



Сервер QUIK

Инструкция по установке

Версия 16.2

2026



Содержание

1. Общие сведения.....	4
1.1 Компоненты системы QUIK	4
1.2 Контроль лицензий на серверах QUIK.....	5
2. Установка и настройка сервера	6
2.1 Технические требования.....	6
2.2 Рекомендации по подготовке платформы	6
2.3 Установка на Windows	7
2.4 Установка на Linux	9
2.5 Настройка сервера	19
2.6 Миграция сервера с Windows на Linux.....	43
2.7 Удаление сервера.....	51
2.8 Установка и настройка QUIK Administrator	53
2.9 Настройка баннера Рабочего места QUIK	79
2.10 Настройка вывода сообщений	81
2.11 Настройка пересылки файлов	82
2.12 Настройка отправки произвольных файлов	82
3. Запуск сервера QUIK	84
3.1 Ключи запуска сервера QUIK	84
4. Шифрование паролей.....	88
5. Приложение.....	89
5.1 Формат позиций	89
5.2 Правила преобразования ini-файлов при миграции ПО с ОС Windows на ОС Linux	91
5.3 Настройка Сервера QUIK для аутентификации в домене Active Directory / Kerberos	93
5.4 Настройка OpenSSL	98
5.5 Настройка MultiPurpose	104
5.6 Настройка КриптоПро	118



5.7	Настройка Сигнал-КОМ.....	128
5.8	Хранимая процедура для стоп-заявок.....	138
5.9	Перенос стоп-заявок	138
5.10	Регламент ежедневного обслуживания сервера QUIK.....	140
5.11	Список кодов ошибок сервера QUIK	146

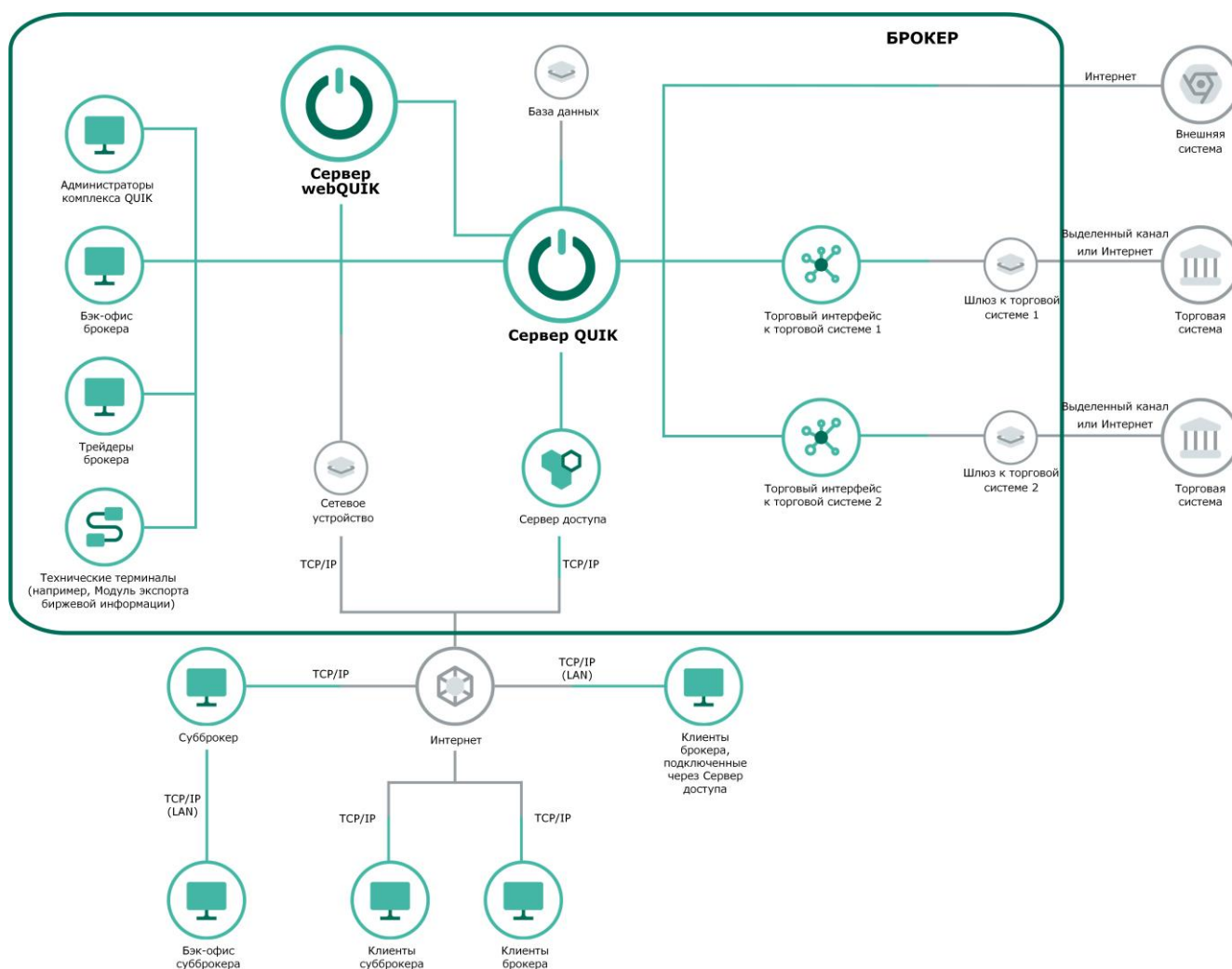
Ваши пожелания и комментарии к данной Инструкции направляйте по электронной почте на адрес: quiksupport@argatech.com



1. Общие сведения

1.1 Компоненты системы QUIK

Программный комплекс QUIK реализован по технологии «клиент-сервер». Обмен данными между сервером и пользовательскими терминалами осуществляется посредством сети интернет и/или локальной сети. Сервер обеспечивает подключение источников информации (торговых систем, потоков новостей и пр.) и обработку поручений клиентов. Клиентские приложения предназначены для отображения информации и ввода поручений клиентов.



Центральное звено программного комплекса – **сервер QUIK**, имеющий логическое ядро и **интерфейсы** к подключаемым элементам (биржевым интерфейсам и другим источникам информации, хранилищу данных). Модульный принцип подключения позволяет наращивать возможности системы по мере необходимости, дополняя базовую конфигурацию новыми функциями.



Взаимодействие с **базой данных** реализовано через специальный интерфейс для упрощения смены используемого типа СУБД. База данных используется для хранения информации со сроком хранения более одного дня – регистрационных данных пользователей и прав на работу с системой, а также журналов совершенных операций.

Информация, поступающая из биржевых торговых систем, обрабатывается в оперативной памяти и в базу данных не заносится. Для быстрого восстановления работоспособности в случае сбоя используется кеширование полученных данных на диске в виде бинарных файлов. Работа с СУБД осуществляется через специализированный сервер базы данных.

Сервер доступа соединяется с основным сервером QUIK, получает от него информацию и распределяет ее между пользователями в соответствии с их правами. Сервер доступа применяется для решения задачи обслуживания большого количества пользовательских подключений, так как позволяет снизить нагрузку на основной сервер системы.

Администрирование комплекса осуществляется в программе **QUIK Administrator**, объединяющей все настройки, используемые логическим ядром сервера. Для наблюдения за состоянием сервера и подключений клиентов используется терминал **QMonitor**.

1.2 Контроль лицензий на серверах QUIK

Лицензия предоставляет право на подключение одного экземпляра приложения (плагина, технологического или клиентского модуля) к серверу QUIK. Приложения одного типа объединены в пул лицензий.

При использовании Брокером нескольких серверов QUIK контролируется общее количество лицензий в рамках пула лицензий, распределенное между ними с помощью сервиса синхронизации данных (программа Репликатор).

При исчерпании максимального количества лицензий выводится соответствующая диагностика в лог-файл сервера. При отсутствии лицензии на плагин в Рабочем месте клиента появляется сообщение «Недостаточно лицензий!».

Приложения, для которых поддерживается контроль лицензий:

- Q2Q adapter;
- Программный интерфейс FIX adapter (счета);
- Программный интерфейс FIX adapter (транзакции);
- Программный интерфейс FIX Drop Copy;
- Программный интерфейс FIX Client Connector;
- Модуль экспорта биржевой информации;
- Модуль экспорта очередей заявок;
- Рабочее место QUIK для мобильных устройств «PocketQUIK»;
- Терминальный модуль риск-менеджера «Colibri SM»;
- Терминальный модуль риск-менеджера «Colibri FM»;
- Терминальный модуль риск-менеджера «Colibri FX»;



- Специализированное рабочее место мультиброкерского обслуживания;
- FX Convertor;
- Модуль BasketTrading;
- Модуль опционной аналитики;
- Терминальный модуль доверительного управляющего «TrustManager»;
- Рабочее место webQUIK;
- QORT2QUIK adapter;
- Программный интерфейс управления позициями.

2. Установка и настройка сервера

2.1 Технические требования

На официальном [сайте QUIK](#) можно ознакомиться с таблицей требований к оборудованию и программному обеспечению:

- Сервера QUIK;
- Торговых интерфейсов;
- Информационных интерфейсов;
- Сервисных модулей;
- Рабочего места администратора QUIK Administrator;
- Рабочего места мониторинга QMonitor;
- Других интерфейсов и модулей к другим биржам.

Требования, представленные на сайте, являются минимальными. Рекомендуется согласовать технические требования со Службой технической поддержки QUIK, например, если предполагается:

- Обслуживание большого количества пользователей;
- Подключение большого количества интерфейсов;
- Использование сервера QUIK для решения маркет-мейкерских задач или для высокочастотного трейдинга.

2.2 Рекомендации по подготовке платформы

На компьютерах с серверным ПО QUIK не рекомендуется использование любого системного ПО, которое в режиме реального времени или с некоторой периодичностью анализирует данные на диске, данные, передаваемые по сети и прочее. К такому ПО можно отнести, например, антивирусы. Его работа может вызвать заметные проблемы с производительностью системы QUIK.



2.3 Установка на Windows

2.3.1 Копирование файлов

1. Создайте каталог для установки системы QUIK (в дальнейшем <quik_dir>).
2. Скопируйте в него каталоги keygen и server из дистрибутива с файлами для установки (<inst_dir>).
3. Скопируйте каталог <inst_dir>/front в директорию, которая предназначена для хранения актуального дистрибутива Рабочего места QUIK (см. [настройку дистрибутива для пользователей](#)).
4. В произвольную директорию скопируйте каталог <inst_dir>/qadminsrv, который содержит файлы, необходимые для [установки QUIK Administrator](#).

2.3.2 Подготовка к установке

Создание ключа для сервера QUIK

С помощью программы **KeyGen** сформируйте публичный и секретный ключи, которые в дальнейшем будут использоваться сервером QUIK (см. файл keygen.pdf – руководство по использованию программы keygen.exe).

1. В качестве параметра «Имя владельца ключа» укажите наименование организации в формате <Название (идентификатор)>, например:

```
Тест-Инвест (testinvest)
```

2. Идентификатор в круглых скобках будет в дальнейшем использоваться для настройки системы (далее <имя_сервера_quik>).
3. Запомните введенный пароль для защиты ключа (далее <пароль_ключа_сервера>).
4. Скопируйте секретный ключ сервера (по умолчанию программа keygen.exe сохраняет файл a:\secring.txk) в каталог <quik_dir>\server. Для удобства в дальнейшей работе переименуйте его в secrserv.txk.
5. Скопируйте публичный ключ сервера (по умолчанию программа keygen.exe создает файл a:\pubring.txk) в каталог <quik_dir>\keygen. Для удобства в дальнейшей работе переименуйте его в <имя_сервера_quik>.txk. Этот ключ будет использоваться всеми пользователями сервера вместе с пакетом программ **KeyGen**.
6. Откройте для редактирования файл <quik_dir>\keygen\qcrypto.cfg. Укажите в качестве параметров:
 - «IMPORT» – идентификатор организации;
 - «Import Keys» – имена ключей прикладных систем, которые будут добавляться к публичному ключу.



Пример:

```
IMPORT=<имя_сервера_QUIK>  
Import Keys=Тест-Инвест (testinvest)
```

7. С помощью программы **KeyGen** создайте публичный и секретный ключи для пользователя сервера QUIK (см. файл keygen.pdf – руководство по использованию программы keygen.exe). На шаге 3 программа предложит выбрать файл с публичным ключом системы – выберите файл <имя_сервера_quik>.txk. В списке ключей выберите публичный ключ сервера (в нашем примере это «Тест-Инвест (testinvest)»). Включите флажок «Записать и использовать, пропуская этот шаг» – в дальнейшем это позволит вашим пользователям при формировании ключа избежать лишней операции.

Установка ODBC-драйверов для работы сервера с БД

Установка ODBC-драйверов на MS Windows

Для получения набора установленных на компьютере ODBC-драйверов необходимо в меню Windows набрать в поиске текст «Источники данных ODBC» и открыть соответствующее окно.

Если на вкладке «Драйверы» в списке присутствует строка с именем необходимого драйвера, значит он установлен, и устанавливать его не требуется.

Если строка с именем драйвера отсутствует, то необходимо скачать его и установить.

Сервером поддерживаются следующие драйверы:

- При работе с MS SQL:
 - _ ODBC Driver 17 for SQL Server
Ссылка для скачивания установочного файла драйвера с официального сайта Microsoft: <https://go.microsoft.com/fwlink/?linkid=2223304>
- При работе с PostgreSQL:
 - _ PostgreSQL ANSI(x64)
Ссылка для скачивания установочного файла драйвера с официального сайта ARQA Technologies:
https://flex.quik.ru:8080/web/client/files?path=/Common/Lib/odbc_pg_win_13.2.0.zip

2.3.3 Регистрация в службах Windows

1. Установите сервер QUIK и интерфейс к торговой системе как службы. Для этого наберите в командной строке:

```
<quik_dir>\server\quik.exe -install
```



2. Откройте `controlpanel\services` и посмотрите, есть ли в списке сервисов записи, идентифицирующие сервер QUIK (по умолчанию: «Quik Server»).
3. Создайте пользователя-администратора, присвоив ему имя (например, `<quikserv>`) и пароль (например, `<passwd>`).
4. Для использования доменной аутентификации на сервере MS SQL укажите в параметрах запуска сервисов имя доменного пользователя и его пароль.

2.4 Установка на Linux

2.4.1 Пользователи для работы с сервисами под Linux

Для работы и управления сервисом применяются следующие пользователи:

- Администратор платформы.

Для обозначения этого пользователя используется имя `root`. Это пользователь, который знает пароль `root` либо добавлен в группу `root`, либо имеет доступ к широкому кругу команд на выполнение от имени `root` через утилиту `sudo`.

Пользователю доступна установка и удаление, а также администрирование сервиса: обновление, запуск и остановка.

- Пользователь, от имени которого работает сервис.

Для обозначения этого пользователя используется имя `arqasrv`. При установке сервиса по умолчанию создается пользователь именно с таким именем.

Пользователю также доступно администрирование сервиса: обновление, запуск и остановка – применяется, если выполнение администрирования пользователем `root` недоступно.

Таким образом, сервис всегда работает от имени пользователя `arqasrv`. Установка и удаление сервиса может производиться только пользователем `root`. Администрирование сервиса может производиться пользователями `root` или `arqasrv`.

2.4.2 Подготовка к установке

Установите на компьютер приведенные ниже пакеты в соответствии с операционной системой, на которой будет работать сервер.

Дополнительные пакеты для Astra Linux

1. Выполните команду обновления списка пакетов:

```
sudo apt-get update
```



2. Выполните команду установки пакетов jemalloc2:

```
sudo apt install libjemalloc2
```

3. Выполните команды установки пакетов libodbc1 и unixodbc:

```
sudo apt install libodbc1  
sudo apt install unixodbc
```

Дополнительные пакеты для Red OS

1. Выполните команду обновления списка пакетов:

```
sudo dnf check-update
```

2. Выполните команду установки пакетов jemalloc:

```
sudo dnf install jemalloc.x86_64
```

3. Выполните команду установки пакетов unixodbc:

```
sudo dnf install unixODBC.x86_64
```

Установка ODBC-драйверов для работы сервера с БД

Установка ODBC-драйверов на Linux

Для получения набора установленных на компьютере ODBC-драйверов необходимо выполнить команду:

```
cat /etc/odbcinst.ini|grep "^\[.*\]$"
```

Если в результате выполнения команды отобразится строка с именем необходимого драйвера, значит он установлен, и устанавливать его не требуется.

Если строка с именем драйвера отсутствует, то необходимо скачать его и установить.

Сервером поддерживается работа только с драйвером PostgreSQL:

- PostgreSQL ANSI (Для Astra Linux)
- PostgreSQL (Для RED OS)



- При работе на Astra Linux 1.7:

Ссылки для скачивания установочных пакетов с официального сайта ARQA Technologies:
https://flex.quik.ru:8080/web/client/files?path=/Common/Lib/odbc_pg_linux_16.0.5.zip.

Для установки пакетов распакуйте архив на компьютере, на котором будет работать сервис, и выполните следующие команды:

```
sudo dpkg -i libpq5_16.3-1.pgdg100+1_amd64.deb
sudo dpkg -i odbc-postgresql_16.00.0005-1.pgdg100+1_amd64.deb
```

- При работе на Astra Linux 1.8:

Выполните команды:

```
sudo apt install libpq5
sudo apt install odbc-postgresql
```

- При работе на RED OS 8.0:

— Выполните команду:

```
sudo dnf install postgresql-odbc.x86_64
```

— Добавьте в файл quik.ini настройку:

```
[db]
driver=PostgreSQL
```

После установки повторно выполните команду и убедитесь в наличии имени драйвера в результатах выполнения команды:

```
cat /etc/odbcinst.ini|grep "^\[.*\]$"
```

Убедитесь, что в файле /etc/odbcinst.ini указан соответствующий драйвер:

- Для Astra Linux:

```
[PostgreSQL ANSI]
Description=PostgreSQL ODBC driver (ANSI version)
Driver=psqlodbc.so
Setup=libodbcpsqlS.so
Debug=0
```



```
CommLog=1
UsageCount=1
```

- Для RED OS:

```
[PostgreSQL]
Description = ODBC for PostgreSQL
Driver = /usr/lib/psqlodbcw.so
Setup = /usr/lib/libodbcpsqlS.so
Driver64 = /usr/lib64/psqlodbcw.so
Setup64 = /usr/lib64/libodbcpsqlS.so
FileUsage = 1
```

Если запись не была добавлена, добавьте ее самостоятельно.

2.4.3 Порядок установки

Установка сервиса должна выполняться пользователем root, вызовом run-файла.

По умолчанию все сервисы устанавливаются в директорию /opt/arqasrv, а выполняются от имени системного пользователя arqasrv. Имя сервиса <srvname> для серверов по умолчанию совпадает с именем исполняемого файла – quik.

При установке наименование сервиса задается только строчными буквами.

Все указанные параметры можно переопределить соответствующими ключами запуска run-файла.

Начальные действия по установке сервиса (см. 1 – 5) должны выполняться пользователем root. Для установки выполните следующие действия:

1. Установите на компьютер, на котором будет работать сервис, необходимые пакеты в соответствии с описанием в п. [«Подготовка к установке»](#).
2. Скопируйте файл install_server-xx.xx.xx.run в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (/home/<user> или ~/).
3. Выполните команду добавления права на выполнение run-файлу:

```
chmod +x install_server-xx.xx.xx.run
```



4. Выполните команду установки сервиса:

```
sudo ./install_server-xx.xx.xx.run -i
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя.

В результате выполнения run-файла будут выполнены следующие действия:

- Если системный пользователь `arqasrv` отсутствует, то он создастся с правами по умолчанию и включится в одноименную группу. В качестве домашней директории пользователю установится директория `/opt/arqasrv`. От имени этого пользователя будет работать устанавливаемый сервис.
- В директории `/opt/arqasrv/quik` создается поддиректория с именем `quik`. Это директория установки сервиса, в которую будут распакованы файлы дистрибутива устанавливаемого сервиса.
- Пользователь `arqasrv` назначается владельцем всех файлов и поддиректорий в директории сервиса.
- В системе управления службами `systemd` регистрируется сервис с именем `quik` и запуском от имени системного пользователя `arqasrv`.
- В директории `/etc/arqasrv` создается файл с именем `quik` для фиксации параметров установки сервиса.
- В директории сервиса генерируются следующие командные файлы:
 - `q_start.sh` – запуск сервиса, в том числе с [ключами запуска](#). Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `q_stop.sh` – остановка сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `q_status.sh` – вывод информации о текущем состоянии сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `uninstall.sh` – удаление сервиса. Предназначен для выполнения пользователем `root`;
 - `postmigration.sh` – выполнение дополнительных операций при миграции. Предназначен для выполнения пользователями `arqasrv` и `root`.

При успешной установке сервиса в консоль выводится сообщение:

«Installation of service “quik” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

5. Если управление установленным сервисом предполагается выполнять пользователем `arqasrv`, выполните следующие действия:

- Для предотвращения внесения пользователем `arqasrv` изменений в скрипты управления сервисом, на которые ему будет выдано разрешение выполнения от имени `root`, сделайте их неизменяемыми, выполнив следующие команды:



```
chattr +i /opt/arqasrv/quik/quik/q_start.sh
chattr +i /opt/arqasrv/quik/quik/q_stop.sh
```

- Выдайте пользователю arqasrv права на выполнение скриптов управления сервисом от имени root, выполнив следующие действия:

- Выполните команду:

```
sudo visudo
```

- В открывшемся vi-подобном редакторе добавьте строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/quik/q_start.sh,
/opt/arqasrv/quik/quik/q_stop.sh
```

Эта строка разрешает пользователю arqasrv выполнять перечисленные скрипты на текущем компьютере от имени root.

