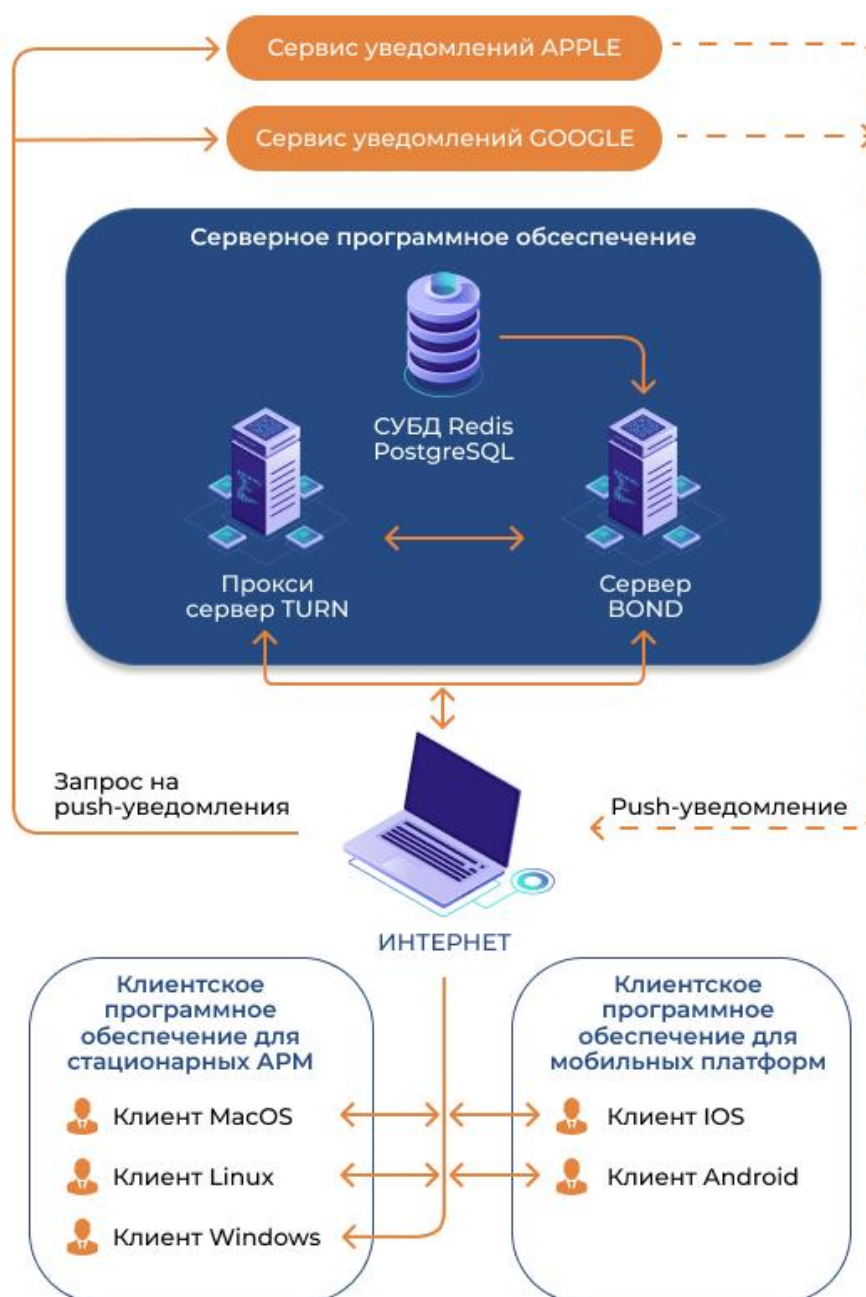


Рисунок 1. Структурная схема СКК «BOND»

## 4 Системные требования

Для эксплуатации СКК «BOND» рекомендуется использовать сервер с характеристиками не хуже указанных в таблице 3.