Дальнейшие действия могут выполняться пользователем arqasrv или root.

6. Проверьте, что в файле qcrypto.cfg сервера указаны следующие параметры:

```
SECRING=secrserv.txk
PUBRING=quik.dwq

[auth]
sign=libsecprov.so
look=qcrypto.cfg,db_look

[db_look]
do=_QXKeyDB
use=libdwqx.so

[CryptoProviders]
placebo=1

[placebo]
Module=libplacebo_pr.so
```



7. Следующие действия необходимо выполнить, если в каталоге сервиса отсутствуют актуальные конфигурационные файлы quik.ini и qcrypto.cfg:

- Сформируйте минимальные конфигурационные файлы quik.ini и qcrypto.cfg для работы сервера на основе шаблонов quik.ini.tpl и qcrypto.cfg.tpl, которые после установки находятся в каталоге сервиса.
- Переименуйте шаблоны, выполнив команды:

```
[sudo] cp quik.ini.tpl quik.ini
[sudo] cp qcrypto.cfg.tpl qcrypto.cfg
```

Указание sudo требуется в случае выполнения команды пользователем root.

- Убедитесь, что полученные файлы имеют кодировку win1251.
- Заполните секции с настройками в файле quik.ini:
- В секции [ctl_module] укажите порт для подключения программы QMonitor к серверу, наименование ключа сервера и пароль этого ключа.

```
[ctl_module]
module=libdwwqctl.so
port=15121
name=broker
password=
```

- В секции [data_ip_module] укажите порт для подключения интерфейсов к серверу.

```
[data_ip_module]
module=libdwtwipsrv.so
port=17100
```

- В секции [db] укажите имя или IP-адрес сервера СУБД, имя базы данных сервера, пользователя, от имени которого происходит подключение к СУБД, и пароль этого пользователя.

```
[db]
server=
base=
user=
password=
```



При соединении с СУБД Postgres с использованием порта, отличного от заданного по умолчанию (5432), его необходимо указать в параметре AdditionalParameters:

```
AdditionalParameters=port=5431
```

- В секции [dealer-library] укажите путь до настроек всех Библиотек расчета лимитов. Если в текущем файле настроек указаны пути с расширением .dll, то замените расширение на .ini.

```
[dealer-library]
ALGO=./dealer/algo.ini
SMS=./dealer/sms.ini
```

- В секции [usend_module] укажите системное имя, порт для подключения пользователей к серверу, наименование ключа сервера и пароль этого ключа.

```
[usend_module]
module=libdwsend.so
sysname=Информационно-торговая система QUIK "broker"
name=broker
password=
port=15100
```

- Если настроена репликация, то в секции [stop_sync] укажите идентификатор сервера.

```
[stop_sync]
serverid="ID_SERV1"
```

- Создайте файл crossrate.ini, (секция [cur_module]) содержащий описания валют, используемых на сервере:

```
[cur_module]
class_cfg=crossrate.ini
```

- Минимальное описание валют в файле crossrate.ini:

```
[crossrate]
RUR=Рубль, Рубль, 3
```



```
[crossrate_rate]
RUR=1
```

- Для корректного отображения наименования валюты, например, в Рабочем месте QUIK, файл crossrate.ini должен быть сохранен в кодировке win1251.

8. Для сервиса, установленного по умолчанию, произведите первый запуск с ключом -clean из директории с установленным сервисом, запустив команду:

```
sudo ./q_start.sh -clean
```

либо из любой директории, отличной от директории сервиса, запуском команды:

```
sudo /opt/arqasrv/quik/quik/q_start.sh -clean
```

9. Настройте автоматику запуска и остановки сервиса. Для этого используйте в скриптах автоматики запуск командных файлов q_start.sh и q_stop.sh, расположенных в директории установленного сервиса.

Сервер необходимо перезапускать ежедневно. Запуск должен производиться за 3-5 минут до запуска первого интерфейса. Остановку сервера необходимо производить через 3-5 минут после остановки интерфейсов.

Структура каталогов имеет значение. Перемещение или переименование файлов сервиса может привести к ошибке в установке.

2.4.4 Ключи запуска установочного gun-пакета под Linux

Поставляемый в дистрибутиве gun-файл поддерживает следующие ключи запуска:

-i [<srvname>]

Выполнение с данным ключом доступно только пользователю root.

Установка сервиса с именем <srvname>. Параметр <srvname> необязателен. При отсутствии используется имя сервиса по умолчанию, равное имени исполняемого файла устанавливаемого ПО. При указании параметра пользователем, его значение приводится к нижнему регистру, и сервис устанавливается с именем в нижнем регистре.

Установка двух одноименных сервисов не допускается, даже в разные корневые директории. При попытке это сделать установка будет завершаться ошибкой.



-d <rootdir>

Ключ запуска, применяемый только при установке сервиса (в комбинации с -i) для указания корневой директории для установки сервиса, отличной от директории по умолчанию /opt/arqasrv. Это директория, в которой создается поддиректория <softwaredir>/<srvname>, в которую будут распакованы бинарные и конфигурационные файлы устанавливаемого ПО.

-n <srvusername>

Ключ запуска, применяемый только при установке сервиса (в комбинации с -i) для указания пользователя <srvusername>, который станет владельцем файлов сервиса и от имени которого будет работать устанавливаемый сервис. Имя пользователя по умолчанию: arqasrv.

-u [<srvname>]

Выполнение с данным ключом доступно пользователям arqasrv или root.

Обновление сервиса с именем <srvname>. Параметр <srvname> необязателен. При отсутствии используется имя сервиса по умолчанию, равное имени исполняемого файла ПО.

Расположение сервиса и имя пользователя-владельца сервера указывать не требуется, т.к. оно сохранено в /etc/arqasrv/<srvname>.

-e

Выполнение с данным ключом доступно любому пользователю.

Распаковка полного содержимого архива, включая конфигурационные ini-файлы. Распаковка производится в поддиректорию с именем, равным имени run-файла (без расширения .run), которая в случае отсутствия создается рядом с исполняемым файлом.

-h, -?

Выполнение с этим ключом доступно любому пользователю.

Вывод краткой информации об аргументах запуска.

Примеры:

Запуск run-файла для установки сервиса:

```
sudo ./install_server-xx.xx.xx.run -i quikserver -d /opt/customdir
```

Запуск run-файла для обновления сервиса:

```
[sudo] ./install_server-xx.xx.xx.run -u quikserver
```

Указание sudo требуется в случае обновления сервиса пользователем root.



Запуск run-файла для распаковки:

```
./install_server-xx.xx.xx.run -e
```

2.5 Настройка сервера

2.5.1 Настройка параметров валют и кросс-курсов

1. На компьютере, на котором запущен сервер QUIK, откройте файл quik.ini в директории quik\server и отредактируйте его следующим образом:

- в секцию [natural_level_section] добавьте строку (если она отсутствует):

```
module=cur_module
```

- в конец файла quik.ini добавьте строки:

```
[cur_module]
module=dwcurg.dll
class_cfg=crossrate.ini
```

2. Откройте файл crossrate.ini в директории quik\server и отредактируйте его следующим образом:

- в секции [crossrate] для каждого кода валюты укажите:
 - полное наименование валюты;
 - сокращенное наименование валюты;
 - точность кросс-курса;
 - точность ведения денежной позиции. Возможные значения: в диапазоне [0, 8]. Если значение не задано явно, по умолчанию устанавливается «2».

Пример:

```
[crossrate]
...
RUR=Рубль, Рубль, 2
SUR=Рубль, Рубль, 2
JPY=Японская иена, Иена, 6, 0
```



ВАЖНО!

Если точность ведения денежной позиции по валюте отлична от «2», все подключаемые к серверу интерфейсы, которые транслируют:

- данную валюту;
- инструменты, которые торгуются за эту валюту;
- валютные пары, содержащие данную валюту;
- любые денежные величины, выраженные в данной валюте;

должны поддерживать трансляцию денежных величин с точностью, отличной от «2», а точность для соответствующей валюты должна совпадать с настроенной на сервере QUIK. В противном случае корректная работа системы не гарантируется.

За информацией о поддержке трансляции денежных величин с точностью, отличной от «2», для конкретного торгового интерфейса обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

- в секции [crossrate_rate] укажите курс конвертации для каждой валюты. Значение курса может быть произвольным числом, содержащим количество знаков после запятой не больше значения параметра «точность кросс-курса», заданного в секции [crossrate] (см. выше).

Пример:

```
[crossrate_rate]
RUR=1
SUR=1.00
JPY=0.627686
```

При необходимости использовать кросс-курс для валюты, отсутствующей в секции [crossrate_rate], в программе QMonitor отобразится соответствующее сообщение об ошибке.

- в секции [main_currency] укажите:
 - код валюты. Значение по умолчанию: «RUR».
 - код символа валюты в стандарте Unicode. Значение по умолчанию: «0».

Коды валют доступны по ссылке:

www.unicode.org/charts/nameslist/n_20A0.html

- строку с HTML-кодом символа валюты в формате <Unicode-код валюты>. Если код указывается в 16-ричной системе, то перед ним необходимо указать символ «х». Значение по умолчанию: «» (пусто).



Пример:

```
[main_currency]
code=RUB
ucode=20BD
htmlcode=8381
```

2.5.2 Настройка параметров сервера QUIK

Настройка параметров сервера QUIK выполняется в следующих файлах:

- [crypto.cfg](#);
- [quik.ini](#);
- [trade_dates.ini](#);
- [settlement_dates.ini](#).

Файл `crypto.cfg`

Откройте файл `crypto.cfg` в каталоге `<quik_dir>\server\` и отредактируйте его следующим образом:

1. В секции `[CryptoProviders]` задайте используемые методы шифрования («0» – выключен, «1» – включен), например:

```
[CryptoProviders]
openssl=1
```

2. В секции, соответствующей выбранному на предыдущем шаге методу шифрования, укажите полный или относительный пути к исполняемому и конфигурационному файлам, например:

```
[openssl]
Module=openssl_pr.dll
IniFile=openssl_pr.ini
```

3. В секции `[auth]` задайте следующие настройки:

```
[auth]
sign=secprov.dll
(для Linux задайте sign=libsecprov.so)
sign_provider=openssl ; метод шифрования, используемый для ЭЦП
```



Для использования механизма аутентификации в домене Active Directory / Kerberos требуется задать следующие настройки:

```
[auth]
ad_use=1
AD_PROVIDER_LIBRARY=ad_provider.dll
(для Linux задайте AD_PROVIDER_LIBRARY=libad_provider.so)
```

И указать следующие настройки:

- **AD_DCDistinguishedName** – имя контроллера домена. Значение по умолчанию: «» (пусто).
- **AD_DomainName** – имя домена для SSO. Значение по умолчанию: «» (пусто).
 - Для Windows указывается часть домена до «\», например, «arqa».
 - Для Linux указывается часть домена после «@», например, «ARQA.RU».

При использовании нескольких доменов AD, между которыми настроены доверительные отношения, необходимо их указывать через запятую:

```
[auth]
AD_DomainName=first.com, second.com
или, для Linux:
AD_DomainName=FIRST.COM, SECOND.COM
```

При проверке логина используются домены по списку в указанном порядке.

Например, для пользователя user выполняется проверка first.com\user, а затем second.com\user. Тот, домен, где проверка прошла, считается корректным.

Если во всех указанных доменах аутентификация завершилась неуспешно, считается, что пользователь не прошел аутентификацию.

Если в обоих доменах есть пользователь с совпадающими логином и паролем, то будет выбран тот, который идет в списке первым.

При этом, если пользователь указывает логин вместе с доменом first.com\user (или user@FIRST.COM для Linux), то проверка выполняется для указанного домена, а домены, указанные в настройке, игнорируются. Тогда результат успешной валидации пользователя (даже в случае успешной аутентификации в домене) зависит от наличия записи с таким логином (выполняется проверка полного соответствия) в программе QUIK Administrator в окне «Логин в другой системе авторизации» (меню **Сервер QUIK / Безопасность / Логин в другой системе авторизации**).

Для корректной настройки аутентификации в домене Active Directory / Kerberos следует выполнить [настройку Сервера QUIK для аутентификации](#).



Файл quik.ini

Файл должен быть в кодировке Windows-1251.

Откройте файл quik.ini в каталоге <quik_dir>\server\ и отредактируйте его следующим образом:

1. В секции [dealer-library] измените следующие параметры:

```
<код_вашей_фирмы_в_торговой_системе>=<относительный путь к файлу настроек>
```

Пример:

```
[dealer-library]
TEST_FIRM=.\dealer\testfirm.ini
```

2. Создайте на SQL-сервере БД для использования сервером QUIK. Для создания БД необходимо:

- Для MS SQL использовать скрипт создания БД full.sql, который входит в дистрибутив;
- Для PostgresPro запустить последовательно командные файлы:
 - Server_create_pg_db_from_windows.cmd;
 - Server_db_fill_windows.cmd.

Для получения актуальных скриптов для создания БД обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

3. В секции [DB] вместо параметра file задайте следующие параметры подключения к базе данных:

- **Server** – имя сервера. Можно указать список серверов БД через запятую. Значение по умолчанию: «QDB1».
- **Base** – имя базы данных. Значение по умолчанию: «QUIK_DB».
- **User** – имя пользователя базы данных.

Пользователь должен быть включен в роль «quik_server» в базе данных сервера QUIK.

- **Password** – пароль пользователя базы данных. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#).



Стоп-заявки пользователей, частично или полностью заблокированных в QUIK Administrator (истек срок доверенности, установлен признак «Блокирован», истек срок доверенности по рынкам), могут также загружаться из базы данных сервера QUIK при старте. Проверка блокировки пользователя и задание периода управляются следующими настройками файла quik.ini:

- **stoporders.load_when_expired_la** – признак загрузки стоп-заявок для пользователей с истекшей общей доверенностью, истекшими доверенностями по рынкам. Возможные значения:
 - «0» (по умолчанию) – стоп-заявки пользователей с истекшей доверенностью не загружаются;
 - «1» – стоп-заявки пользователей с истекшей доверенностью загружаются.
- **stoporders.mark_expired_as_foreign** – признак маркировки стоп-заявок пользователей с истекшей доверенностью признаком «Foreign». Настройка используется, если stoporders.load_when_expired_la=1. Возможные значения:
 - «0» – стоп-заявки пользователей с истекшей доверенностью не маркируются признаком «Foreign»;
 - «1» (по умолчанию) – стоп-заявки пользователей с истекшей доверенностью маркируются признаком «Foreign».
- **stoporders.expired_la_period** – период в днях, за который нужно загружать стоп-заявки по заблокированным пользователям. Значение по умолчанию: «14».
- **db_connect_timeout** – время ожидания соединения сервера QUIK с сервером БД (в секундах). Диапазон допустимых значений: от 1 до 600. Значение по умолчанию: «60».
- **AuthMode** – используемый тип аутентификации на сервере MS SQL. Возможные значения:
 - «login» (по умолчанию) – используются логин и пароль, указанные в параметрах user и password (пароль может быть [зашифрован](#));
 - «domain» – используется доменная аутентификация.

При AuthMode=domain параметры user и password в секции [DB] игнорируются и могут быть не указаны.

- **Driver** – наименование драйвера, используемого для подключения к базе данных сервера QUIK. Возможные значения:
 - «ODBC Driver 17 for SQL Server» (по умолчанию) – используется для работы с MS SQL Server 2014, 2016 или более новой версией СУБД (из списка поддерживаемых). Ссылка для скачивания установочного файла драйвера с официального сайта Microsoft:
<https://go.microsoft.com/fwlink/?linkid=2223304>;
 - «PostgreSQL ANSI(x64)» – используется для работы с PostgresPRO. Ссылка для скачивания установочного файла драйвера с официального сайта ARQA Technologies:



https://flex.quik.ru:8080/web/client/files?path=/Common/Lib/odbc_pg_win_13.2.0.zip.

При работе с MS SQL Server должен быть установлен драйвер ODBC Driver 17 for SQL Server, а при работе с PostgresPRO – драйвер psqIODBC версии не ниже 13.2.

Пример:

```
[DB]
server=<имя SQL-сервера без префикса «tcp:»>,<порт>
Driver=ODBC Driver 17 for SQL Server
AdditionalParameters=MultiSubnetFailover=Yes;Network=dbmssocn
db_connect_timeout=120
```

- **MultiSubnetFailover** – режим подключения к базе данных, который обеспечивает более быстрое обнаружение и подключение к активному серверу группы доступности MS SQL Server Always On. Поддерживается только при работе с MS SQL Server. Возможные значения:
 - «0» (по умолчанию) – режим выключен;
 - «1» – режим включен.
- **AdditionalParameters** – настройка для задания дополнительных параметров подключения к СУБД. Значение по умолчанию: «» (пусто).

При соединении с кластером MS SQL необходимо установить значение настройки **AdditionalParameters=MultiSubnetFailover=Yes** и **Network=dbmssocn**.

```
AdditionalParameters=MultiSubnetFailover=Yes;Network=dbmssocn
```

При соединении с СУБД PostgresPRO с использованием порта, отличного от заданного по умолчанию (5432), его необходимо указать в параметре **AdditionalParameters**:

```
AdditionalParameters=port=5431
```

- **SSLMode** – режим безопасного подключения. Поддерживается только при настройке подключения к СУБД PostgresPRO. Возможные значения:
 - «» (пусто, по умолчанию) – подключение выполняется без шифрования;
 - «require»;



- _ «verify-ca»;
- _ «verify-full»;
- _ «disable»;
- _ «allow»;
- _ «prefer».

Описание режимов безопасного подключения см. на официальном сайте PostgreSQL: www.postgresql.org/docs/current/libpq-ssl.html.

Если параметр не задан, то параметры CertCAFileName, CertFileName, CertPKeyFileName и CertPass игнорируются.

- _ **CertCAFileName** – путь к файлу-контейнеру сертификатов удостоверяющих центров. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertFileName** – путь и наименование файла сертификата безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertPKeyFileName** – путь и наименование файла приватного ключа безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertPass** – пароль для файла приватного ключа безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#).

4. Настройте возможность получения пользователем непрочитанных сообщений за предыдущие торговые дни:

- _ **messages_delivery_period** – количество дней, за которые загружаются сообщения. Значение по умолчанию: «0» (загружаются только сообщения за текущую торговую дату).

5. В секции [db_module] настройте используемый провайдер базы данных:

- _ **driver** – имя исполняемого файла провайдера базы данных. Значение по умолчанию: «» (пусто). Возможные значения:
 - _ При использовании MS SQL – задайте значение «quik_db_ms.dll»;
 - _ При использовании PostgresPRO – задайте значение «quik_db_pg.dll».

Пример секций при подключении к СУБД MS SQL:

```
[DB]
server=MSSQL_SRV
base=QUIK_DB
user=sa
password=пароль
db_connect_timeout=30
AuthMode=login
```



```
Driver=ODBC Driver 17 for SQL Server
AdditionalParameters=MultiSubnetFailover=No;ApplicationIntent=ReadWrite

[db_module]
module=dstubrc.dll
driver=quik_db_ms.dll
```

Пример секций при подключении к СУБД PostgresPRO:

```
[DB]
server=PostgreSQL_SRV
base=QUIK_DB
user=sa
password=пароль
Driver=PostgreSQL ANSI (x64)
SSLMode=verify-full
CertCAFileName=certs/root.crt
CertFileName=certs/user.crt
CertPKeyFileName=certs/user.key
CertPass=secret

[db_module]
module=dstubrc.dll
Driver=quik_db_pg.dll
```

6. В секции [Files] настройте следующие параметры:

- **EventsLogFileName *** – путь и наименование основного лог-файла. Значение по умолчанию: «events.log».
- **ErrorsLogFileName *** – путь и наименование лог-файла ошибок. Значение по умолчанию: «errors.log».
- **DeallibLogFileName *** – путь и наименование лог-файла Библиотеки расчета лимитов. Значение по умолчанию: «deallib.log».
- **DataFilesFolderName **** – путь к файлам данных (файлы с расширением .ik). Значение по умолчанию: «.\».
- **LogFilesFolderName** – путь к лог-файлам (events.log, errors.log, deallib.log, провайдер БД). Значение по умолчанию: «.\».

(*) Если в параметре указано только наименование лог-файла, используется путь, указанный в параметре LogFilesFolderName.

() В DataFilesFolderName указывается путь к папке, в которой будут формироваться и храниться файлы с расширением .ik. Такая папка должна**



быть создана до запуска сервера. При отсутствии данной папки сервер остановится.

7. В секции [usend_module] измените следующие параметры:

- _ Module – задает соответствие загружаемой библиотеки сервера и секции настроек, относящихся к ней;
- _ Sysname – наименование системы, отображаемое в информационном окне при установлении связи с сервером;
- _ Name – ключ сервера;
- _ Password – пароль для обращения к ключу сервера;
- _ Port – номер порта для подключения пользовательских терминалов;
- _ crypto_provider_ini_file – полный или относительный путь к файлу настроек шифрования;
- _ connection_acceptance_tmo_ms – время ожидания приема нового подключения в миллисекундах. Возможные значения: от 0 до 60000. Значение по умолчанию: «50».

Например:

```
module=dwsend.dll
sysname=Информационно-торговая система QUIK "Тест Инвест"
name=testinvest
password=secret
port=15100
crypto_provider_ini_file=.\openssl_pr.ini
connection_acceptance_tmo_ms=50
```

Если провайдеров несколько, тогда для задания настроек нужно использовать следующие настройки:

- _ «crypto_provider_ini_file_mp» – задание криптопровайдера MP;
- _ «crypto_provider_ini_file_sslpro» – задание криптопровайдера SSL-Pro;
- _ «crypto_provider_ini_file_openssl» – задание криптопровайдера OpenSSL.

Например:

```
[usend_module]
crypto_provider_ini_file_openssl=.\openssl_pr.ini
crypto_provider_ini_file_sslpro=.\signalcom_pr.ini
```



8. В секции [ctl_module] измените следующие параметры:

```
module=dwwqctl.dll
port=15120 ; номер порта для подключения программы QMonitor
name=testinvest ; ключ сервера
password=secret ; пароль для обращения к ключу сервера
```

9. В секции [time-set] укажите параметр hourshift, если время сервера QUIK отличается от времени интерфейса:

```
hourshift=3 ; разница между временем на сервере QUIK и на данных, транслируемых интерфейсом, в часах
```

10. В секции [mail] измените следующие параметры доступа к SMTP-серверу:

```
Server=smtp.quik.ru ; Имя или IP-адрес SMTP-сервера
Port=25000 ; Порт SMTP-сервера. Значение по умолчанию: «25».
User=test_user ; Имя пользователя для аутентификации на SMTP-сервере
Password=secret ; Пароль пользователя для аутентификации на SMTP-сервере. Пароль не должен начинаться с символов «$» и «#». Пароль может быть зашифрован
FromAddress ; Адрес электронной почты, с которого отправляются письма сервера QUIK (например: двухфакторная аутентификация, восстановление пароля, загрузка лимитов и другие)
```

11. В секции [limits_module] настройте параметры:

- для рассылки электронной почты:

```
loadlimits_mail_to=test1@post.ru ; Адреса получателей сообщений через запятую
sign_settings_file=.\\qloadlimitx.ini ; Путь к файлу с настройками Программы для установки позиций клиентов QLoadLimitsX для загрузки сервером QUIK подписанного ЭЦП файла лимитов
```

- **calclimit_old_stoporders** – признак блокировки средств под стоп-заявки предыдущих дней. Возможные значения:
 - «0» (по умолчанию) – не блокировать средства;
 - «1» – блокировать средства.

Пример:

```
calclimit_old_stoporders=0
```



Настройка не должна использоваться совместно с настройкой «Не блокировать средства для стоп-заявок по классам» Библиотеки расчета лимитов (описание настройки см. в Руководстве по администрированию «Настройки Библиотеки расчета лимитов»).

12. В секции [trans_module] настройте параметры:

- **Change_wrong_single_clientcode** – алгоритм замены кода клиента при наличии единственного действующего кода клиента у пользователя. Возможные значения:
 - «0» – транзакция отвергается с диагностикой «Неверный код клиента», если указан код клиента, не совпадающий с правами пользователя (у клиента указан только один код, не совпадающий с правами, либо у клиента указаны два кода, по одному из которых кончился срок доверенности, и в подаваемой транзакции указан код клиента, не совпадающий с правами);
 - «1» (по умолчанию) – транзакция не отвергается.

Пример:

```
change_wrong_single_clientcode=1
```

- **trans_handling_privileged_users** – список пользователей, пре-трейд контроль транзакций которых может производиться параллельно. Рекомендуется включать для технологических пользователей, генерирующих заявки от разных кодов клиента (например, при работе с Модулем алгоритмической торговли, Модулем QUIK SOR и т.д.), для уменьшения задержек обработки транзакций. При включении UID пользователя в настройку, сохраняется гарантия порядка обработки транзакций от одного кода клиента – транзакции обрабатываются в порядке поступления.

Настройки ограничений на количество транзакций в Библиотеке расчета лимитов имеют больший приоритет над настройкой trans_handling_privileged_users. Рекомендуется настраивать такое ограничение, чтобы исключить негативные эффекты в виде задержек обработки данных, получаемых из торговой системы.

Настройка применяется после сохранения файла настроек и не требует перезагрузки сервера.

Формат использования:

```
trans_handling_privileged_users=<список UID через запятую>
```

Пример:



```
trans_handling_privileged_users=100,200,300
```

13.В секции [data_module] настройте параметры:

- **inactive_stops_lifetime** – максимально возможное время в днях от последней активации стоп-заявки, по истечении которого стоп-заявка снимается. Значения от 1 до 13 приводятся к минимально возможному значению – 14.
 - «0» – настройка выключена;
- «14» (по умолчанию) – минимально возможное количество дней (настройка включена).

Пример:

```
inactive_stops_lifetime=14
```

- **news_days_keep** – продолжительность хранения новостей на сервере (в днях). При запуске сервера, новости, срок хранения которых превышает указанное в параметре значение, удаляются из хранилища. Значение по умолчанию: «2».

Если в данной секции включены настройки замены (firm_substitute=1, client_codes_substitute=1), а файлы codes.ini или firms.ini пустые или отсутствуют, работа сервера завершается с ошибкой:

Причина ошибки	Диагностика
Отсутствует файл замен codes.ini	Configuration file «путь-к-codes.ini» not found
Отсутствует файл замен firms.ini	Configuration file «путь-к-firms.ini» not found
Пустой файл замен codes.ini	Configuration file «путь-к-codes.ini» is empty
Пустой файл замен firms.ini	Configuration file «путь-к-firms.ini» is empty

- **generate_holiday_stop_trans** – генерация описания транзакции стоп-заявок для классов, полученных сервером от HolidayTW.
 - «0» (по умолчанию) – настройка выключена;
 - «1» – настройка включена.

14.В секции [Position] задается соответствие между алиасом фирмы (псевдонимом, используемым для замены кода фирмы на любой другой для объединения нескольких фирм в одну в рамках единой денежной позиции) из Торгового интерфейса и кодом фирмы сервера QUIK с настроенной единой денежной позицией (ЕДП). Настройка актуальна, если код фирмы Торгового интерфейса и код ЕДП-фирмы совпадают. Алиас указывается Торговым интерфейсом при трансляции данных по фьючерсным



ограничениям и позициям ЕДП-фирмы. Использование алиаса определяет, для какого вида счета предназначены данные из Торгового интерфейса.

Формат:

```
<алиас ЕДП-фирмы из Торгового интерфейса>=<код ЕДП-фирмы сервера QUIK>
```

Пример:

```
UNIFIED_FIRM=NC0038900000
```

Дополнительная настройка алиаса также требуется в секции [Position] Торгового интерфейса. Длина алиаса не должна превышать 12 символов.

15.Если настроена репликация, то в секции [data_pipe_module] настройте входящую/исходящую репликацию даты/времени последнего логина с помощью настроек:

- **disable_last_login_replication_in** – принимать / не принимать информацию о дате/времени последнего логина от репликатора. Значение по умолчанию: «0» (принимать).
- **disable_last_login_replication_out** – посылать / не посылать информацию о дате/времени последнего логина в репликатор. Значение по умолчанию: «0» (посылать).

16.Если используется внешний Модуль формирования кросс-курсов, то сервер отклоняет подключения других Интерфейсов до соединения с этим Модулем. Чтобы отключить данный режим, в секции [data_pipe_module] используется настройка:

- **WaitforCrossrate** – режим ожидания кросс-курсов. Возможные значения:
 - «0» – отключить режим.
 - «1» (по умолчанию) – включить режим.

Когда сервер использует встроенный Модуль формирования кросс-курсов, значение настройки игнорируется.

В настройках сервиса Q2Q класс CROSSRATE должен быть выделен в секцию отдельного соединения для корректной работы slave-сервера.

Пример:

```
[pt_connect_crossrate]
connection_transport=tcp
server_ip_address=127.0.0.1
```



```
port=17103
check_tmo=150
Classes=|CROSSRATE|
```

- 17.** Выполните настройку двухфакторной аутентификации в соответствии с п. 2 Инструкции по настройке двухфакторной аутентификации QUIK.
- 18.** Выполните настройку запрета ввода длительных заявок, чтобы запрещать или разрешать пользователю вводить в торговую систему заявки со сроком действия «До даты» / «До отмены».
- В секции [gtc-orders] задайте следующие параметры:
 - **markets** – список рынков в произвольном порядке через запятую.
 - Параметры вида **<Рынок>_classes** – классы рынка, который указан в наименовании параметра, в любом порядке через запятую.
 - Параметры вида **<Рынок>_expiration_mark_field** – наименование поля признака экспирации для рынка.
 - Параметры вида **<Рынок>_expiration_date_field** – наименование поля даты экспирации для рынка.

Пустой список рынков или классов в этих рынках означает, что запрет ввода длительных заявок отключен.

- В секции [calc-limits] в параметре **max_days_to_expire_order** задайте максимальный срок действия длительных заявок в днях, который будет действовать на все классы инструментов, перечисленные в параметрах вида **<Рынок>_classes**. Подача заявки, срок действия которой превышает ограничение **max_days_to_expire_order**, прервется с ошибкой.

Например:

```
[calc_limits]
max_days_to_expire_order=<число>

[gtc-orders]
markets=MARKET1, MARKET2
MARKET1_classes=XXXXX,NNNNN
MARKET2_classes=YYYYY,MMMMM
MARKET1_expiration_mark_field=UseExpDate
MARKET1_expiration_date_field=ExpDate
MARKET2_expiration_mark_field=IMMCANCEL
MARKET2_expiration_date_field=EXPIRYDATE
```



Если в программе QUIK Administrator в настройках пользователя установлен флажок «Заявки “До отмены”», значение параметра `max_days_to_expire_order` не повлияет на срок действия заявки.

Если в сервере значение настройки `max_days_to_expire_order` указано больше, чем ограничения, заданные в модуле/интерфейсе (например, Модуль алгоритмической торговли, Торговый интерфейс Срочного рынка Московской Биржи), то модуль/интерфейс отклонит ее.

19. В секции [behavior] можно задать гиперссылку, которая отображается в Рабочем месте QUIK в таблице «Информация об инструменте», для перехода на сайт с подробным описанием инструмента:

- `security.hyperlink` – задает формат гиперссылки. Для создания уникальной гиперссылки для каждого инструмента могут использоваться метасимволы.
- `security.show_hyperlinks` – задает признак, что гиперссылка на описание инструмента отображается в Рабочем месте QUIK в таблице «Информация об инструменте». Возможные значения:
 - «0» (по умолчанию) – не отображается в Рабочем месте QUIK.
 - «1» – отображается в Рабочем месте QUIK.

Пример:

```
[behavior]
security.hyperlink=https://www.moex.com/ru/issue.aspx?code=<SECCODE>
security.show_hyperlinks=1
```

20. В секции [trade_date] задаются следующие параметры:

- **ClearingTime** – время смены сессии на сервере QUIK в формате <ЧЧММСС>. Этот момент времени должен выпадать на период, когда сервер QUIK остановлен. Значение по умолчанию: «000000».
- **no_weekend** – признак работы сервера QUIK в режиме «без выходных» (суббота и воскресенье считаются рабочими днями). Возможные значения:
 - «0» (по умолчанию) – режим работы сервера QUIK определяется стандартным календарем рабочих (будни) и нерабочих (выходные) дней;
 - «1» – сервер QUIK работает в режиме «без выходных».

Файл `trade_dates.ini`

Откройте файл `trade_dates.ini` в каталоге `<quik_dir>\server\` и отредактируйте его.

В секции [trade_date] задаются даты-исключения для календаря торговых и неторговых дней, используемого на сервере QUIK. По умолчанию Сервер QUIK считает торговыми дни



с понедельника по пятницу включительно, а субботу и воскресенье – неторговыми. День считается торговым, если в этот день на данном сервере QUIK проходят торги на любой из торговых площадок:

- Если в будний день запланированы торги хотя бы на одной площадке из доступных на сервере QUIK, то эту дату не нужно добавлять в секцию [trade_date].
- Если в будний день торги не запланированы ни на одной из площадок, то нужно добавить эту дату с признаком holiday в секцию [trade_date].
- Если в выходной день запланированы торги хотя бы на одной площадке из доступных на сервере QUIK, то нужно добавить эту дату с признаком workday в секцию [trade_date].

Даты-исключения из стандартного календаря, в соответствии с которым сервер QUIK запускается в режиме рабочего или нерабочего дня, в формате:

```
<ГГГГММДД>=holiday  
<ГГГГММДД>=workday
```

Где:

- _ holiday – нерабочий день;
- _ workday – рабочий день.

Пример заполнения секции см. в [примечании](#).

При запуске сервера QUIK с ключом [-holiday](#) или [-workday](#) значения секции имеют меньший приоритет.

Файл settlement_dates.ini

Откройте файл settlement_dates.ini в каталоге <quik_dir>\server\ и отредактируйте его.

В секции [settlement_date] задаются даты-исключения для календаря расчетных и нерасчетных дней, используемого на основной торговой площадке. По умолчанию Сервер QUIK считает расчетными дни с понедельника по пятницу включительно, а субботу и воскресенье – нерасчетными.

Если на основной торговой площадке будний день считается нерасчетным, то его нужно добавить в секцию [settlement_date] с признаком holiday, а если выходной день считается расчетным, то его нужно добавить с признаком workday.

Действие описанных дат-исключений распространяется на все режимы торгов, но имеет меньший приоритет, чем календари, задаваемые через программу QUIK Administrator. Если дата задана в секции [settlement_date] как выходной, а в календаре программы QUIK Administrator как рабочий день, то она будет считаться рабочим днем.



Наличие/отсутствие выходных приводит к сдвигу даты расчетов, что выражается в увеличении/уменьшении календарных дней между заключением сделки и расчетом при выполнении операций с кодами расчетов, отличными от T0, например, T1, T2.

Заполнение секции [settlement_date] влияет на:

- Корректность учета объема комиссии;
- Определение цепочки лимитов, на которую распространяются блокировка, начисления и списания;
- Определение последнего вида лимитов в цепочке лимитов операции для отчетов/сделок на исполнение второй части РЕПО;
- Расчет срока РЕПО по безадресным и адресным режимам РЕПО и РЕПО с ЦК;
- Учет НКД при расчете блокируемого объема заявки на лимитах для РЕПО-М и РЕПО с ЦК;
- Расчет комиссии торговой системы по поставочным свопам на валютном рынке, который определяет дату начала первой части РЕПО;
- Определение срока жизни GTD/GTC-заявок в том числе OMS-заявок, в рамках которого рассчитывается максимальный объем заявки с учетом динамически настроенного НКД и номинала облигации, что влияет на объем заблокированных средств.

Формат секции:

```
<ГГГГММДД>=holiday  
<ГГГГММДД>=workday
```

Где:

- holiday – нерасчетный день;
- workday – расчетный день.

Примеры для секций [trade_date] и [settlement_date]:

Пример 1

На сервере два Интерфейса: к Фондовому рынку Московской биржи и рынку иностранных ценных бумаг СПБ Биржи. 4 ноября 2022 года – праздничный день, который является нерасчетным на Фондовом рынке Московской биржи, но торговым на рынке иностранных ценных бумаг СПБ Биржи.

Нужно задать следующие настройки:

```
[settlement_date]  
20221104=holiday
```



Пример 2

На сервере один Интерфейс – к Фондовому рынку Московской биржи.

4 ноября 2022 года – праздничный день, который является нерасчетным на Фондовом рынке Московской биржи. Таким образом, на сервере нет ни одного режима торгов, в котором будут проходить торги в этот день.

Нужно задать следующие настройки:

```
[settlement_date]  
20221104=holiday
```

```
[trade_date]  
20221104=holiday
```

Пример 3

На сервере один Интерфейс – к Фондовому рынку Московской биржи. 5 марта 2022 года (суббота) – торговый и расчетный день.

Нужно задать следующие настройки:

```
[settlement_date]  
20220305=workday
```

```
[trade_date]  
20220305=workday
```

2.5.3 Настройка дистрибутива для пользователей

Каталог <inst_dir>/front содержит актуальный дистрибутив Рабочего места QUIK и предназначен для распространения клиентам. При подключении пользователя к серверу выполняется сравнение версии Рабочего места QUIK пользователя с версией, которая хранится в директории с актуальным дистрибутивом Рабочего места QUIK. Если версии не совпадают, то пользователю предлагается обновление.

Скопируйте содержимое каталога <inst_dir>/front в директорию, которая предназначена для хранения дистрибутива Рабочего места QUIK.

Сервер по умолчанию использует в качестве директории с дистрибутивом Рабочего места QUIK:



- <quik_dir>/server/areas/frontend/x64/release – для Рабочего места QUIK версии 8.0.0 и выше;
- <quik_dir>/server/areas/frontend/release – для Рабочего места QUIK версии ниже, чем 8.0.0.

Расположение директории с дистрибутивом Рабочего места QUIK может быть переопределено настройкой frontend в секции [areas] конфигурационного файла сервера QUIK quik.ini. В настройке указывается только путь до общей директории, в которой хранятся оба дистрибутива. Значение по умолчанию: «frontend=areas/frontend».

Пример:

```
[areas]
frontend=clientfront
```

В данном примере дистрибутив Рабочего места QUIK хранится в следующих директориях:

- <quik_dir>/server/clientfront/x64/release – для Рабочего места QUIK версии 8.0.0 и выше;
- <quik_dir>/server/clientfront/release – для Рабочего места QUIK версии ниже, чем 8.0.0.

2.5.4 Настройка прокси для подключения пользователей

Сервер поддерживает протокол HAProxy версии 1 при обработке пользовательских подключений. При настройке прокси необходимо указать порт сервера, который прописан в секции [usend_module].

2.5.5 Настройка блочного шифрования

Откройте для редактирования файл в каталоге <quik_dir>\server\quik.ini и в секции [usend_module] настройте следующие параметры:

- **enable_block_crypt** – признак использования блочного шифрования. Возможные значения:
 - _ «0» (по умолчанию) – блочное шифрование не используется;
 - _ «1» – используется.
- **block_crypt_size** – размер блока шифрования. Возможные значения: от 100 до 8192 (включительно). Значение по умолчанию: «1024».

2.5.6 Настройка асинхронного использования Библиотеки расчета лимитов

При необходимости настройки параллельного проведения пре-трейд и пост-трейд контроля операций по разным заявкам рекомендуется обратиться



за дополнительными инструкциями в Службу технической поддержки QUIK:
quiksupport@argatech.com.

Фирмы, для которых применяется стратегия асинхронного использования Библиотеки расчета лимитов, перечисляются в файле <quik_dir>\server\quik.ini в секции [dealer-library-async]. Например:

```
[dealer-library-async]
NC0038900000=
SPBFUT389=
```

В секции [behavior] настраиваются следующие параметры:

- **numberofexecutors** – общее количество очередей параллельной обработки алгоритмов Библиотеки расчета лимитов для всех фирм, которые используют Библиотеку расчета лимитов асинхронно.
- **deallib.temppath** – путь к директории для временного хранения экземпляров DLL для Библиотеки расчета лимитов.

Пример:

```
[behavior]
deallib.temppath=.\temp
numberofexecutors=3
```

2.5.7 Исключения для антивирусного ПО

В данном разделе перечислены файлы и каталоги сервера QUIK, которые необходимо исключить из проверки антивирусным ПО, так как они используются при работе сервера.