Таблица 3. Требования к характеристикам сервера

№	Характеристики сервера	Минимальные требования
1.	Количество ядер процессора	8
2.	Архитектура процессора	Рекомендуется x86
3.	Оперативная память	16 ГБ
4.	Диск	SSD Минимум для запуска - 10 GB. Для 400 пользователей, отправляющих в день по 10MB данных (картинки/текст/видео) - расчёт из хранения 4GB в день (на год требуется 1.5TB) HDD для архива документов по согласованию с Заказчиком
5.	Сеть	Внутренняя сеть – 1 Гб Внешняя сеть – 1 Гб
6.	ОС	– CentOS 7 – Debian (10/Buster или новее) – Ubuntu (18.04 или новее) – Archlinux
7.	Резидентная СУБД Redis	Версия не ниже 6.0

Специалисты, осуществляющие техническое сопровождение BOND, должны обладать следующими навыками и знаниями:

1. Знание топологии инфраструктуры
2. Наличие опыта работы с облачными хранилищами

3. Наличие опыта работы с СУБД PostgreSQL, СУБД Redis
4. Администрирование ОС Windows и/или UNIX, MacOS
5. Наличие опыта по установке и настройке iOS/Android приложений
6. Наличие опыта администрирования Linux серверов
7. Наличие опыта работы с Ansible

#### 4.1 Доступ

- root-доступ к серверу
- установка Python устанавливается на сервер



Большинство дистрибутивов устанавливают Python по умолчанию, но некоторые этого не поддерживают (например, Ubuntu 18.04) и требуют ручной установки (например, `apt-get install python 3`). В некоторых дистрибутивах Ansible может неправильно определить версию Python (2 против 3), и может потребоваться явно указать путь интерпретатора в инвентаре/хостах во время установки (например, `ansible_python_interpreter=/usr/bin/python3`).

- установка программы Ansible
- веб-сервер с поддержкой HTTPS на базовом доменном имени (<ваш-домен>), способный обслуживать статические файлы. Если вы не решите обслуживать базовый домен с сервера Bond или, альтернативно, использовать записи DNS SRV для делегирования сервера.
- настройка записи DNS для <ваш-домен> (более подробно описано в разделе «Настройка DNS»).

#### 4.2 Порты

Необходимо открыть следующие сетевые порты TCP/UDP, представленные в таблице 4.



**Таблица 4. Сетевые порты**

№	Порт	Описание
1.	TCP:80	веб-сервер HTTP
2.	TCP:443	веб-сервер HTTPS
3.	TCP:3478	TURN через TCP (используется Coturn)
4.	UDP:3478	TURN через UDP (используется Coturn)
5.	TCP:5349	TURN через TCP (используется Coturn)
6.	UDP:5349	TURN через UDP (используется Coturn)
7.	TCP:8448	HTTPS веб-сервер Bond Federation API. В некоторых случаях это может быть необходимо даже при отключенной федерации.
8.	Диапазон 49152-49172/UDP	TURN через UDP



Серверам интеграции (например, Dimension) и серверам идентификации (например, malsd) может потребоваться доступ к API openid на порте федерации.

## 5 Развёртывание и настройка сервера

Сервер мессенджера обеспечивает инфраструктуру для централизованного взаимодействия с клиентами на мобильных устройствах и рабочих станциях. Развертывание и настройка сервера мессенджера осуществляется в инфраструктуре Заказчика.

### 5.1 Настройка вашего DNS-сервера

Для настройки работы BOND в своем домене, необходимо выполнить настройку DNS-сервера. Для этого нужно указать подсети, в которой находится сервис BOND, что сервисы BOND для <ваш-домена> делегированы на bond.<ваш-домен>.

Делегирование можно выполнить следующими способами:

- с помощью файла `https://<ваш-домен>/.well-known/matrix/server`
- с помощью записи DNS SRV `_matrix._tcp` (не идентифицировать ее с записью SRV `_matrix-identity._tcp`, описанной ниже).

Для установки BOND на домен, необходимо настроить DNS, конфигурация DNS представлена в таблице 5.

**Таблица 5. Конфигурация DNS**

№	Тип	Хост	Приоритет	Вес	Порт	Назначение
1.	A	matrix	-	-	-	matrix-server-IP
2.	CNAME	element	-	-	-	matrix.<your-domain>
3.	SRV	_matrix-identity._tcp	10	0	443	matrix.<your-domain>
4.	CNAME	dimension	-	-	-	matrix.<your-domain>
5.	CNAME	jitsi	-	-	-	matrix.<your-domain>
6.	CNAME	stats	-	-	-	matrix.<your-domain>
7.	CNAME	goneb	-	-	-	matrix.<your-domain>
8.	CNAME	signal	-	-	-	matrix.<your-domain>
9.	CNAME	hydrogen	-	-	-	matrix.<your-domain>
10.	CNAME	cinny	-	-	-	matrix.<your-domain>

## 5.2 Настройка поддоменов

Как показано в приведенной выше таблице, необходимо создать 2 поддомена (`bond.<ваш-домен>` и `element.<ваш-домен>`) и направить их оба на IP-адрес вашего нового сервера (запись DNS A или запись CNAME) .