Исключаемые файлы и каталоги:

1. Каталог с сервером QUIK.
2. Каталоги и файлы, указанные в настройках сервера в файле quik.ini:
 - пути к логам и файлам с расширением .ik, задаваемые в секции [Files] в параметрах LogFilesFolderName и DataFilesFolderName, например:

```
LogFilesFolderName=.\logs
DataFilesFolderName=.\data
```



- пути к файлам замен, задаваемые в секции [data_module] в параметрах `firm_substitute_file` и `client_codes_substitute_file`, например:

```
firm_substitute_file=.\firms.ini
client_codes_substitute_file=.\codes.ini
```

- пути к архивам, задаваемые в секции [archive_module] в параметрах `ttp_dir` и `minutes_dir`, например:

```
ttp_dir=.\archive\minutes_ttp
minutes_dir=.\archive\minutes
```

- путь к настройкам кросс-курсов, задаваемый в секции [cur_module] в параметре `class_cfg`, например:

```
class_cfg=crossrate.ini
```

- пути к настройкам криптопровайдера, задаваемые в секции [usend_module], например:

```
crypto_provider_ini_file=.\openssl_pr.ini - параметр для задания единственного
криптопровайдера;
crypto_provider_ini_file_mp=.\mp_pr.ini - параметр для задания криптопровайдера
MP;
crypto_provider_ini_file_sslpro=.\sslpro_pr.ini - параметр для задания
криптопровайдера SSL-Pro;
crypto_provider_ini_file_openssl=.\openssl_pr.ini - параметр для задания
криптопровайдера OpenSSL.
```

- пути к шаблонам, задаваемые в секции [quik_auth] в параметрах `TemplateRuRetrievingNotSupportedFileName` и `TemplateRuUnknownErrorFileName`, например:

```
TemplateRuRetrievingNotSupportedFileName=templates\ru\retrievingnotsupported
TemplateRuUnknownErrorFileName=templates\ru\unknownerror
```

3. Каталоги с настройками криптопровайдеров в файле `crypto.cfg`, задаваемые в параметре `IniFile`, например:

```
IniFile=openssl_pr.ini
```



В исключения необходимо добавить сетевые порты, указанные в настройках сервера и серверов доступа в файле quik.ini в параметре port.

2.5.8 Настройка текста уведомления об истечении срока действия доверенности

Чтобы настроить текст отправляемых уведомлений о скором истечении срока действия доверенности подключаемого пользователя, задайте в `crypto.cfg` следующие настройки:

- В секции `[register]` укажите количество дней до истечения срока действия доверенности, за которое пользователю начнут приходить ежедневные уведомления (при каждом подключении). Значение по умолчанию: «3».

Пример:

```
[register]
license_warning_days=4
```

- В секции `[auth]` укажите текстовые описания сообщений. Ключом выступает шаблонная строка вида:

```
lic_exp_<d>_day_<lang>
```

Где:

- `<d>` – количество дней до истечения доверенности. Может принимать значения «1», «2», «3», «...» и так далее;
- `lic_exp_today_<lang>` – соответствует текущему дню;
- `n` – всем остальным дням;
- `<lang>` – код языка рабочего места. Возможные значения:
 - «25» – русский;
 - «9» – английский.

Шаблонная строка `lic_exp_today_<lang>` используется для установки текстового описания, когда срок доверенности для клиента истекает сегодня.

Шаблонная строка `lic_exp_n_days_<lang>` используется для установки текстового описания по умолчанию.

Пример:

```
[auth]
```



```
lic_exp_n_days_25=Скоро закончится срок доверенности
lic_exp_1_day_25=Остался один день до истечения срока доверенности
lic_exp_today_25=Срок доверенности истекает сегодня
```

Текстовое описание поддерживает идентификаторы формата, которое позволяет в сообщении вставлять на их место дату прекращения доверенности. Поддерживаются следующие идентификаторы:

- `<>` – количество дней до истечения срока;
- `<d>` – номер дня в месяце, когда истекает срок;
- `<m>` – номер месяца в году, когда истекает срок;
- `<y>` – год, когда истекает срок.

Пример:

```
[auth]
lic_exp_n_days_25=Срок действия вашей доверенности прекращается через <> дня
```

Пример:

```
[auth]
lic_exp_n_days_25=Срок вашей доверенности истекает <d>.<m>.<y>
```

2.5.9 Роллирование позиций

Сервер QUIK может быть запущен в режиме роллирования позиций клиентов по деньгам и инструментам (фондовый рынок).

Перед настройкой роллирования позиций обратитесь за дополнительными инструкциями в Службу технической поддержки QUIK:
quiksupport@argatech.com.

Для роллирования позиций выполните настройки:

1. В файле `quik.ini`, который находится в каталоге `<quik_dir>\server\`, настройте следующие параметры:
 - в секции `[data_module]`:
 - **rolling.rotation_depth** – глубина ротации файлов с позициями, которые находятся в директории Backup. Сервер хранит не более указанного в настройке количества файлов для каждого из типов позиций по деньгам и по



инструментам. По достижении максимального значения настройки старые файлы удаляются. Значение по умолчанию: «7».

- **rolling.CPLimitTag** – теги через запятую, которые используются Модулем QUIK REPO для ведения лимитов на контрагентов при роллировании позиций по деньгам. Учитываются только позиции со сроком расчетов T0 с указанными тегами. Значение по умолчанию: «» (пусто).
- в секции [calc-limits]:
 - **UnifiedLeverageOnClient** – признак использования единого размера плеча на всех позициях по деньгам клиента, для которого используется схема маржинального кредитования «По дисконтам» или «МД+». Установите значение «1». Значение по умолчанию: «0».

2. Выполните запуск сервера с ключом [-rolling \(«/ro»\)](#).

3. Подключите интерфейс, который выполнит активацию позиций после роллирования.

Информация по перенесенным позициям обновляется только после подключения торговых интерфейсов или Информационного интерфейса Holiday.

При ведении позиций в сроках расчетов (например, если настроена цепочка T0, T1, T2, T365, а используется только T0), то при переходе на роллирование позиций возможно значительное увеличение потребляемой оперативной памяти и дискового пространства. Это вызвано процессом роллирования, который создает лимиты для пропущенных сроков расчетов.

2.6 Миграция сервера с Windows на Linux

При миграции ПО с ОС Windows на ОС Astra Linux необходимо учитывать следующие ограничения Linux-версии по сравнению с Windows-версией:

- Отсутствует поддержка криптопровайдера MP.
- Для переноса ПО, работающего на ОС Windows, на компьютер с ОС Astra Linux:
 - Версия ПО, которая переносится с ОС Windows, должна быть равна версии ПО, которая будет устанавливаться на ОС Astra Linux.
 - ПО на ОС Astra Linux должно использовать в качестве СУБД PostgreSQL.
 - Перенос должен осуществляться в строго неторговое время: после завершения торгов и остановки сервиса, и до начала торгов, перед первым запуском сервиса.

Перенос сервиса выполняется в два этапа:

- Установка сервиса на ОС Astra Linux (производится пользователем root);
- Перенос конфигурации с ОС Windows (производится пользователем root или arqasrv).

Для установки ПО на ОС Astra Linux выполните следующий порядок действий:

1. Установите на компьютер, на котором будет работать сервис, [необходимые пакеты](#).



2. Скопируйте файл `install_server-xx.xx.xx.run` в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (`/home/<user>` или `~/`).
3. Выполните команду добавления права на выполнение run-файлу:

```
chmod +x install_server-xx.xx.xx.run
```

4. Выполните команду установки сервиса:

```
sudo ./install_server-xx.xx.xx.run -i
```

Для выполнения команды может потребоваться введение пароля текущего пользователя. В процессе исполнения run-файла выполняются следующие действия:

- Если системный пользователь `arqasrv` отсутствует, он создается с правами по умолчанию и включается в одноименную группу. В качестве домашней директории пользователю устанавливается директория `/opt/arqasrv`. От имени этого пользователя будет работать устанавливаемый сервис.
- В директории `/opt/arqasrv/quik` создается поддиректория с именем `quik`, в которую распакуются файлы дистрибутива устанавливаемого сервиса.
- Пользователь `arqasrv` назначается владельцем всех файлов и поддиректорий в директории сервиса.
- В системе управления службами `systemd` регистрируется сервис с именем `quik` и запуском от имени системного пользователя `arqasrv`.
- В директории `/etc/arqasrv` создается файл с именем `quik` для фиксации параметров установки сервиса.
- В директории установки сервиса сгенерируются следующие командные файлы:
 - `q_start.sh` – запуск сервиса, в том числе с [ключами запуска](#). Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `q_stop.sh` – остановка сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `q_status.sh` – вывод информации о текущем состоянии сервиса. Предназначен для выполнения пользователями `arqasrv` и `root`;
 - `uninstall.sh` – удаление сервиса. Предназначен для выполнения пользователем `root`;
 - `postmigration.sh` – выполнение дополнительных операций при миграции. Предназначен для выполнения пользователями `arqasrv` и `root`.



При успешной установке сервиса выводится сообщение: «Installation of service "quik" has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

5. Если управление установленным сервисом предполагается выполнять пользователем `argasrv`, выполните следующие действия:

- Для предотвращения внесения пользователем `argasrv` изменений в скрипты управления сервисом, на которые ему будет выдано разрешение выполнения от имени `root`, сделайте их неизменяемыми, выполнив следующие команды:

```
chattr +i /opt/argasrv/quik/quik/q_start.sh
chattr +i /opt/argasrv/quik/quik/q_stop.sh
```

- Выдайте пользователю `argasrv` права на выполнение скриптов управления сервисом от имени `root`, выполнив следующие действия:

- Выполните команду:

```
sudo visudo
```

- В открывшемся vi-подобном редакторе добавьте строку:

```
argasrv ALL=(root) /opt/argasrv/quik/quik/q_start.sh,
/opt/argasrv/quik/quik/q_stop.sh
```

Эта строка разрешает пользователю `argasrv` выполнять перечисленные скрипты на текущем компьютере от имени `root`.

Для переноса конфигурации с ОС Windows выполните следующий порядок действий:

1. Скопируйте из директории Windows-сервиса в директорию Linux-сервиса `/opt/argasrv/quik/<srvname>` следующие файлы:

- Основной файл настроек: `quik.ini`;
- Общий файл настроек криптопровайдеров: `crypto.cfg`;
- Файлы настроек Библиотек расчета лимитов: каталог `Dealer/`;
- Файлы шаблонов-сообщений для двухфакторной аутентификации: каталог `Templates`;
- Файл настроек кросс-курсов: `crossrate.ini`;
- Файл настроек замены фирм: `areas/firms.ini`;



- _ Файл запрещенных к подключению UID: restu.cfg;
- _ Файл настроек замены кодов клиента: codes.ini;
- _ Другие файлы настроек .ini (в случае наличия таких файлов) с сохранением их расположения относительно директории установки сервиса;
- _ Файлы ключей (.txk), каталоги сертификатов провайдеров:
 - _ Ключи secrserv.txk, pubring.txk – для настройки криптопровайдера qcrypto32;
 - _ Каталог certs – для настройки криптопровайдера OpenSSL_pr;
 - _ Каталог signalcom – для настройки криптопровайдера Signalcom_pr;
 - _ Каталог, содержащий архивы графиков (значение по умолчанию: «minutes»), если они хранятся локально, рядом с сервером.

2. Приведите имена скопированных в предыдущем пункте файлов и директорий к нижнему регистру. Для этого выполните в директории /opt/arqasrv/quik/<srvname> команду:

```
sudo ./postmigration.sh
```

3. Измените настройки в перенесенных файлах:

- _ Все упоминания динамических библиотек (.dll) необходимо преобразовать в соответствующее наименование на Linux. Для этого к имени необходимо добавить префикс «lib», а расширение заменить на .so, например:

```
module=dwdata.dll
замените на:
module=libdwdata.so
```

- _ Список секций файла quik.ini, в которых указаны наименования динамических библиотек, которые необходимо преобразовать:

```
[data_module]
module=dwdata.dll
замените на:
module=libdwdata.so

[conn_module]
module=dwxs.dll
замените на:
module=libdwxs.so

[trans_module]
module=dwtrans.dll
замените на:
module=libdwtrans.so
```



```
[auth_module]
module=dwqx.dll
замените на:
module=libdwqx.so

[limits_module]
module=dwlimits.dll
замените на:
module=libdwlimits.so

[usend_module]
module=dwsend.dll
замените на:
module=libdwsend.so

[ctl_module]
module=dwwqctl.dll
замените на:
module=libdwwqctl.so

[msg_module]
module=dwqtalk.dll
замените на:
module=libdwqtalk.so

[archive_module]
module=dwarch.dll
замените на:
module=libdwarch.so

[banner_module]
module=dwbanner.dll
замените на:
module=libdwbanner.so

[data_ip_module]
module=dtwipsrv.dll
замените на:
module=libdtwipsrv.so

[report_module]
module=dwrep.dll
замените на:
module=libdwrep.so
```



```
[data_pipe_module]
module=dtwsrv.dll
замените на:
module=libdtwsrv.so

[db_module]
module=dstubrc.dll
driver=quik_db_pg.dll
замените на:
module=libdstubrc.so
driver=libquik_db_pg.so

[cur_module]
module=dwcurg.dll
замените на:
module=libdwcurg.so
```

- Замените наименования динамических библиотек в файле `qcrypto.cfg`. Секции, в которых указаны наименования динамических библиотек:

```
[auth]
sign=secprov.dll
замените на:
sign=libsecprov.so
```

- Для настройки `look` необходимо найти указанную секцию, например, если настроена `db_look`:

```
[auth]
look=qcrypto.cfg,db_look

[db_look]
use=dwqx.dll
замените на:
use=libdwqx.so
```

- В настройках криптопровайдеров файла `qcrypto.cfg` измените наименования динамических библиотек и регистр файла настроек (при наличии перечисленных секций):

```
[openssl]
Module=openssl_pr.dll
IniFile=openssl_pr.ini
замените на:
```



```
[openssl]
Module=libopenssl_pr.so
IniFile=openssl_pr.ini

[SignalComMessageAndSSLPro]
Module=signalcom_pr.dll
IniFile=signalcom_pr.ini
замените на:
[SignalComMessageAndSSLPro]
Module=libsignalcom_pr.so
IniFile=signalcom_pr.ini

[placebo]
Module=placebo_pr.dll
замените на:
[placebo]
Module=libplacebo_pr.so
```

- Если, кроме перечисленных криптопровайдеров, в файле `crypto.cfg` есть другие настроенные криптопровайдеры, то соответствующие секции настроек необходимо закомментировать путем добавления в начало строки символа «;» (точка с запятой). Также необходимо закомментировать объявление криптопровайдера в секции `[CryptoProviders]`, например, отключение провайдера MP:

```
[CryptoProviders]
;mp=1

; [mp]
;Module=mp_pr.dll
;IniFile=mp_pr.ini
```

- В списке загружаемых настроек Библиотеки расчета лимитов файла `quik.ini` измените наименование и регистр файла настроек, например:

```
[dealer-library]
ALGO=./dealer/algo.ini
```

- Если ранее в этой секции были настроены пути к файлам с расширением `.dll`, то расширение у них необходимо заменить на `.ini`, например:

```
[dealer-library]
ALGO=.\Dealer\ALGO.dll
замените на:
```



```
[dealer-library]
ALGO=./dealer/algo.ini
```

- Все упоминания путей к файлам и каталогам необходимо привести к виду, принятому в файловой системе Linux – обратные слэши («\») необходимо заменить на прямые («/»), например:

```
crypto_provider_ini_file=.\openssl_pr.ini
замените на:
crypto_provider_ini_file=./openssl_pr.ini
```

- Перечень настроек quik.ini, которые содержат пути к файлам или директориям с примерами значений:

```
[ctl_module]
rest_users_file=restu.cfg

[usend_module]
suspect_data_file=stats/suspect.txt

[key_management]
key_info_file=key_info.ini

[areas]
frontend=areas/frontend
msg_priv=areas/msg_priv
public=areas/public
company=areas/company
private=areas/private
unrestricted=areas/unrestricted
hasharchives=hasharchives
hasharchivesttp=hasharchivesttp

[archive_module]
minutes_dir=minutes
ttp_dir=ttp

[auth_module]
settings_file=qcrypto.cfg
```

- Перечень настроек qcrypto.cfg, которые содержат пути к файлам или директориям с примерами значений:

```
[auth]
```



```
mail_settings_file=qrypto.cfg
arw_log=stats/arw.log
```

- Отредактируйте путь к файлу баннера, если он настроен. Файлом конфигурации баннера считается первый найденный сервером .ini-файл в директории /areas/banners. Например:

```
[url_set]
image=./banner.bmp
```

- Сетевые диски обычно монтируются к локальным каталогам, поэтому необходимо уточнить у сетевых администраторов точку монтирования и прописать путь к ней, например:

```
[areas]
Archives=\\minutes\qminreplicator\archive\
замените на:
[areas]
Archives=/mnt/qminreplicator/archive
```

4. Настройте автоматику ежедневного запуска и остановки сервиса. Для этого используйте в скриптах автоматики запуск командных файлов q_start.sh и q_stop.sh, расположенных в директории установленного сервиса.

2.7 Удаление сервера

Удаление сервиса на платформах Windows и Astra Linux происходит по-разному.

2.7.1 Удаление сервера, установленного на Windows

Для удаления сервиса выполните следующие действия:

1. Остановите службу сервера. Сделать это можно через приложение «Службы», открытое от имени администратора, либо вкладку «Службы» диспетчера задач, также запущенного от имени администратора.
2. Выполните удаление службы сервера путем выполнения команды в консоли, запущенной от имени администратора:

```
quik.exe -remove
```

3. Выполните удаление БД сервера.



4. Выполните удаление каталога сервера.

2.7.2 Удаление сервера, установленного на Linux

Удаление сервиса производится пользователем root вызовом скрипта `uninstall.sh`, который находится в каталоге соответствующего сервиса.

Далее приведен порядок действий при удалении сервиса с именем по умолчанию – `quik`.

Для удаления сервиса выполните следующие действия:

1. Остановите службу Сервера QUIK из директории с установленным сервисом, запустив команду:

```
sudo ./q_stop.sh
```

либо из любой директории, отличной от директории сервиса, запуском команды:

```
sudo /opt/arqasrv/quik/quik/q_stop.sh
```

2. Если управление установленным сервисом выполнялось пользователем `arqasrv`, выполните следующие действия:

- Отмените у пользователя `arqasrv` права на выполнение скриптов управления сервисом от имени `root`, выполнив следующие действия:
 - Выполните команду:

```
sudo visudo
```

- В открывшемся `vi`-подобном редакторе удалите строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/quik/q_start.sh,  
/opt/arqasrv/quik/quik/q_stop.sh
```

- Снимите признак неизменяемости со скриптов управления сервисом, выполнив следующие команды:

```
chattr -i /opt/arqasrv/quik/quik/q_start.sh  
chattr -i /opt/arqasrv/quik/quik/q_stop.sh
```

3. В директории установленного сервиса `/opt/arqasrv/quik/quik` запустите командный файл `uninstall.sh`:



```
sudo ./uninstall.sh
```

либо из любой директории, отличной от директории сервиса командой:

```
sudo /opt/arqasrv/quik/quik/uninstall.sh
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя. В результате выполнения команды выполняются следующие действия:

- Удаляется регистрация сервиса с именем quik в системе управления службами systemd.
- Удаляется файл /etc/arqasrv/quik, в котором были зафиксированы параметры установленного сервиса.
- Директория, в которой установлен сервис /opt/arqasrv/quik/quik, переименовывается в /opt/arqasrv/quik/quik.backup_YYYY.MM.DD_hh.mm.ss. Переименование, а не удаление директории выполняется на случай, если потребуются данные из нее. Если такой необходимости нет, удалите директорию вручную.

При успешном удалении сервиса в консоль выводится сообщение: «Removing of service “quik” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

2.8 Установка и настройка QUIK Administrator

2.8.1 Установка и настройка серверной части QUIK Administrator

1. Для настройки соединения с БД установите ODBC-драйверы для ОС.

Для ОС Windows:

- При подключении к СУБД MS SQL на компьютере, где устанавливается сервис qadminsrv, должен быть установлен ODBC-драйвер «ODBC Driver 17 for SQL Server». Для проверки наличия драйвера в меню Windows наберите в поиске текст «Источники данных ODBC» и откройте соответствующее окно. Убедитесь, что на вкладке «Драйверы» в списке присутствует драйвер с наименованием «ODBC Driver 17 for SQL Server».
- Если такой драйвер отсутствует, скачайте установочный файл драйвера с официального сайта Microsoft (<https://go.microsoft.com/fwlink/?linkid=2223304>) и установите его на компьютер, на котором будет работать сервис.
- При подключении к СУБД PostgresPRO на компьютере, где устанавливается сервис qadminsrv, должен быть установлен ODBC-драйвер «PostgreSQL ANSI(x64)» версии не ниже 13.02. Для проверки наличия драйвера и его версии в меню Windows запустите утилиту odbcad32. Убедитесь, что на вкладке



«Драйверы» в списке присутствует драйвер с именем «PostgreSQL ANSI(x64)» и версией не ниже 13.02.

- Если такой драйвер отсутствует либо версия ниже ожидаемой, скачайте установочный файл драйвера с официального сайта ARQA Technologies (https://flex.quik.ru:8080/web/client/files?path=/Common/Lib/odbc_pg_win_13.2.0.zip) и установите его на компьютер, на котором будет работать сервис.

Для ОС Linux:

- 1. Команды установки драйверов должны выполняться от имени пользователя root.**
- 2. Необходимо наличие доступа в интернет.**

Установите на компьютер, на котором будет работать сервис, [ODBC-драйвер для работы с БД](#).

2. Установите сервис qadminsrv.

Для ОС Windows:

- Скопируйте все файлы из каталога <inst_dir>\qadminsrv\server в произвольный каталог. В данном каталоге имеется файл qadminsrv.ini, содержащий настройки программы.
- В каталоге <inst_dir>\qadminsrv\client\ находится клиентское приложение программы.
- Для установки программы войдите в систему под именем пользователя, имеющего права администратора.
- В файле qadminsrv.ini установите название сервиса. Для этого укажите в секции [Service] соответствующие значения в параметрах name, displayname.
- Выполните из командной строки команду:

```
qadminsrv -install
```

Для ОС Linux:

Установка сервиса производится пользователем root через консоль, вызовом run-файла <install_qadminsrv-xx.xx.xx.run>, где xx.xx.xx – версия продукта.

- Установите на компьютер, на котором будет работать сервис, необходимые пакеты в соответствии с описанием в п. [«Подготовка к установке»](#).
- Скопируйте файл install_qadminsrv-xx.xx.xx.run в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (/home/<user> или ~/).
- Выполните команду добавления прав на выполнение run-файлу:

```
chmod +x ./install_qadminsrv-xx.xx.xx.run
```



- Выполните команду установки сервиса (qadminsrv – имя устанавливаемого сервиса по умолчанию):

```
sudo ./install_qadminsrv-xx.xx.xx.run -i [qadminsrv] [-d <rootdir>] [-n <srvusername>]
```

- Установка выполняется в директорию /opt/arqasrv/quik/. В процессе исполнения run-файла будут выполнены следующие действия:
 - В случае отсутствия системного пользователя arqasrv, он будет создан с правами по умолчанию и включен в одноименную группу. В качестве домашней директории ему будет установлена директория /opt/arqasrv. От имени этого пользователя будет работать устанавливаемый сервис.
 - В директории /opt/arqasrv/quik/ будет создана поддиректория с именем сервиса, в которую будут распакованы файлы дистрибутива устанавливаемого ПО.
 - Пользователь arqasrv будет назначен владельцем всех файлов и поддиректорий в директории сервиса.
 - В системе управления службами systemd будет зарегистрирован сервис с именем qadminsrv и запуском от имени системного пользователя arqasrv.
 - В директории /opt/arqasrv/quik/qadminsrv будет создан файл .actions.log, в котором ведется логирование процесса установки сервиса.
 - В директории /etc/arqasrv будет создан файл с именем qadminsrv для фиксации параметров установки сервиса.
 - В директории сервиса будут сгенерированы командные файлы для:
 - q_start.sh – запуск сервиса, в том числе с [ключами запуска](#). Предназначен для выполнения пользователями arqasrv и root;
 - q_stop.sh – остановка сервиса. Предназначен для выполнения пользователями arqasrv и root;
 - q_status.sh – вывод информации о текущем состоянии сервиса. Предназначен для выполнения пользователями arqasrv и root;
 - uninstall.sh – удаление сервиса. Предназначен для выполнения пользователем root;
 - postmigration.sh – выполнение дополнительных операций при миграции. Предназначен для выполнения пользователями arqasrv и root.

При успешной установке сервиса выводится сообщение:

«Installation of service “qadminsrv” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

Запрещено вносить изменения в структуру каталогов – перемещение или переименование может привести к ошибкам.



В случае, если управление установленным сервисом предполагается выполнять пользователем `arqasrv`, выполните следующие действия:

- Для предотвращения внесения пользователем `arqasrv` изменений в скрипты управления сервисом, на которые ему будет выдано разрешение выполнения от имени `root`, сделайте их неизменяемыми, выполнив следующие команды:

```
chattr +i /opt/arqasrv/quik/qadminsrv/q_start.sh
chattr +i /opt/arqasrv/quik/qadminsrv/q_stop.sh
```

- Выдайте пользователю `arqasrv` права на выполнение скриптов управления сервисом от имени `root`, выполнив следующие действия:

- Выполните команду:

```
sudo visudo
```

- В открывшемся `vi`-подобном редакторе добавьте строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/qadminsrv/q_start.sh,
/opt/arqasrv/quik/qadminsrv/q_stop.sh
```

Эта строка разрешает пользователю `arqasrv` выполнять перечисленные скрипты на текущем компьютере от имени `root`.

Дальнейшие действия могут выполняться пользователем `arqasrv` или `root`.

3. В файле `qadminsrv.ini` выполните настройки:

- В секции `[Instances]` укажите конфигурационные файлы соединений с базами данных, в формате:

```
<Порт, используемый для данной БД>=<Имя конфигурационного файла>
```

Пример:

```
[Instances]
15301=cfg_broker1.ini
15302=cfg_broker2.ini
```

Для ОС Linux выполните преобразования для файлов, которые добавляются в секцию `[Instances]` конфигурационного файла `qadminsrv.ini` в соответствии



- Параметры соединения с каждой базой данных настраиваются в отдельном файле.
- В секции [Files] в настройке Logs укажите имя файла для логирования, если необходимо.
- В секции [General] отредактируйте следующие настройки, если необходимо:
 - **MaxDeallibSize** – максимальный размер файла настроек Библиотеки расчета лимитов, который допустимо сохранять в журнал аудита. Значение по умолчанию: «10485760» (значение в байтах соответствует 10 МБ).
 - **MaxDeallibSize_<Instance>** – максимальный размер файла настроек Библиотеки расчета лимитов, который допустимо сохранять в журнал аудита, для указанного порта («<Instance>»). По умолчанию используется значение настройки MaxDeallibSize.
 - **PathRelease** – путь к каталогу, содержащему файлы обновления клиентской части программы QUIK Administrator. Путь может быть абсолютным или относительным. Значение по умолчанию для ОС Windows: «frontend\release\», для ОС Linux: «frontend/release/» (относительный путь от директории с серверной частью QUIK Administrator).
 - **InactiveUserDisconnectTimeout** – признак того, что соединение между серверной и клиентской частями программы QUIK Administrator разрывается по истечении периода неактивности пользователя в секундах, указанного в настройке. Если указано значение «0», настройка выключена. Значение по умолчанию: «900».
 - **DisconnectWhenSessionLock** – признак разрыва соединения между серверной и клиентской частями программы QUIK Administrator при блокировке сессии и отключении удаленного сеанса. Возможные значения:
 - «0» – соединение не разрывается;
 - «1» (по умолчанию) – соединение разрывается.
 - **buildemptyreport** – создание пустого отчета.
 - «0» (по умолчанию) – не создавать;
 - «1» – создавать.
- В секции [auth] для использования механизма аутентификации в домене Active Directory / Kerberos задайте следующие настройки:
 - **AD_DCDistinguishedName** – имя контроллера домена. Значение по умолчанию: «» (пусто).
 - **AD_DomainName** – имя домена для SSO. Значение по умолчанию: «» (пусто).
 - Для Windows указывается часть домена до «\», например, «arqa».
 - Для Linux указывается часть после «@», например, «ARQA.RU».



При использовании нескольких доменов AD, между которыми настроены доверительные отношения, необходимо их указывать через запятую:

```
[auth]
AD_DomainName=first.com, second.com
или, для Linux:
AD_DomainName=FIRST.COM, SECOND.COM
```

При проверке логина используются домены по списку в указанном порядке.

Например, для пользователя user выполняется проверка first.com\user, а затем second.com\user. Тот, домен, где проверка прошла, считается корректным.

Если во всех указанных доменах аутентификация завершилась неуспешно, считается, что пользователь не прошел аутентификацию.

Если в обоих доменах есть пользователь с совпадающими логином и паролем, то будет выбран тот, который идет в списке первым.

При этом, если пользователь указывает логин вместе с доменом first.com\user (или user@FIRST.COM для Linux), то проверка выполняется для указанного домена, а домены, указанные в настройке, игнорируются. Тогда результат успешной валидации пользователя (даже в случае успешной аутентификации в домене) зависит от наличия записи с таким логином (выполняется проверка полного соответствия) в программе QUIK Administrator в окне «Логин в другой системе авторизации» (меню **Сервер QUIK / Безопасность / Логин в другой системе авторизации**).

Для корректной настройки аутентификации в домене Active Directory / Kerberos следует выполнить [настройку Сервера QUIK для аутентификации](#).

4. В файле настроек сервера <имя конфигурационного файла>.ini выполните настройки.

Для ОС Linux выполните преобразования для всех секций конфигурационного файла в соответствии с [правилами преобразования ini-файлов при миграции ПО с ОС Windows на ОС Linux](#).

- В секции [DB] укажите параметры доступа к базе данных:
 - **Server** – имя сервера.
 - **Base** – имя базы данных.
 - **User** – имя пользователя базы данных.

Пользователь должен быть включен в роли «quik_rbo» и «quik_auditor» в базе данных сервера QUIK.



- **Password** – пароль пользователя базы данных. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#).
- **UsePersonalLogin** – при необходимости использования персональных логинов для подключения к базе данных укажите значение «1».
- **AuthMode** – используемый тип аутентификации на сервере MS SQL. Возможные значения:
 - «login» (по умолчанию) – используются логин и пароль, указанные в параметрах user и password (пароль может быть [зашифрован](#));
 - «domain» – используется доменная аутентификация.

При AuthMode=domain параметры user и password в секции [DB] игнорируются и могут быть не указаны.

- **Driver** – наименование ODBC-драйвера, используемого для подключения к базе данных сервера QUIK. Возможные значения:
 - Для Windows:
 - «ODBC Driver 17 for SQL Server» (по умолчанию) – используется для работы с MS SQL Server 2014, 2016 или более новой версией СУБД (из списка поддерживаемых);
 - «PostgreSQL ANSI(x64)» – используется для работы с PostgresPRO;
 - Если значение настройки не задано, используется «ODBC Driver 17 for SQL Server».
 - Для Astra Linux:
 - «PostgreSQL ANSI» (по умолчанию) – используется для работы на Linux.
 - Для RED OS:
 - «PostgreSQL» – используется для работы на RED OS.

При работе с MS SQL Server должен быть установлен драйвер ODBC Driver 17 for SQL Server, а при работе с PostgresPRO – драйвер psqlODBC 13.2 и выше.

- **Port** – порт для подключения к серверу PostgresPRO. Значение по умолчанию: «5432».
- **AdditionalParameters** – настройка для задания дополнительных параметров подключения к СУБД. Значение по умолчанию: «» (пусто).
- **SSLMode** – режим безопасного подключения. Поддерживается только при настройке подключения к СУБД PostgresPRO. Возможные значения:
 - «» (пусто, по умолчанию) – подключение выполняется без шифрования;
 - «require»;
 - «verify-ca»;
 - «verify-full»;



- _ «disable»;
- _ «allow»;
- _ «prefer».

Описание режимов безопасного подключения см. на официальном сайте PostgreSQL: www.postgresql.org/docs/current/libpq-ssl.html.

Если параметр не задан, то параметры CertCAFileName, CertFileName, CertPKeyFileName и CertPass игнорируются.

- _ **CertCAFileName** – путь к файлу-контейнеру сертификатов удостоверяющих центров. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertFileName** – путь и наименование файла сертификата безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertPKeyFileName** – путь и наименование файла приватного ключа безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO.
- _ **CertPass** – пароль для файла приватного ключа безопасного подключения. Значение по умолчанию: «» (пусто). Поддерживается только при настройке подключения к СУБД PostgresPRO. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#).

Пример для MS SQL:

```
[DB]
Server=QSERV
Base=QBROKER
User=login
Password=secret
UsePersonalLogin=1
AuthMode=login
AdditionalParameters=MultiSubnetFailover=No;ApplicationIntent=ReadWrite
```

Пример для PostgreSQL/PostgresPRO:

```
[DB]
Server=QSERV
Base=QBROKER
User=login
Password=secret
Driver=PostgreSQL ANSI
SSLMode=verify-full
CertCAFileName=certs/root.crt
CertFileName=certs/user.crt
```



```
CertPKeyFileName=certs/user.key  
CertPass=secret
```

- В секции вида [DataBaseLogin_<произвольный текст>] задайте персональные логины, если параметр UsePersonalLogin равен «1». Допустимо произвольное количество секций.
 - **User** – логин для работы с базой данных;
 - **Password** – пароль для работы с базой данных. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#);
 - **Users** – список идентификаторов пользователей, которые должны использовать данный логин.

При использовании режима субадминистратора для установления соединения с серверной частью QUIK Administrator идентификатор должен быть также указан в файле subbroker_template.tpl, предназначенном для настройки режима субброкера в программе QUIK Administrator. Подробнее о файле subbroker_template.tpl см. в п. 1.2 Руководства по администрированию QUIK Administrator для субброкера.

- В секции [Connect] укажите параметры авторизации:
 - **Name** – идентификатор ключа;
 - **Password** – пароль для ключа. Пароль не должен начинаться с символов «\$» и «#». Пароль может быть [зашифрован](#);

Пример:

```
[Connect]  
Name=testinvest  
Password=secret
```

- В секции [QuikOptions] укажите параметры:
 - **RSASKeysInTransReport** – режим отображения RSA-ключей пользователя в отчете по транзакциям. Возможные значения:
 - «0» – в отчете по транзакциям не отображаются RSA-ключи пользователя;
 - «1» – в отчете по транзакциям отображаются все RSA-ключи пользователя;
 - «2» – в отчете по транзакциям отображаются только RSA-ключи пользователя, не отозванные на момент регистрации транзакции.
 - **ClientCodeDelimiter** – разделитель, используемый при настройке списка «Коды клиентов у дилера» в правах по классам диалога редактирования пользователя. Значение по умолчанию: «,» (запятая).



- **FirmId** – список фирм через запятую, доступных для выбора в поле «Код фирмы» в правах по классам диалога редактирования пользователя.
- **UserExpireCheckDays** – количество дней, за которое система предупреждает об истечении срока действия доверенности пользователя. Значение по умолчанию: «5».
- **ServiceUserExpireCheckDays** – количество дней, за которое система предупреждает об истечении срока действия доверенности служебного пользователя. Значение по умолчанию: текущее значение параметра **UserExpireCheckDays**.
- **Title** – дополнительный заголовок окна программы QUIK Administrator. Отображается после UID пользователя.
- **PINCodesInTransReport** – признак отображения PIN-кодов, используемых при двухфакторной аутентификации вида «Quik», в отчете по транзакциям. Возможные значения:
 - «0» (по умолчанию) – PIN-коды не отображаются в отчете по транзакциям;
 - «1» – PIN-коды отображаются в отчете по транзакциям.
- **UsersCountThreshold** – количество строк в справочнике пользователей в программе QUIK Administrator, по достижении которого справочник разделяется на страницы с количеством строк, заданным в параметре **PageSize**. Значение по умолчанию: «10000».
- **PageSize** – количество строк на странице в справочнике пользователей в программе QUIK Administrator. Параметр используется, если в справочнике достигнуто количество строк, заданное в параметре **UsersCountThreshold**. Значение по умолчанию: «100».
- В секции [DealerLibraryOptions] укажите параметры:

```
QuikIni=D:\QUIK1\Server\quik.ini
```

Где **quik.ini** – файл настроек сервера QUIK. Указанный файл должен быть доступен для чтения.

Допускается указание полного или сетевого имени файла. Подробности по указанию этой настройки для Linux см. [правила преобразования ini-файлов при миграции ПО с ОС Windows на ОС Linux](#).

В файле quik.ini должна быть заполнена секция [dealer-library], например:

```
[dealer-library]
NC0038900000=.\dealer\deallib389.ini
NC0058900000=.\dealer\deallib589.ini
MB0099800000=.\dealer\mb998.ini
SPBFUT389=.\dealer\spbfut389.ini
```



Указанные ini-файлы настроек Библиотеки расчета лимитов должны быть доступны для записи пользователю и процесса сервера qadminsrv.

Файлы настроек Библиотеки расчета лимитов, перечисленные в этой настройке, доступны в клиентской части QUIK Administrator для редактирования (при наличии соответствующих прав).

5. В файле qcrypto.cfg в первых двух строках, без заголовка секции, пропишите следующие настройки:

- **PUBRING** – значение: «quik.dwq»;
- **SECRING** – путь к файлу с секретным ключом сервера.

Пример:

```
PUBRING=quik.dwq
SECRING=secrserv.txk
```

6. Для [создания учетной записи QUIK Administrator](#) и назначения пользователю прав администратора запустите серверную часть QUIK Administrator с ключом -set-admin-right.

2.8.2 Настройка криптопровайдеров в QUIK Administrator

Настройка криптопровайдеров в программе QUIK Administrator средствами библиотек криптографии MP и OpenSSL.

Криптопровайдер MP используется только для ОС Windows.

1. В файле qadminsrv.ini задайте настройки используемых (для аутентификации на сервере QUIK Administrator и для проверки ЭЦП) криптопровайдеров.
 - В секции [CryptoProviders] перечислите доступных провайдеров:
 - «openssl» – признак использования провайдера OpenSSL. Возможные значения:
 - «0» – провайдер отключен;
 - «1» – провайдер включен.
 - «mp» – признак использования провайдера MP. Возможные значения:
 - «0» – провайдер отключен;
 - «1» – провайдер включен.
 - «cryptopro» – признак использования провайдера КриптоПро. Возможные значения:
 - «0» – провайдер отключен;
 - «1» – провайдер включен.



- «signalcom» – признак использования провайдера Сигнал-КОМ. Возможные значения:
 - «0» – провайдер отключен;
 - «1» – провайдер включен.

Пример:

```
[CryptoProviders]
openssl=1
mp=1
cryptopro=1
signalcom=1
```

- При использовании провайдера openssl в секции [openssl] задайте его настройки:
 - «Module» – путь к модулю провайдера. Значение по умолчанию для ОС Windows: «openssl_pr.dll». Значение для ОС Linux: «libopenssl_pr.so».
 - «IniFile» – путь к файлу настроек провайдера. Значение по умолчанию: «openssl_pr.ini».
- При использовании провайдера MP в секции [mp] задайте его настройки:
 - «Module» – путь к модулю провайдера. Значение по умолчанию: «mp_pr.dll».
 - «IniFile» – путь к файлу настроек провайдера. Значение по умолчанию: «mp_pr.ini».
- При использовании провайдера КриптоПро в секции [cryptopro] задайте его настройки:
 - «Module» – путь к модулю провайдера. Значение по умолчанию: «cpcsp_pr.dll». Значение для ОС Linux: «libcpcsp_pr.so».
 - «IniFile» – путь к файлу настроек провайдера. Значение по умолчанию: «cpcsp_pr.ini».
- При использовании провайдера Сигнал-КОМ в секции [signalcom] задайте его настройки:
 - «Module» – путь к модулю провайдера. Значение по умолчанию: «signalcom_pr.dll». Значение для ОС Linux: «libsignalcom_pr.so».
 - «IniFile» – путь к файлу настроек провайдера. Значение по умолчанию: «signalcom_pr.ini».

Для ОС Windows:

```
[openssl]
Module=.\openssl_pr.dll
IniFile=.\openssl_pr.ini

[mp]
```



```
Module=.\mp_pr.dll
IniFile=.\mp_pr.ini

[cryptopro]
Module=.\cpcsp_pr.dll
IniFile=.\cpcsp_pr.ini

[signalcom]
Module=.\signalcom_pr.dll
IniFile=.\signalcom_pr.ini
```

Для ОС Linux:

```
[openssl]
Module=./libopenssl_pr.so
IniFile=./openssl_pr.ini

[cryptopro]
Module=./libcpcsp_pr.so
IniFile=./cpcsp_pr.ini

[signalcom]
Module=./libsignalcom_pr.so
IniFile=./signalcom_pr.ini
```

Для проверки подписи необходимо наличие только корневого сертификата УЦ, доступного в настройке криптопровайдера.

При работе под ОС Windows для криптопровайдеров «mp_pr» и «cpcsp_pr» корневые УЦ сертификаты должны быть установлены в системное хранилище корневых сертификатов («КриптоПро» имеет собственную утилиту) и должны быть доступны для пользователя, под которым запускается сервер qadminsrv.

При работе под ОС Linux корневые сертификаты должны быть установлены через утилиту «КриптоПро». Команда выполняется от имени пользователя, под которым запускается сервер qadminsrv (по умолчанию: «arqasrv»).