Поддомен `element.<ваш-домен>` может быть необходим для установки, веб-клиента Element.

Поддомен `jitsi.<ваш-домен>` может быть необходим для установки платформы видеоконференций Jitsi.



Установка Jitsi отключена по умолчанию, так как она может быть тяжелой и не является основным обязательным компонентом.

Поддомен `stats.<ваш-домен>` может быть необходим для настройки сервиса сбора и анализа системных логов и показателей производительности Grafana.



Установка Grafana отключена по умолчанию, так как она может быть тяжелой и не является основным обязательным компонентом. Можно установить Prometheus без установки Grafana, для этого также не потребуется поддомен `stats.<ваш-домен>`.

### 5.3 Настройка Ansible

Для настройки системы управления конфигурациями Ansible необходимо

- иметь сервер, на котором будут работать службы Matrix
- настроить записи DNS
- получить исходный код `playbook` на ваш компьютер

После того, как вы скачали архив с Бондом, его нужно распаковать выполнив следующую команду:

```
tar -xvf bond*.tar.gz
```

Далее необходимо перейти в файловую директорию, где расположен BOND и выполнить следующую последовательность шагов:

1. Создать каталог для хранения конфигурации (`mkdir inventory/host_vars/bond.<ваш-домен>`)

2. Скопировать пример файла конфигурации (cp examples/vars.yml inventory/host\_vars/bond.<ваш-домен>/vars.yml)
3. Отредактировать файл конфигурации (inventory/host\_vars/bond.<ваш-домен>/vars.yml).
4. Скопировать пример файла inventory hosts (cp examples/hosts inventory/hosts)
5. Отредактировать файл inventory hosts.

## 5.4 Установка сервисов Бонда

Если вы настроили свой DNS и настроили playbook, вы можете начать процедуру установки.

Запустите эту команду, чтобы установить службы Bond:

```
ansible-playbook -i inventory/hosts setup.yml --tags=setup-all
```

Примечания:

- если не используются ключи SSH для аутентификации, а применяется пароль, то может потребоваться добавить --ask-pass к вышеуказанным (и всем другим) командам Ansible
- если используются ключи SSH для аутентификации и используется пользователь без полномочий root, чтобы стать пользователем root (sudo), то может потребоваться добавить -K (-ask-become-pass) к вышеуказанным (и всем другим) командам Ansible

## 5.5 SSL-сертификаты

Для использования собственных SSL-сертификатов можно использовать следующую конфигурацию

```
matrix_ssl_retrieval_method: manually-managed
```

В рамках данной конфигурации необходимо поместить файлы SSL-сертификата в каталог, указанный matrix\_ssl\_config\_dir\_path (по умолчанию /matrix/ssl/config), соблюдая следующую иерархию:

```
<matrix_ssl_config_dir_path>/live/<domain>/fullchain.pem  
<matrix_ssl_config_dir_path>/live/<domain>/privkey.pem  
<matrix_ssl_config_dir_path>/live/<domain>/chain.pem
```

Здесь <домен> относится к необходимым доменам (обычно это bond.<ваш-домен> и element.<ваш-домен>).

Перед запуском служб рекомендуется выполнить следующие действия:

1. Импорт существующей базы данных SQLite (из другой установки Synapse) (необязательно)
2. Импорт существующей базы данных Postgres (из другой установки) (необязательно)
3. Импорт файлов данных media\_store из существующей установки Synapse (необязательно)

## 5.6 Запуск служб

Для запуска служб необходимо выполнить следующую команду:

```
ansible-playbook -i inventory/hosts setup.yml --tags=start
```

Далее необходимо завершить процесс установки настроив обнаружение служб через сервис дискаверинга посредством .well-known.

После того, как вы запустили службы и завершили процесс настройки сервиса дискаверинга посредством .well-known необходимо проверить работоспособность сервисов и создать учетную запись в BOND.