```
/opt/cprocsp/bin/amd64/certmgr -install -store root -file certnew.p7b
```

Где:



- `/opt/cproscsp/bin/amd64/certmgr` – менеджер сертификатов.
- `<-install>` – команда установки сертификатов.
- `<-store root>` – хранилище корневых доверенных сертификатов.
- `<-file certnew.p7b>` – имя файла контейнера, содержащего корневые сертификаты.

Для криптопровайдеров «signalcom_pr» и «openssl_pr» корневые сертификаты копируются в соответствующую директорию «CA», указанную в файле настроек.

Для криптопровайдера «signalcom_pr», который имеет опцию «Проверять по справочнику», требуется наличие списка клиентских сертификатов аналогично серверу QUIK.

При расположении сервера QUIK Administrator на одном компьютере с сервером QUIK допускается использование .ini файлов, которые используются для настройки криптопровайдеров.

Если на одном сервере QUIK Administrator настроено использование двух или более экземпляров сервера QUIK Administrator, то они все используют единые настройки криптопровайдеров.

2. Задайте настройки провайдера в файле `openssl_pr.ini` или `mp_pr.ini` (в зависимости от используемого провайдера) и укажите номер схемы аутентификации.

При использовании провайдера openssl в файле openssl_pr.ini:

- в секции `[tls connection settings]` задайте номер схемы аутентификации в параметре **ServerHandShakeScheme**. Возможные значения:
 - «2» – аутентификация в домене по логину и паролю;
 - «4» – аутентификация по имени пользователя и паролю;
 - «32» – аутентификация внутри домена.

При поддержке нескольких схем значение настройки задается в виде суммы значений, соответствующих поддерживаемым схемам. Например, чтобы указать сразу две схемы («2» и «4»), установите значение «6», а чтобы указать три схемы («2», «4» и «32»), установите значение «38».

При использовании провайдера MP задайте настройки в файле mp_pr.ini:

- в секции `[certificate stores]` настройте хранилище сертификатов.
- в секции `[tls connection settings]` задайте следующие настройки:
 - **UsedHandShakeScheme** – номер схемы аутентификации в соответствии с правилами совместимости схем аутентификации на сервере и у клиента. Возможные значения:
 - «2» – аутентификация в домене по логину и паролю;
 - «4» – аутентификация по имени пользователя и паролю;
 - «32» – аутентификация внутри домена.
 - **CSPUseLocalMachineStore=0** – ключ хранится в текущем хранилище пользователя;



- **CheckRevocation=0** – не проверять сертификат на отзыв;
- **CSPCertHash** – хеш сертификата сервера.

2.8.3 Добавление сертификата в хранилище сертификатов сервера QUIK

В файле настроек qadminsrv.ini, в секции [Instances] указан файл настроек подключения, например:

```
16300=SERV_03.ini
```

1. Задайте значения в файле SERV_03.ini:

```
[QuikCryptoProvider]
CryptoType=CryptoPro
Storage=/opt/arqasrv/quik/quik/userstore.sto
```

Где:

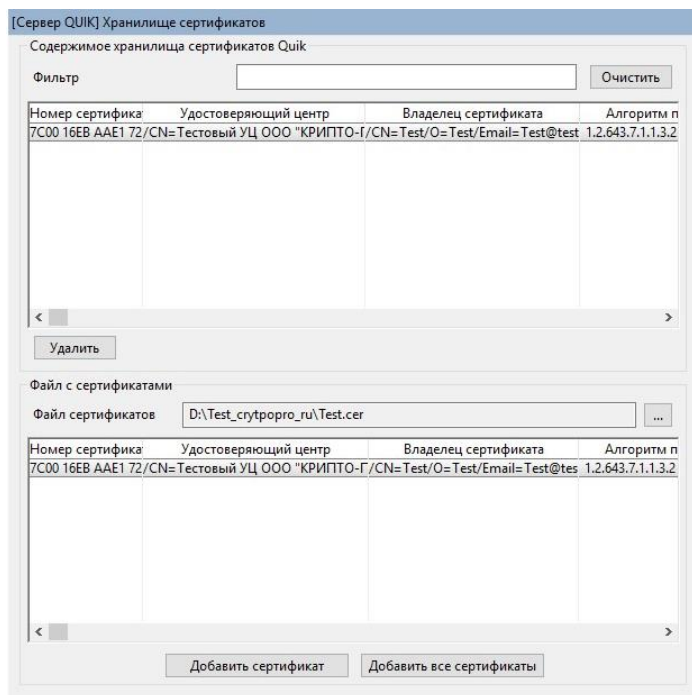
- «userstore.sto» – хранилище сертификатов. Этот файл нужно создать (пустой) в месте, указанном в параметре Storage.

Если QUIK Administrator установлен на Linux, то файл создается пользователем arqasrv.

2. Откройте пункт меню **Сервер QUIK / Безопасность / Хранилище сертификатов** в QUIK Administrator.



3. Выберите «Файл сертификатов», укажите путь до сохраненного сертификата Пользователя и нажмите «Открыть». Отобразится информация о выбранном сертификате Пользователя.



4. Нажмите «Добавить сертификат».



5. На вкладке «Редактирование (Пользователи)» в QUIK Administrator выполните следующие действия:

Редактирование (Пользователи)

Выбрать...

Импорт... Сохранить Отменить

Общие права Безопасность Торговые роли Права по классам Операции

Информация о последнем входе в систему
Последний вход в систему выполнен 17.10.2024 13:48:21 с адреса 192.168.32.167.

Разрешенные IP-адреса

Изменить...

Аутентификация по логину и паролю
Настроить... Логин: 13

Доступ к приложениям:
☒ webQUIK
☒ QUIK

Временная блокировка: нет
Снять блокировку

Электронная цифровая подпись CryptoPro

☒ Подпись обязательна

Ключи электронной цифровой подписи

Номер сертификата	Дата присвоения	Отозван

Изменить...

Ключи QUIK

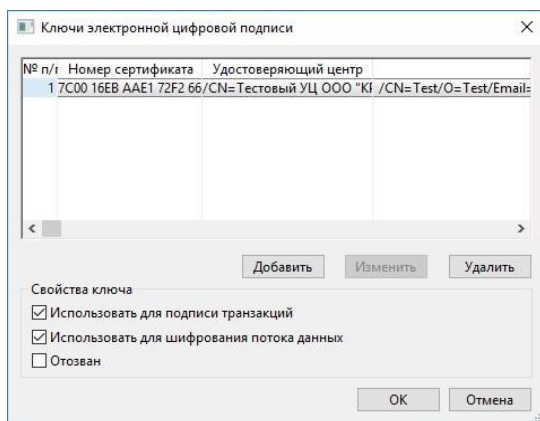
ID ключа	Дата присвоения	Отозван
85DF784F9A26C53D	8/1/2024	Нет

Изменить...

Редактирование (Пользователи) Фильтры (Пользователи)

- Выберите нужного пользователя;
 - В параметре «Электронная цифровая подпись» выберите «CryptoPro»;
 - Установите флажок «Подпись обязательна»;
 - Нажмите «Изменить» в рамке «Ключи электронной цифровой подписи», в открывшемся окне нажмите «Добавить».
6. Выберите сертификат пользователя и нажмите «Открыть».
7. Установите флажки «Использовать для подписи транзакций» и «Использовать для шифрования потока данных» в окне «Ключи электронной цифровой подписи». Нажмите «ОК».





8. Нажмите «Сохранить» для сохранения внесенных изменений.

9. Проверьте внесение номера сертификата в БД (таблица `crypto_pro_key`).

2.8.4 Работа с сервисом `qadminsrv` для ОС Linux

Управление сервисом `qadminsrv` происходит через системный сервис `systemctl`. Для регистрации сервиса `qadminsrv` создается специальный конфигурационный файл с расширением `.service`. В системной директории `systemd` создается ярлык, а конфигурационный файл находится в каталоге соответствующего сервиса. Наименование конфигурационного файла соответствует наименованию сервиса. Например, для сервиса `qadminsrv` в каталоге `/opt/arqasrv/quik/qadminsrv` создается конфигурационный файл с именем `qadminsrv.service`.

Управление работой сервиса осуществляется следующими командами от имени пользователя с правами администратора:

- Получить текущее состояние сервиса:

```
sudo systemctl status qadminsrv
```

- Запустить сервис:

```
sudo systemctl start qadminsrv
```

- Остановить работу сервиса:

```
sudo systemctl stop qadminsrv
```

Запуск, остановку и получение статуса сервиса можно осуществить с помощью скриптов `q_start.sh`, `q_stop.sh` и `q_status.sh`. При этом запуск скриптов необходимо производить через утилиту `sudo`, например:



```
sudo ./q_start.sh
```

Дистрибутив

Сервис qadminsrv распространяется для установки на компьютеры с ОС Astra Linux в формате файла вида <install_qadminsrv-xx.xx.xx.run>, где xx.xx.xx – версия продукта (далее run-файл).

С помощью run-файла производится установка и обновление сервисов в системе.

Run-файл поддерживает следующий набор ключей запуска:

- -i [<srvname>]

Установка сервиса с именем <srvname>. Параметр <srvname> необязателен. При отсутствии используется имя сервиса по умолчанию, соответствующее имени исполняемого файла сервиса – qadminsrv.

Установка двух одноименных сервисов не допускается.

- -d <rootdir>

Ключ запуска, применяемый только при установке сервиса (в комбинации с -i) для указания корневой директории для установки сервиса, отличной от директории по умолчанию /opt/arqasrv.

- -n <srvusername>

Ключ запуска, применяемый только при установке сервиса (в комбинации с -i) для переопределения владельца сервиса (имя пользователя по умолчанию: arqasrv), который станет владельцем файлов сервиса и от имени которого будет работать устанавливаемый сервис.

- -u [<srvname>]

Обновление сервиса с именем <srvname>. Параметр <srvname> необязателен. При отсутствии используется имя сервиса по умолчанию, соответствующее имени исполняемого файла сервиса – qadminsrv.

Расположение сервиса и имя пользователя-владельца сервера указывать не требуется, так как оно сохранено в /etc/arqasrv/<srvname>.

- -e

Распаковка полного содержимого архива, включая конфигурационные ini-файлы.

Распаковка производится в поддиректорию с именем, равным имени run-файла (без .run), которая в случае отсутствия создается рядом с исполняемым файлом.

- -h, -?



Вывод краткой информации об аргументах запуска.

Примеры:

Запуск run-файла для установки сервиса:

```
sudo ./install_qadminsrv-xx.xx.xx.run -i qadminsrv -d /opt/customdir
```

Запуск run-файла для обновления сервиса:

```
sudo ./install_qadminsrv-xx.xx.xx.run -u qadminsrv
```

Запуск run-файла для распаковки:

```
./install_qadminsrv-xx.xx.xx.run -e
```

Обновление сервиса

Обновление сервиса производится пользователем root вызовом run-файла.

При обновлении необходимо указать имя сервиса. Если обновляется сервис с именем по умолчанию – qadminsrv, то имя можно не указывать. Далее приведен порядок действий при обновлении сервиса с именем по умолчанию.

Для обновления выполните следующие действия:

1. Остановите службу сервиса qadminsrv из директории с установленным сервисом командой:

```
sudo ./q_stop.sh
```

либо из любой директории, отличной от директории сервиса командой:

```
sudo /opt/arqasrv/quik/qadminsrv/q_stop.sh
```

2. Скопируйте файл install_qadminsrv-xx.xx.xx.run в директорию, на операции в которой у текущего пользователя есть права, например, домашний каталог (/home/<user> или ~/).



3. Выполните команду добавления прав на выполнение run-файлу:

```
chmod +x install_qadminsrv-xx.xx.xx.run
```

4. Выполните команду обновления сервиса:

```
sudo ./install_qadminsrv-xx.xx.xx.run -u
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя.

В результате выполнения run-файла будут выполнены следующие действия:

- Выполнено автоматическое резервное копирование. В директории, где установлен сервис – /opt/arqasrv/quik/qadminsrv, в поддиректории .backup будет создан архив qadminsrv_YYYY.MM.DD_hh.mm.ss.tar.gz, в который будут помещены все файлы обновляемого сервиса, кроме лог-файлов и файлов хранилищ, актуальных только внутри дня.
- В директории обновляемого сервиса будет произведена замена прежних файлов новым набором файлов.
- Пользователь arqasrv будет назначен владельцем всех обновленных файлов и поддиректорий в директории сервиса.
- При необходимости будет выполнена конвертация настроек в конфигурационных файлах.

При успешном обновлении сервиса в консоль выводится сообщение:

«Update of service "qadminsrv" has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

Отложенные файлы от предыдущих установок могут накапливаться, поэтому рекомендуется периодически удалять архивы из каталога .backup.

Удаление сервиса

Удаление сервиса производится пользователем root вызовом скрипта uninstall.sh, который находится в каталоге соответствующего сервиса.

Далее приведен порядок действий при удалении сервиса с именем по умолчанию – qadminsrv.

Для удаления сервиса выполните следующие действия:

1. Остановите службу сервиса qadminsrv из директории с установленным сервисом командой:



```
sudo ./q_stop.sh
```

либо из любой директории, отличной от директории сервиса командой:

```
sudo /opt/arqasrv/quik/qadminsrv/q_stop.sh
```

2. В случае, если управление установленным сервисом выполнялось пользователем arqasrv, выполните следующие действия:

- _ Заберите у пользователя arqasrv права на выполнение скриптов управления сервисом от имени root, выполнив следующие действия:
- _ Выполните команду:

```
sudo visudo
```

- _ В открывшемся vi-подобном редакторе удалите строку:

```
arqasrv ALL=(root) /opt/arqasrv/quik/qadminsrv/q_start.sh,  
/opt/arqasrv/quik/qadminsrv/q_stop.sh
```

- _ Снимите признак неизменяемости со скриптов управления сервисом, выполнив следующие команды:

```
chattr -i /opt/arqasrv/quik/qadminsrv/q_start.sh  
chattr -i /opt/arqasrv/quik/qadminsrv/q_stop.sh
```

3. В директории установленного сервиса /opt/arqasrv/quik/qadminsrv запустите командный файл uninstall.sh командой:

```
sudo ./uninstall.sh
```

либо из любой директории, отличной от директории сервиса командой:

```
sudo /opt/arqasrv/quik/qadminsrv/uninstall.sh
```

Для выполнения команды может потребоваться ввести пароль текущего пользователя. В результате выполнения команды будут выполнены следующие действия:

- _ Удаляется регистрация сервиса с именем qadminsrv в системе управления службами systemd.



- Удаляется файл /etc/arqasrv/qadminsrv, в котором были зафиксированы параметры установленного сервиса.
- Директория, в которой установлен сервис /opt/arqasrv/quik/qadminsrv, переименовывается в /opt/arqasrv/quik/qadminsrv.backup_YYYY.MM.DD_hh.mm.ss. Переименование, а не удаление директории производится на случай, если потребуются данные из нее. Если такой потребности нет, удалите эту директорию вручную.

При успешном удалении сервиса в консоль выводится сообщение:

«Removing of service “qadminsrv” has been successfully completed».

В случае вывода другой диагностики, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

2.8.5 Миграция сервиса qadminsrv с ОС Windows на ОС Linux

При миграции ПО с ОС Windows на ОС Astra Linux необходимо учитывать следующие ограничения Linux-версии по сравнению с Windows-версией:

- Для ОС Astra Linux поддержана работа только с СУБД PostgresPRO. При использовании БД сервера QUIK на СУБД, отличной от указанной, необходимо сначала выполнить миграцию БД на PostgresPRO. Для получения инструкции по миграции БД на PostgresPRO обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.
- Отсутствует поддержка криптопровайдера MP.
- Для переноса ПО, работающего на ОС Windows, на компьютер с ОС Astra Linux:
 - Версия ПО, которая переносится с ОС Windows, должна быть равна версии ПО, которая будет устанавливаться на ОС Astra Linux.
 - Перенос должен осуществляться в строго неторговое время: после завершения торгов и остановки сервиса, и до начала торгов, перед первым запуском сервиса.

Перед миграцией сервиса с ОС Windows на ОС Linux необходимо выполнить обновление всех используемых плагинов для QUIK Administrator до версий, указанных ниже:

- EES 2.30.100;
- QME 2.2.100;
- InvAdvDistributor 3.11.100;
- Instructions 20.7.100;
- BrokerQuote 4.48.100;
- OMS 6.2.100;
- POService 1.9.100;
- QuikAuctions 1.1.100;
- QChatGate 1.14.100;
- QuikREPO 1.2.100;
- SecDescDistributor 3.4.100;
- SMS 3.19.100;
- SOR 4.8.100.



Для получения соответствующего обновления обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

Перенос сервиса на ОС Astra Linux должен производиться пользователем root.

Для ОС Linux должны быть выполнены преобразования для всех перенесенных файлов в соответствии с [правилами преобразования ini-файлов при миграции ПО с ОС Windows на ОС Linux](#).

Для переноса ПО с ОС Windows на ОС Astra Linux выполните следующий порядок действий:

1. Установите сервис, выполнив [действия](#).
2. Скопируйте из директории Windows-сервиса в директорию Linux-сервиса /opt/arqasrv/quik/qadminsrv следующие файлы:
 - _ Конфигурационные файлы .ini;
 - _ Файлы настроек криптопровайдеров .cfg;
 - _ Файлы ключей (.txk), каталоги сертификатов провайдеров:
 - _ Ключи secring.txk, pubring.txk – для настройки криптопровайдера qcrypto32;
 - _ Каталог certs – для настройки криптопровайдера OpenSSL_pr;
 - _ Каталог signalcom – для настройки криптопровайдера Signalcom_pr.
3. Приведите имена скопированных в предыдущем пункте файлов и директорий к нижнему регистру. Для этого выполните в директории /opt/arqasrv/quik/qadminsrv команду:

```
sudo ./postmigration.sh
```

4. Запустите сервис qadminsrv из директории сервиса командой:

```
sudo ./q_start.sh
```

либо командой:

```
sudo systemctl start qadminsrv
```

5. Проверьте, что сервис успешно запущен командой (из директории сервиса):

```
sudo ./q_status.sh
```



либо командой:

```
sudo systemctl status qadminsrv
```

В случае возникновения проблем, пожалуйста, обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

2.8.6 Создание учетной записи QUIK Administrator

С помощью программы **KeyGen** были созданы публичный и секретный ключи для администратора сервера QUIK. Подробнее о создании ключей см. файл `keygen.pdf` – руководство по использованию программы `keygen.exe`.

После создания ключей необходимо:

- Скопировать публичный ключ сервера (по умолчанию программа `keygen.exe` создает файл `a:\pubring.txk`) в каталог `\quikadministrator\client\Key\pubring.txk`. Данный ключ используется только для Информационно-торговой системы QUIK “broker”.
- Скопировать секретный ключ пользователя (по умолчанию программа `keygen.exe` сохраняет файл `a:\secreing.txk`) в каталог `\quikadministrator\client\Key\secreing.txk`. Данный ключ используется для пользователя администратора.
- Скопировать секретный ключ сервера (по умолчанию программа `keygen.exe` сохраняет файл `a:\secreing.txk`) в каталог `\quikadministrator\server\Key\secreing.txk`. Данный ключ используется только для Информационно-торговой системы QUIK “broker”.

Для создания учетной записи QUIK Administrator и назначения пользователю прав администратора запустите серверную часть QUIK Administrator с ключом `-set-admin-right`.

Формат использования:

```
qadminsrv.exe -set-admin-right -instance=[<instance>] -UID=[<UID>] -QUIK-key-  
filename=[<QUIK-key-filename>]
```

Где:

- `<instance>` – идентификатор базы данных. Идентификаторы баз данных перечислены в секции `[Instances]` файла `qadminsrv.ini`. Если сервер QUIK работает с одной БД, то параметр не обязателен.
- `<UID>` – идентификатор пользователя, которому должен быть присвоен ключ RSA. Если параметр не указан, и БД пустая, то создается новый пользователь.
- `<QUIK-key-filename>` – путь и имя файла с публичным ключом RSA. Может указываться относительный или абсолютный путь. Если имя и/или путь содержит пробелы, то значение заключается в кавычки, например, для ОС Windows: `«c:\path\to\file\somefile.txk»`, для ОС Linux: `«/path/to/file/somefile.txk»`. Если файл



содержит более одного публичного RSA-ключа, то используется первый из ключей, имеющих в файле. Если указан параметр <UID>, и для этого пользователя уже имеется ключ RSA, то данный параметр не обязателен.

Пример для ОС Windows:

```
qadminsrv.exe -set-admin-right -UID=350 -QUIK-key-  
filename="c:\path\to\file\somefile.txk"
```

Пример для ОС Linux:

```
./qadminsrv -set-admin-right -UID=350 -QUIK-key-filename=/path/to/file/somefile.txk
```

2.8.7 Регистрация пользователей системы QUIK

1. Запустите программу **QUIK Administrator**.
2. Выберите пункт меню **Сервер QUIK/Организации**. Добавьте свою организацию в справочник, заполнив все поля.
3. Выберите пункт меню **Сервер QUIK/Пользователи**. Добавьте в справочник пользователей учетную запись администратора системы QUIK. Для этого выберите из справочника наименование вашей организации, введите ФИО менеджера, проставьте период действия доверенности.

Список классов содержит наименования указанных в настройках классов бумаг.

Последовательно выберите каждый из них и нажмите кнопку «Менеджер» для установки прав на работу по данному классу.

4. В поле «Код фирмы» (вкладка «Права по классам» в окне редактирования пользователя) укажите идентификатор участника торгов в торговой системе. Поле «Коды клиентов у дилера» для менеджера не заполняется.
5. Настройте аутентификацию пользователя:
 - Для входа с использованием ключей. С помощью программы KeyGen [создайте](#) публичный и секретный ключи пользователя. На вкладке «Безопасность», в рамке «Ключи QUIK» нажмите кнопку «Изменить...». Загрузите ключ нажатием кнопки «Добавить».
 - Для использования механизма аутентификации по логину, требуется в программе QUIK Administrator задать логины пользователей:
 - Для входа по логину и паролю в домене – задайте логин в справочнике «Логины в другой системе авторизации».
 - При аутентификации допускается указывать логин как вместе с доменом, так и без него. Если домен указан, проверяется полное соответствие домена и логина. Если домен не указан, проверка логина выполняется для домена по умолчанию.