## 5.7 Регистрация пользователя

Для регистрации пользователя необходимо выполнить следующую команду:

```
ansible-playbook -i inventory/hosts setup.yml --extra-vars='username=<your-username> password=<your-password> admin=<yes|no>' --tags=register-user
```



Обязательно необходимо отредактировать <your-username> и <your-password>

Для создания других пользователей необходимо перейти в следующую директорию:

```
bond.<ваш-домен>/synapse-admin
```

## 5.8 Пример конфигурационного файла

```
#Пример значения: example.com
matrix_domain: avsw.ru
matrix_server_fqn_matrix: "bond.{{ matrix_domain }}"
#Пример значения: someone@example.com
matrix_ssl_lets_encrypt_support_email: 'user@mail'
#A shared secret (between Coturn and Synapse) used for
authentication.
#Можно поместить сюда любую строку, но предпочтительнее
сгенерировать строгую строку (например, `pwgen -s 64 1`).
matrix_coturn_turn_static_auth_secret: 'secret key'
#Уникальный ключ, используемый для защиты ключей доступа,
выдаваемых сервером.
#Можно поместить сюда любую строку, но предпочтительнее
сгенерировать строгую строку (например, `pwgen -s 64 1`).
matrix_synapse_macaroon_secret_key: 'secret key'
```

#Ключ (токен авторизации), выдаваемый сервером и подписанный им `matrix\_homeserver\_generic\_secret\_key`.

matrix\_homeserver\_generic\_secret\_key:

"{{ matrix\_synapse\_macaroon\_secret\_key }}"

matrix\_synapse\_workers\_container\_host\_bind\_address: '0.0.0.0'

#Пароль Postgres для использования суперпользователем Postgres.

# Playbook создает дополнительных пользователей и базы данных Postgres (по одному для каждой включенной службы)

#Используется учетная запись суперпользователя

matrix\_postgres\_connection\_password: 'password'

#ssl

matrix\_ssl\_retrieval\_method: manually-managed

matrix\_coturn\_tls\_enabled: false

matrix\_coturn\_turn\_external\_ip\_address: 'external ip'