- Для входа по логину и паролю – задайте логин в окне редактирования пользователя на вкладке «Безопасность».

6. Аналогичным образом добавьте других пользователей вашей системы, устанавливая необходимые параметры доступа к системе, используя шаблоны прав. В поле ввода «Код клиента у дилера» введите символьный код, который менеджер будет использовать впоследствии для установки лимитов и идентификации пользователей при работе с системой.

Подробнее о работе с программой **QUIK Administrator** см. Руководство администратора к ней.

Система QUIK готова к работе!

Запустите Рабочее место QUIK, воспользовавшись ключами доступа и учетными данными вашего пользователя.

2.9 Настройка баннера Рабочего места QUIK

В Рабочем месте QUIK на панели инструментов может располагаться баннер, при нажатии на который открывается сайт (например, сайт брокера).

2.9.1 Настройка баннера

Чтобы настроить баннер, выполните следующие действия:

1. Скопируйте файл с изображением баннера в директорию quik\server\areas\banners.

Требования к файлу:

- формат файла – .bmp;
- разрешение – любое. Рекомендуемое разрешение – 468*60 пикселей;
- глубина цвета – 8 бит.

2. В директории quik\server\areas\banners в файле banners.ini задайте настройки в секции [url_set]:

- **url** – URL-адрес сайта.
- **image** – наименование файла с изображением баннера.

Пример:

```
[url_set]
url=http://www.broker-website-example.ru
image=broker.bmp
```

3. На компьютере, на котором запущен сервер QUIK, в файле quik\server\quik.ini задайте следующие настройки:

```
[natural_level_section]
```



```
module=banner_module  
[banner_module]  
module=dwbanner.dll
```

Настройка баннера для сервера и сервера доступа совпадает.

2.9.2 Отключение баннера

Чтобы отключить получение баннеров с сервера доступа, выполните следующие действия:

1. Убедитесь, что в файле настроек сервера доступа quik.ini в секции [natural_level_section] присутствует строка:

```
module=banner_module
```

2. Убедитесь, что в quik.ini сервера доступа присутствует секция:

```
[banner_module]  
module=dwbanner.dll
```

3. Убедитесь, что в секции [banner_module] quik.ini сервера доступа отображается значение ключа по умолчанию – «1»:

```
ignore_up_dwell=1
```

```
[banner_module]  
module=dwbanner.dll  
ignore_up_dwell=1
```

4. Убедитесь в наличии модуля dwbanner.dll и затем запустите сервер доступа.

После применения таких настроек баннер не будет отправляться с сервера на сервер доступа, и пользователи сервера доступа не будут его видеть.

2.9.3 Замена баннера

Чтобы заменить баннер, настройте схему следующим образом:

1. В директории .\areas\banners\ должен находиться .ini файл с настройками следующего вида:



```
[url_set]
url=c:\
image=test.bmp
```

где:

- значение ключа «url» – url, который открывается во Рабочем месте QUIK;
- «image» – имя файла в директории .\areas\banners\.

2. Замените старый файл на новый, с именем, отличным от имени текущего баннера (например, test2.bmp) в директорию .\areas\banners\.

3. Поменяйте значение ключа «image» в .ini файле на новое – «test2.bmp».

«URL» может быть изменен без изменения «image».

Также без изменения «image» и «url» можно добавить другой .ini файл с другим «url» и «image». В этом случае используется баннер из нового .ini файла.

2.10 Настройка вывода сообщений

Настройки позволяют задавать путь к директории приветственных сообщений для пользователей, которые сервер будет отправлять при их подключении:

```
[areas]
msg_all=./areas/msg_all
msg_priv=./areas/msg_priv/
```

Где:

- «msg_all» – корневая директория сообщений для всех пользователей. Значение по умолчанию: «./areas/msg_all».
- «msg_priv» – корневая директория индивидуальных сообщений для пользователей с определенным идентификатором. Значение по умолчанию: «./areas/msg_priv/».

Пример содержимого файла приветственного сообщения для всех пользователей:

- Расположение: «./areas/msg_all/hello.txt».
- Содержимое: «Приветствуем Вас на нашем сервере!».

Пример содержимого файла приветственного сообщения для пользователя с идентификатором 42:

- Расположение: «./areas/msg_priv/42/hello_42.txt»
- Содержимое: «До 31.01.2025 вам доступно совершение сделок со сниженной комиссией».



Если пользователю назначены приветственные сообщения из директории msg_priv, то сообщения из директории msg_all ему не отправляются.

Приветственные сообщения должны храниться в виде текстовых файлов. Максимальный размер текста сообщения 799 байт.

2.11 Настройка пересылки файлов

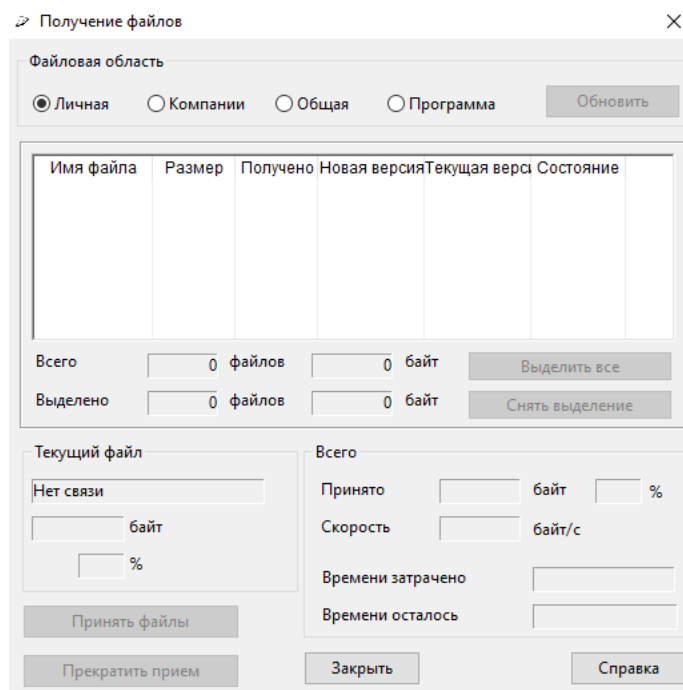
В системе QUIK можно пересылать файлы с сервера на Рабочие места QUIK (через персональные файловые области на сервере QUIK). Таким образом можно организовать распространение отчетов для клиентов, отчеты при этом могут быть подписаны ЭЦП.

Для отправки клиентам файлов, не предназначенных для обновления Рабочего места QUIK, файлы необходимо выкладывать в указанную директорию:

- server\areas\private\ – для отсылки конкретным пользователям.
- server\areas\public\ – для отсылки всем пользователям.

Для размещения документов и файлов, предназначенных для сотрудников компании, необходимо использовать директорию server\areas\company\.

После этого необходимо пользоваться диалогом «Система» / «Получение файлов»:



2.12 Настройка отправки произвольных файлов

В системе QUIK существует возможность пересылать произвольные файлы на Рабочие места QUIK, при подключении Рабочего места QUIK к серверу.



Для отправки произвольных файлов, их необходимо выкладывать в директорию, указанную в настройке `unrestricted` в секции `[areas]` файла `quik.ini`. Значение по умолчанию: `«areas/unrestricted»`.

Каждому файлу данного каталога должен соответствовать файл с таким же именем и расширением `.UNR`, который определяет правила рассылки.

Например, для отправки файла `test.txt` необходимо создать файл `test.txt.UNR`.

Файлы с расширением `.UNR` имеют следующую структуру:

Каждая настройка является обязательной.

- Секция `[common]`:
 - **file-location** – путь, по которому скачивается файл относительно каталога Рабочего места QUIK.
 - **alias** – строка до 128 символов, определяющая для Рабочего места QUIK назначение файла; в настоящий момент предполагается единственное значение:
 - `FRONTEND_ARBITRARY_FILE` – произвольный файл в каталоге Рабочего места QUIK.
 - **processing_mode** – строка, задающая способ отправки файла, возможные значения:
 - `ASK_CONFIRMATION` – файл скачивается после подтверждения пользователя;
 - `SILENT` – файл скачивается без подтверждения пользователя.
- Секция `[server]`:
 - **TARGET_LIST** – список UID адресатов-получателей, возможные значения:
 - `ALL` – файл отправляется всем пользователям;
 - список UID пользователей, через запятую – файл отправляется только перечисленным пользователям.
 - **VALID_FROM_DATE** – дата в формате `<ГГГГ.ММ.ДД>`, начиная с которой действуют описанные в данном файле правила рассылки. Значение по умолчанию: `«»` (пусто).
 - **VALID_TO_DATE** – дата в формате `<ГГГГ.ММ.ДД>`, до которой действуют описанные в этом данном файле правила рассылки. Значение по умолчанию: `«»` (пусто).
 - **VALID_FROM_TIME** – время в формате `<ЧЧ:ММ:СС>`, начиная с которого действуют описанные в данном файле правила рассылки. Значение по умолчанию: `«»` (пусто).
 - **VALID_TO_TIME** – время в формате `<ЧЧ:ММ:СС>`, до которого действуют описанные в данном файле правила рассылки. Значение по умолчанию: `«»` (пусто).



3. Запуск сервера QUIK

Сервер QUIK запускается как сервис. Из файлов хранилищ загружается рыночная информация, а также информация о заявках и сделках, которая доступна всем пользователям, подключенным к серверу QUIK. Это позволяет, например, выгружать информацию о сделках за предыдущий торговый день. Очистка данных за предыдущую торговую сессию происходит в момент подключения к серверу QUIK первого торгового интерфейса.

Запуск сервера QUIK также выполняется с использованием [ключей](#).

Для загрузки позиций сервером QUIK при его запуске необходимо скопировать подготовленный файл с расширением .lim на компьютер, где установлен сервер QUIK. Служба сервера QUIK при этом запускается с ключами, указывающими на необходимость загрузки позиций из этого файла. Например:

```
-clean -loadlimits <файл_с_лимитами>
```

При подключении модулей/интерфейсов к серверу QUIK загруженные позиции отобразятся в Рабочем месте QUIK.

При возникновении вопросов обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

3.1 Ключи запуска сервера QUIK

1. Ключи установки на [Windows](#) и [Linux](#) и удаления [Сервера](#), а также [установки](#) и [удаления](#) QUIK Administrator описаны в соответствующих пунктах.
2. Для корректной работы ключей запуска у пользователя должны быть права на директорию с установленным сервисом.
3. Если используется Linux версия, то при необходимости запуска сервера QUIK с передачей ключей в качестве сервиса, установленного как сервис systemd, используйте скрипт q_start.sh, который создается в директории при установке сервиса.



Если файл настроек Библиотеки расчета лимитов пустой либо отсутствует, то запуск сервера QUIK прерывается с выводом диагностики в лог-файл.

3.1.1 -new или /n

Запуск сервера QUIK в режиме загрузки с новыми данными, при котором:

- из торговой системы запрашиваются биржевая информация и данные о заявках и сделках;
- позиции клиентов рассчитываются на основе полученной информации с учетом сделок за текущую сессию и корректировок позиций;
- очищаются все файлы с расширением .ik, кроме следующих:
 - файл новостей (news.ik);
 - файл серверных QPILE-портфелей (cstructp.ik);
 - файл позиций по деньгам (mlimit.ik);
 - файл позиций по инструментам (dlimit.ik).

Ключ может использоваться в комбинации с ключом [-rolling](#).

3.1.2 -clean или /c

Запуск сервера QUIK в режиме загрузки с полной очисткой данных, а также очистка всех файлов с расширением .ik.

Если указать ключи -new и -clean одновременно, то будет использоваться ключ -clean.

Ключ может использоваться в комбинациях с ключами:

- [-loadlimits](#);
- [-rolling](#) и [-loadlimits](#).

3.1.3 -old или /o

Запуск сервера QUIK в режиме загрузки со старыми данными без очистки хранилищ.

3.1.4 -holiday или /h

Запуск сервера QUIK в режиме выходного дня в день, являющийся рабочим согласно стандартному календарю или в соответствии с настройками секции [\[trade_date\]](#) файла trade_dates.ini.



3.1.5 -workday или /w

Запуск сервера QUIK в режиме рабочего дня в день, являющийся выходным согласно стандартному календарю или в соответствии с настройками секции [\[trade_date\]](#) файла trade_dates.ini.

3.1.6 -loadlimits или /l

Запуск с сервера QUIK с загрузкой позиций из файла. После ключа в командной строке указывается имя файла с позициями и путь к нему. Форматы полей загружаемых позиций приведены в [Приложении](#). Информация по позициям, загруженным из файла, обновляется после подключения торговых интерфейсов или Информационного интерфейса Holiday.

Ключ может использоваться в комбинации с ключами [-clean](#) и [-rolling](#).

3.1.7 -removestops или /rs

Остановка обработки условных заявок, принадлежащих данному серверу QUIK. Выполняется путем принудительной установки идентификатора принадлежности стоп-заявок в значение «Другой» в терминах таблицы стоп-заявок Рабочего места QUIK или foreign в терминах таблицы Stop Orders Программного интерфейса QMonitor. Команда требует подтверждения пользователем. Подробнее см. п. [переноса стоп-заявок](#).

После запуска пользователям необходимо сделать своими стоп-заявки на любом другом сервере, чтобы эти заявки могли срабатывать.

Команда «Remove all stoporders» или запуск с ключом -removestops – это аварийный для сервера случай, после которого сервер теряет информацию о принадлежности имеющихся стоп-заявок. Поэтому необходимо, чтобы были созданы условия для полной репликации текущих меток. Например, штатный перезапуск (по расписанию) на следующий день, подключение Репликатора и всех торговых интерфейсов во всем контуре. Возвращать стоп-заявки лучше на следующий день, до начала торгов или после их окончания.

Ключ -removestops может использоваться в комбинации с ключами -new, -clean.

3.1.8 -text или /t

Вывод данных определенного типа в текстовый файл.

Формат использования:

```
quik.exe -text [<FILE>] [<TYPE>] [tsv]
```



где:

- <FILE> – экспортируемый файл с заявками или сделками.
- <TYPE> – тип данных. Возможные значения:
 - «orders» – экспорт из файла заявок (order.ik);
 - «trades» – экспорт из файла сделок (trade.ik).

Если названия файлов заявок и сделок отличны от order.ik и trade.ik, то параметр <TYPE> обязателен.

- tsv – преобразование файла в tsv-формат.

Пример для ОС Windows:

```
quik.exe -text trade.ik trades tsv > trade.txt
```

Пример для ОС Linux:

```
./quik -text trade.ik trades tsv > trade.txt
```

3.1.9 -removelimits или /rl

Запуск с очисткой информации о позициях клиентов по деньгам и инструментам, а также ограничений по счетам на срочном рынке. Прочие данные (например, заявки, сделки, данные Таблицы текущих торгов и т.д.) не удаляются. Ключ можно использовать в комбинации с ключом -loadlimits.

3.1.10-rolling или /ro

Запуск сервера QUIK с роллированием позиций. Информация по перенесенным позициям обновляется только после подключения торговых интерфейсов или Информационного интерфейса Holiday.

Ключ может использоваться в комбинации с ключами:

- [-clean](#), [-loadlimits](#);
- [-new](#).

3.1.11-v или /v

Запуск сервера QUIK в консольном режиме для вывода информации о версии сервера.



Пример для ОС Windows:

```
quik.exe -v
```

Пример для ОС Linux:

```
./quik -v
```

Формат версии сервера QUIK, отображаемый в консоли:

```
QUIK SERVER, version <Мажорная версия>.<Минорная версия>.<Номер патча>.<Номер сборки>
```

3.1.12-clean -loadlimits

Запуск сервера QUIK в режиме загрузки с полной очисткой данных, а также очистка всех файлов с расширением .ik и загрузка позиций из файла. Позиции пересчитываются с учетом сделок за текущую сессию, но не учитываются корректировки позиций в течение торгового дня (необходимо выполнить корректировки повторно).

3.1.13-clean -loadlimits -rolling

Запуск сервера QUIK в режиме загрузки с полной очисткой данных, а также очистка всех файлов с расширением .ik. При этом файл, содержащий позиции на момент завершения предыдущего торгового дня, используется как источник данных для роллирования.

Форматы полей загружаемых позиций приведены в [Приложении](#).

4. Шифрование паролей

Пароли, задаваемые в настройках, могут быть зашифрованы. Пароль не должен начинаться с символов «\$» и «#». Если используется пароль, который начинается с одного из указанных символов, то такой пароль следует изменить.

Для включения шифрования пароля добавьте в файле настроек символ «\$» перед текстом пароля.

Например:

```
Password=$secret
```



При попытке использования пароля сервер зашифрует его и сохранит в файл настроек в зашифрованном виде. Зашифрованный пароль маркируется символом «#» в начале строки.

При переносе программы на другой компьютер или переустановке операционной системы зашифрованные пароли становятся недоступными для дешифрования. В таком случае необходимо указать соответствующие пароли заново.

5. Приложение

5.1 Формат позиций

Параметры, обязательные для заполнения, отмечены символом «*».

Формат позиции по инструментам:

Параметр	Значение	Размер, точность (в символах)
* DEPO:	Заголовок строки с отражаемой позицией по инструментам	
* FIRM_ID	Идентификатор участника торгов	12
* SECCODE	Код инструмента	12
* TRDACCID	Торговый счет	12
* CLIENT_CODE	Код клиента	12
* OPEN_LIMIT	Входящий лимит	15
* OPEN_BALANCE	Позиция клиента	15
CURRENT_LIMIT	Текущий лимит	15
WA_POSITION_PRICE	Цена приобретения	15
WA_PRICE_CURR_CODE	Валюта цены приобретения	12



Параметр	Значение	Размер, точность (в символах)
LIMIT_KIND	Срок расчетов. Возможные значения: _ «0» – для текущих лимитов; _ «<N>» – для лимитов по позициям с расчетами T+<N>; _ значение меньше нуля – для технологических лимитов; _ «<ГГГГММДД>» – для лимитов по позициям, которые ведутся в календарных днях	10

Формат позиций по деньгам:

Параметр	Значение	Размер, точность (в символах)
* MONEY:	Заголовок строки с отражаемой денежной позицией	
* FIRM_ID	Идентификатор участника торгов	12
* CURR_CODE	Код валюты	12
* TAG	Тег расчетов	4
* CLIENT_CODE	Код клиента	12
OPEN_LIMIT	Входящий лимит	15
* OPEN_BALANCE	Позиция клиента	15
CURRENT_LIMIT	Текущий лимит	15
LIMIT_KIND	Срок расчетов. Возможные значения: _ «0» – для текущих лимитов; _ «<N>» – для лимитов по позициям с расчетами T+<N>; _ значение меньше нуля – для технологических лимитов; _ «<ГГГГММДД>» – для лимитов по позициям, которые ведутся в календарных днях	15
LEVERAGE	Плечо. Возможные значения: _ Неотрицательные значения; _ «-1» – плечо отсутствует	15



Пример записей в файле позиций:

```
MONEY: FIRM_ID = NC0038900000; TAG = EQTS; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = -46.52; OPEN_LIMIT = 0.00;
MONEY: FIRM_ID = NC0038900000; TAG = EQTS; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = -46.52; LEVERAGE = -1;
MONEY: FIRM_ID = NC0038900000; TAG = EQTV; CURR_CODE = SUR ; CLIENT_CODE = 004;
OPEN_BALANCE = 1048.51; OPEN_LIMIT = 450000.00; LIMIT_KIND = 1;
DEPO: FIRM_ID = NC0038900000; SECCODE = HYDR; CLIENT_CODE =10004/10004; OPEN_BALANCE
= 113955; OPEN_LIMIT = 0; TRDACCID = L01-00000F00;
DEPO: FIRM_ID = NC0038900000; SECCODE = IRAO-004D; CLIENT_CODE =10006/10006;
OPEN_BALANCE = 738467; OPEN_LIMIT = 0; TRDACCID = L01-00000F00; LIMIT_KIND = 1;
```

Формат профиля клиента:

Параметр	Значение
CLPROF:	Заголовок строки с профилем клиента
*FIRM_ID	Идентификатор участника торгов
*CLIENT_CODE	Код клиента
COMM	Идентификатор комиссионного шаблона. Диапазон значений от 0 до 65535
MARG	Идентификатор маржинального шаблона. Диапазон значений от 0 до 65535
REST	Идентификатор шаблона ограничений. Диапазон значений от 0 до 65535
CIMSK	Маска сложного финансового инструмента. Диапазон значений от 0 до 18446744073709551615

Пример:

```
CLPROF: FIRM_ID = NC0038900000; CLIENT_CODE = Q1; COMM = 1; MARG = 2; REST = 3; CIMSK
= 0;
```

5.2 Правила преобразования ini-файлов при миграции ПО с ОС Windows на ОС Linux

Для файлов и путей необходимы следующие преобразования:

- Наименования файлов и путей должны быть в нижнем регистре.



- Все упоминания динамических библиотек (.dll) должны быть преобразованы в соответствующее наименование на Linux. Для этого к имени добавляется префикс «lib», а расширение заменяется на .so, например:

```
module=openssl_pr.dll  
замените на:  
module=libopenssl_pr.so
```

- Разделители путей – обратный слеш («\») должен быть заменен на прямой («/»).