#Контролирует, предоставляет ли контейнер matrix-synapse-admin свой HTTP-порт

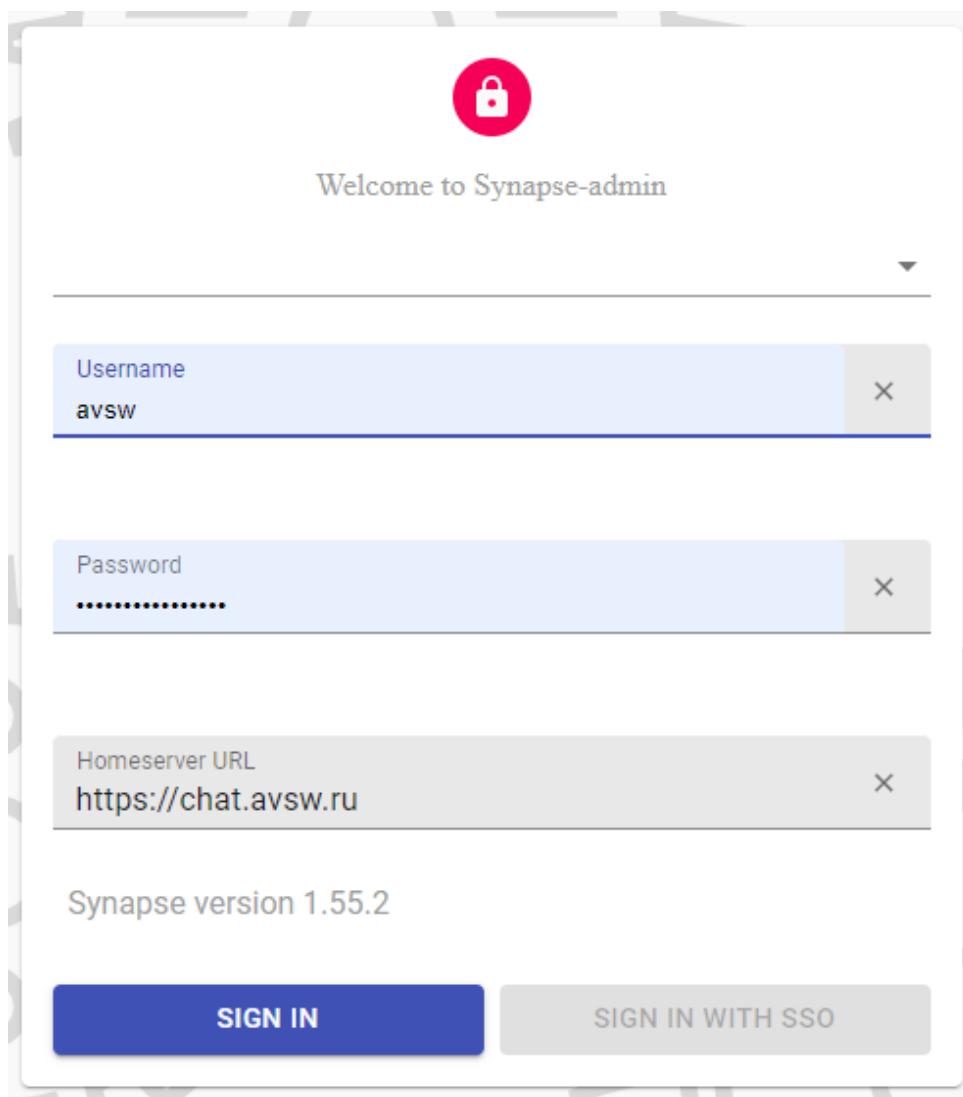
matrix\_synapse\_admin\_enabled: true

matrix\_mal\_sd\_enabled: true

## 6 Панель администратора

Для корректной работы панели администратора необходимо, чтобы она имела сетевой доступ к серверу BOND. Резервное копирование реализуется на стороне Заказчика. Административная панель локально хранит данные пользователей. В случае, если авторизацию для административной панели настраивают специалисты «АВ СОФТ», то нужно сохранить логин и пароль для доступа администратора. Логин, пароль администратора по умолчанию предоставляет разработчик программного обеспечения.

Доступ к панели администратора осуществляется с помощью веб-браузера. Для входа в админ-панель в адресной строке браузера указываем адрес сервера с путём «<https://chat.avsw.ru/synapse-admin/#/login>». Далее необходимо ввести учетные данные и URL и нажать «SIGN IN» (Рисунок 2).



Username  
avsw

Password  
.....

Homeserver URL  
<https://chat.avsw.ru>

Synapse version 1.55.2

**SIGN IN** SIGN IN WITH SSO

Рисунок 2. Авторизация администратора



После успешного прохождения авторизации отобразится страница «Users» - Пользователи (Рисунок 3).

<input type="checkbox"/>	Avatar	User-ID ↑	Displayname	Guest	Server Administrator	Deactivated	Creation timestamp
<input type="checkbox"/>		@avsw.avsw.ru	avsw	×	✓	×	31.03.2022, 12:37:43
<input type="checkbox"/>		@test5.avsw.ru	Test5	×	×	×	31.03.2022, 12:38:23
<input type="checkbox"/>		@test6.avsw.ru	Test6	×	×	×	31.03.2022, 12:38:45
<input type="checkbox"/>		@test7.avsw.ru	Test7	×	×	×	31.03.2022, 12:39:03
<input type="checkbox"/>		@test8.avsw.ru	Test8	×	×	×	31.03.2022, 12:39:23

**Рисунок 3. Страница «Users» - «Пользователи»**

Для создания нового пользователя необходимо нажать кнопку «Create» и она отобразит форму для заполнения данных по новому пользователю (Рисунок 4).

User-ID \*

Displayname

Password

☐ Server Administrator

3PIDs

SSO

**Рисунок 4. Добавление нового пользователя**

После заполнения всех данных необходимо нажать кнопку «SAVE» и удостовериться, что новый пользователь отобразился в общей таблице.

Пример:

User-ID: <имя>-<число>:avsw.ru

Displayname: <имя>-<число>

Password: <имя>

Если перейти во вкладку «Rooms» - Комнаты, то в ней отобразятся чаты, которые можно гибко создавать между несколькими серверами (Рисунок 5).

<input type="checkbox"/>		Name ↑	Members	Visible in room directory
<input type="checkbox"/>		Пуб. К1	3	×
<input type="checkbox"/>		приватное пространство	1	×
<input type="checkbox"/>		публ. прост	2	×
<input type="checkbox"/>		IRqXqTjwwNZmxuOesKt:avsw.ru	2	×
<input type="checkbox"/>		IjyuSuoCJrVryJxWroR:avsw.ru	2	×
<input type="checkbox"/>		IqPUeEBCyKtYEJPhhZP:avsw.ru	2	×
<input type="checkbox"/>		ITVJoEuxCdKILLqZsYn:avsw.ru	2	×

**Рисунок 5. Вкладка «Rooms» - Комнаты**

В рамках технической поддержки в случае выявления каких-либо проблем в работе админ-панели необходимо сообщить об этом факте одним из способов (в порядке уменьшения приоритета):

- На адрес электронной почты office@avsw.ru;
- Позвонив по телефону: +7(495)988-92-25.