Настройки, которые содержат пути к файлам, находящимся на сервере QUIK, необходимо изменить таким образом, чтобы путь был корректным в семантике ОС Linux.

Если сервер QUIK установлен на отдельном компьютере, необходимо выполнить подключение сетевого ресурса командой от имени пользователя root, при этом необходимо наличие установленного пакета cifs-utils, входящего в дистрибутив AstraLinux.

Например, настройка QuikIni секции [DealerLibraryOptions] для ОС Windows имеет вид:

```
[DealerLibraryOptions]  
QuikIni=\\QUIKSERVER\DRIVE_D\QUIK1\Server\quik.ini
```

На компьютере, где установлен сервер QUIK с сетевым именем QUIKSERVER доступен ресурс DRIVE_D.

Выполняется подключение сетевого ресурса командой:

```
sudo mount.cifs //QUIKSERVER/DRIVE_D/ /mnt/q1/ -o uid=argasrv,user=winuser
```

Где:

- QUIKSERVER – имя компьютера, где установлен сервер QUIK;
- DRIVE_D – имя сетевого ресурса;
- /mnt/q1/ – путь подключения сетевого диска (директория должна существовать);
- argasrv – пользователь Linux, от имени которого запускается сервис QUIK;
- winuser – пользователь Windows, которому разрешено подключение сетевого ресурса.

После выполнения подключения сетевого ресурса настройка имеет вид (путь регистрозависим):

```
[DealerLibraryOptions]  
QuikIni=/mnt/q1/QUIK1/Server/quik.ini
```



Файлы Библиотеки расчета лимитов, перечисленные в секции [dealer-library] должны быть доступны для записи пользователю, от имени которого выполнялось подключение сетевого ресурса.

За подробной информацией о подключении сетевых ресурсов в ОС Linux рекомендуем обращаться к системному администратору.

5.3 Настройка Сервера QUIK для аутентификации в домене Active Directory / Kerberos

Для настройки аутентификации в домене Active Directory / Kerberos необходимо включить соответствующий режим в [настройках файла crypto.cfg](#) сервера QUIK и в [настройках сервера qadminsrv.ini](#).

Аутентификация в домене Active Directory / Kerberos может работать в трех режимах:

- В качестве второго фактора аутентификации используется доменный пароль пользователя Active Directory.
- В качестве первого фактора аутентификации в режиме «2» – «По логину и паролю в домене».
- В качестве первого фактора аутентификации в режиме «32» – «Внутри домена (SSO)».

При работе в любом из этих режимов необходимо указать логин пользователя Active Directory в настройках пользователя, в справочнике «Логины в другой системе авторизации» (подробнее см. [настройку аутентификации в Active Directory](#)).

Режимы аутентификации первого фактора в домене Active Directory доступны только при использовании провайдеров `tp_pr` (недоступно в Linux) и `openssl_pr` в качестве провайдеров шифрования.

Особенности использования схемы аутентификации «Внутри домена» (32):

1. При расположении сервера QUIK на платформе с ОС Windows требуется, чтобы компьютер с сервером QUIK, где выполняется аутентификация, был включен в домен Active Directory.
2. При расположении сервера QUIK на платформе с ОС Linux требуется:
 - включение компьютера с сервером QUIK, где выполняется аутентификация, в домен Active Directory, либо подключение иными способами к службе;
 - доступ к сервису Kerberos;
 - у пользователя, под которым запускается сервер QUIK, должно быть достаточно прав для доступа к `keytab`-файлу с аутентификационными записями для выполнения операций.
3. Включение в домен необходимо только для серверов нулевой зоны.



4. Включение компьютеров с Серверами доступа (СД) не требуется независимо от ОС платформы с СД.
5. Требуется корректно задать следующие настройки в ini-файлах соответствующих провайдеров (см. настройку криптопровайдеров [openssl_pr](#) и [mp_pr](#)):

- _ **spn_sspi** – SPN сервера для Windows. Значение по умолчанию: «» (пусто).
- _ **spn_gss** – SPN сервера для Linux. Значение по умолчанию: «» (пусто).

В данной настройке указывается SPN сервера нулевой зоны – компьютера, который выполняет валидацию пользователя. Если данная настройка не задана, корректная работа SSO невозможна.

Также данная настройка указывается для Серверов доступа. Значение настройки должно совпадать со значением на сервере, к которому подключен Сервер доступа.

Значение настроек задается в виде SPN-записей для компьютера, который выполняет валидацию пользователя, и является ОС-зависимой.

Например:

```
spn_sspi=RestrictedKrbHost/qfront.arqa.ru
spn_gss=restrictedkrbhost/qfront.arqa.ru@ARQA.RU
```

Получить значение настройки для хоста с ОС Windows можно выполнив команду:

```
>setspn -l qfront
RestrictedKrbHost/QFRONT
HOST/QFRONT
RestrictedKrbHost/QFRONT.arqa.ru
HOST/QFRONT.arqa.ru
```

Из списка значений следует выбрать то, которое начинается с RestrictedKrbHost и содержит полное имя домена как в примере выше.

Получить значение настройки для хоста с ОС Linux можно с помощью утилиты ktutil и следующей последовательности команд (вывод усечен, здесь указан файл ключей Kerberos, заданный по умолчанию, если используется другой файл с ключами, следует указать его):

```
#ktutil
ktutil: read_kt /etc/krb5.keytab
ktutil: list -k -e
slot KVNO Principal
1      1 restrictedkrbhost/qserver.arqa.ru@ARQA.RU (aes256-cts-hmac-sha1-96)
```



```
2      1  restrictedkrbhost/QSERVER@ARQA.RU (aes256-cts-hmac-sha1-96)
3      1  host/qserver.arqa.ru@ARQA.RU (aes256-cts-hmac-sha1-96)
4      1  host/QSERVER@ARQA.RU (aes256-cts-hmac-sha1-96)
```

Из списка значений следует выбрать то, которое начинается с `restrictedkrbhost` и содержит полное имя домена как в примере выше.

Указать `keytab`-файл, отличный от заданного по умолчанию, можно, добавив в переменные окружения сервиса запись:

```
KRB5_KTNAME=/path/to/mykeytab
```

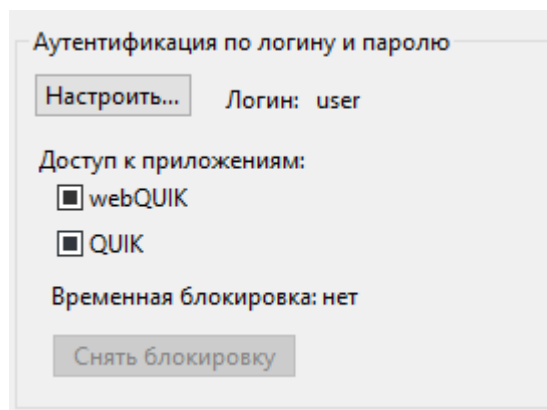
Где:

— `/path/to/mykeytab` – полный путь к `keytab`-файлу.

5.3.1 Аутентификация по логину и паролю

Схема аутентификации клиента по логину пользователя и паролю настраивается в программе `QUIK Administrator`.

Выберите пункт меню `Сервер QUIK / Пользователи` и выполните настройки в форме редактирования пользователя:



1. «Настроить...» – настройка логина и пароля пользователя.
2. «Логин» – текущий логин пользователя.
3. «Доступ к приложениям:»
 - «webQUIK» – при установленном признаке пользователю настраиваются права на доступ в систему `webQUIK`;
 - «QUIK» – при установленном признаке пользователю настраиваются права на доступ в систему `QUIK`.



4. «Временная блокировка» – признак блокировки учетной записи пользователя в результате ввода неверных данных для аутентификации заданное количество раз. Если учетная запись не заблокирована, отображается «нет», иначе – дата и время окончания периода блокировки в формате <ДД.ММ.ГГГГ, ЧЧ:ММ>. Блокировка снимается при нажатии на кнопку «Снять блокировку».

В окне «Аутентификация по логину и паролю» доступны следующие параметры:

Настройки логина и пароля

Логин
client205

Пароль

Тип пароля: постоянный
Создан: 17.01.2020, 12:21
Истекает: 16.01.2021, 12:21, через 364 дн. 23 ч. 59 мин.

Срок действия постоянного пароля:
 дней

Новый пароль
Пароль должен содержать не менее 8 символов, включать латинские буквы в верхнем и нижнем регистре и цифры. Допускается использование символов "-" и "_".
 ☐ Показать

☐ Запросить изменение пароля при следующем входе

1. «Логин» – логин пользователя.

Недопустимо использование логина, который отличается от логина, уже зарегистрированного на сервере, только регистром.

При нажатии на кнопку «Удалить логин» логин удаляется после предварительного подтверждения. Окно «Аутентификация по логину и паролю» закрывается, в окне редактирования настроек пользователя логин переводится в положение «не задан».

2. «Тип пароля»: «временный» / «постоянный».
3. «Создан» – дата и время создания пароля.
4. «Истекает» – дата и время окончания срока действия пароля.
5. «Срок действия постоянного пароля» – срок действия пароля. Допустимые значения: целые числа от «1» до «365».
6. «Новый пароль» – пароль пользователя. Длина пароля должна быть не менее 8 знаков. Допустимые символы: «А» – «Z», «0» – «9», «-» (тире) и «_» (подчеркивание) с учетом регистра. Чтобы посмотреть введенный пароль, установите флажок «Показать».



7. «Запросить изменение пароля при следующем входе» – признак необходимости смены пароля при следующем входе. Значение по умолчанию:

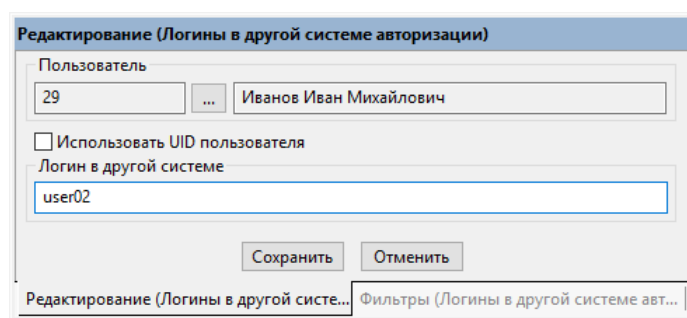
- Включен – при создании нового пользователя;
- Выключен – при редактировании пользователя.

Настройка аутентификации завершается нажатием кнопки «Сохранить». Кнопка «Отменить» закрывает окно без сохранения изменений.

5.3.2 Настройка аутентификации в Active Directory

Если на сервере настроена схема аутентификации клиента по Active Directory (далее «AD») по логину и паролю либо внутри домена (SSO) (значение настройки ServerHandShakeScheme в секции [TLS Connection Settings] файла openssl_pr.ini равно «2» или «32»), то в программе QUIK Administrator необходимо добавить соответствие между пользователем и идентификатором (логин). Для этого выберите пункт меню **Сервер QUIK / Безопасность / Логины в другой системе авторизации**.

Выбором в контекстном меню таблицы пункта «Добавить» открывается форма добавления нового логина в другой системе авторизации:



Назначение полей окна:

1. «Пользователь» – введите UID пользователя или выберите его из справочника нажатием кнопки «...». В поле справа отображаются фамилия, имя и отчество пользователя.
2. «Использовать UID пользователя» – признак использования UID клиента в качестве идентификатора пользователя при проверке токен-кода. В этом случае клиент при подключении к серверу не обязан вводить какой-либо идентификатор (логин) на этапе аутентификации с помощью токена.
3. «Логин в другой системе» – введите значение логина пользователя. Поле недоступно для изменения, если включен признак «Использовать UID пользователя».

Нажатием кнопки «Сохранить» настройки пользователя сохраняются. Кнопка «Отменить» служит для выхода из окна добавления нового логина.



5.4 Настройка OpenSSL

Для проверки ЭЦП на компьютерах, где расположены сервер QUIK и серверной части QUIK Administrator, должны быть установлены все необходимые корневые сертификаты УЦ. Файлы с данными сертификатами загружаются из внешних источников и могут быть в формате .p7b, .pfx, .pem, .cer.

Криптопровайдер OpenSSL предоставляет сервисы для использования электронной цифровой подписи (ЭЦП) и шифрования по протоколу TLS.

Работа с шифрованием и ЭЦП осуществляется с использованием криптографических функций, предоставляемых библиотекой OpenSSL.

Криптопровайдер OpenSSL предоставляет весь необходимый функционал для построения TLS защищенных каналов и создания / проверки ЭЦП, а именно:

- Создание ключевых пар (public/private key);
- Создание запросов на сертификаты, соответствующие созданным ключам;
- Установка выпущенных по запросу сертификатов в соответствующее хранилище сертификатов ОС;
- Аутентификация пользователя по сертификату, по имени и паролю, а также по имени и паролю с использованием контроллера домена.

5.4.1 Установка и настройка программы

1. В корневой директории сервиса создайте поддиректории:

- _ certs/ca – для хранения файла корневого сертификата;
- _ certs/crl – для хранения списков отзыва;
- _ client/serial – для размещения клиентских сертификатов, предназначенных для проверки подписи транзакций.

Скопируйте корневой сертификат, списки отзыва и клиентские сертификаты в соответствующие поддиректории.

2. В корневой директории сервиса создайте файл [openssl_pr.ini](#) со следующими настройками:

```
[General]
CertStoreFile=certs\store.pem
ServerCertificateKey=<ключ сертификата сервера>

[TLS Connection Settings]
CA=certs/ca
CRL=certs/crl

ServerHandShakeScheme=<поддерживаемый режим аутентификации>
UsedHandShakeSchemePrefer=<предпочтительный режим аутентификации>
```



```
ServerCertificateFile=certs\server.crt  
ServerPrivateKeyFile=certs\server.key
```

3. Укажите в файле qcrypto.cfg сервера QUIK следующие настройки провайдера:

```
[CryptoProviders]  
openssl=1  
  
[openssl]  
Module=openssl_pr.dll      полный или относительный путь до исполняемого файла;  
IniFile=openssl_pr.ini     полный или относительный путь до файла с настройками  
  
[auth]  
sign=secprov.dll  
sign_provider=openssl
```

4. В файле quik.ini сервера QUIK в секции [usend_module] добавьте ключ crypto_provider_ini_file:

```
[usend_module]  
crypto_provider_ini_file=openssl_pr.ini      полный или относительный путь до файла  
с настройками
```

Если провайдеров несколько, тогда для задания настроек нужно использовать настройку «crypto_provider_ini_file_openssl» – ключ для задания криптопровайдера OpenSSL.

5. Если используется QUIK Administrator, то в корневой директории программы добавьте в qadminsrv.ini следующие настройки:

- В секции [CryptoProviders] перечислите доступных провайдеров:
 - «openssl» – признак использования провайдера OpenSSL. Возможные значения:
 - «0» – провайдер отключен;
 - «1» – провайдер включен.

Пример:

```
[CryptoProviders]  
openssl=1
```



- В секции [openssl] задайте настройки:
 - «Module» – путь к модулю провайдера. Значение по умолчанию для ОС Windows: «openssl_pr.dll». Значение для ОС Linux: «libopenssl_pr.so».
 - «IniFile» – путь к файлу настроек провайдера. Значение по умолчанию: «openssl_pr.ini».

Пример для ОС Windows:

```
[openssl]
Module=.\openssl_pr.dll
IniFile=.\openssl_pr.ini
```

Пример для ОС Linux:

```
[openssl]
Module=./libopenssl_pr.so
IniFile=./openssl_pr.ini
```

Для криптопровайдера «openssl_pr» корневые сертификаты копируются в соответствующую директорию «CA», указанную в файле настроек.

При расположении сервера QUIK Administrator на одном компьютере с сервером QUIK допускается использование ini-файлов, которые используются для настройки криптопровайдеров.

Если на одном сервере QUIK Administrator настроено использование двух или более экземпляров сервера QUIK Administrator, то они все используют единые настройки криптопровайдеров.

6. Запустите сервер QUIK и убедитесь в наличии следующих строк в файле events.log:

```
Crypto provider 'OpenSSL' initied           при использовании режима шифрования
Sign provider 'OpenSSL' initialized successfully   при использовании режима ЭЦП
```

7. [Зарегистрируйте ключи пользователя](#) в программе QUIK Administrator.

5.4.2 Регистрация ключей пользователя

Для просмотра списка зарегистрированных ключей в программе QUIK Administrator выберите пункт меню **Сервер QUIK / Безопасность / Ключи OpenSSL**. Список зарегистрированных ключей отображается в таблице справа.



Выберите пункт «Добавить» в контекстном меню таблицы, чтобы открыть окно регистрации нового ключа OpenSSL со следующими параметрами:

Редактирование (Ключи OpenSSL)

Пользователь

Пользователь

100787

...

Tech_User02

Из организации с кодом

1

ЗАО "ТестИнвест"

Имеет ключ

Владелец сертификата

/C=RU/SP=NSO/O=TESTINVEST/OU=Pos01/CN=Tech_User02/Email=techuser02@

№ сертификата

00D5 FA18 C976 975F 82

Удостоверяющий центр

/C=RU/SP=NSO/O=ARQA/CN=arqa.ru

Действует с

26.07.2017

По

26.07.2018

Ключ присвоен

26.07.2017 10:21:45

Ключ отозван

Доступные ключи

Номер сертификата	Удостоверяющий центр	Владелец
00D5 FA18 C976 975F 82	/C=RU/SP=NSO/O=ARQA/CN=arqa.ru	/C=RU/SP=NSO/O=TESTINVEST/OU=Pos01/C

<

>

Выбор ключа

☒ Использовать для подписи транзакций

☒ Использовать для шифрования потока данных

☐ Отозван

Сохранить

Отменить

<

>

Редактирование (Ключи OpenSSL)

Фильтры (Ключи OpenSSL)

1. «Пользователь»:

- «Пользователь» – введите UID пользователя или выберите его из справочника, нажав на кнопку «...». В поле справа отображаются фамилия, имя и отчество пользователя;
- «Из организации с кодом» – информационное поле, отображающее номер организации в справочнике. В поле справа отображается название организации.

2. «Имеет ключ» – поля заполняются автоматически при выборе ключа в таблице «Доступные ключи»:

- «Владелец сертификата» – данные о владельце сертификата;



- «Номер сертификата» – серийный номер сертификата, присвоенный данному пользователю;
- «Удостоверяющий центр» – данные об удостоверяющем центре, выпустившем сертификат.
- «Действует с ... По ...» – дата начала и окончания действия сертификата.

3. «Ключ присвоен» – дата и время присвоения ключа. Информационное поле.

4. «Ключ отозван» – дата и время отзыва ключа. Информационное поле.

5. «Доступные ключи» – перечень идентификаторов ключей, содержащихся в выбранном файле и доступных для использования. Информация представлена в виде таблицы, в столбцах отображаются следующие параметры:

Параметр	Назначение
Номер сертификата	Серийный номер сертификата
Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат
Владелец сертификата	Имя владельца сертификата
Алгоритм подписи	Наименование алгоритма, используемого для формирования ЭЦП
Алгоритм шифрования	Наименование алгоритма, используемого для потокового шифрования данных
Email	Email
Дата начала	Срок начала действия сертификата (выдачи)
Дата окончания	Срок окончания действия сертификата

- «Выбор ключа» – выбор файла с ключами.

6. «Использовать для подписи транзакций» – признак использования ключа из указанного сертификата для формирования электронной цифровой подписи на поручениях клиента.

7. «Использовать для шифрования потока данных» – признак использования сертификата для шифрования данных, передаваемых между пользователем и сервером брокера.

Перед использованием данного свойства обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

8. «Отозван» – при установленном признаке сертификат сохраняется в базе, но его использование запрещено.

Нажатием кнопки «Сохранить» настройки пользователя сохраняются. Кнопка «Отменить» служит для выхода из окна регистрации сертификатов.



Редактирование ключа доступно в карточке пользователя (меню Сервер QUIK / Пользователи) на вкладке «Безопасность».

5.4.3 Формат файла настроек шифрования OpenSSL

В файле openssl_pr.ini задаются настройки шифрования средствами библиотеки криптографии OpenSSL (www.openssl.org). Использование OpenSSL позволяет не хранить сертификаты в реестре ОС на платформе с сервером QUIK, что упрощает их установку и последующее обслуживание.

Секция [General]

- **CertStoreFile** – имя файла хранилища сертификатов. Значение по умолчанию: «certs\store.pem».
- **ServerCertificateKey** – пароль ключа сертификата сервера. Пароль должен быть [зашифрован](#).
- **NewServerCertHash** – новый хеш сертификата сервера.
- **NewServerCertDomainName** – новый домен сертификата сервера.

Настройки NewServerCertHash и NewServerCertDomainName задают параметры нового сертификата при плановой замене сертификата на сервере. После замены сертификата значения настроек NewServerCertHash и NewServerCertDomainName записываются в параметры ServerCertHash и ServerCertDomainName файла openssl_pr.ini в Рабочем месте QUIK.

- **ClientCertificatesDir** – путь к директории, содержащей сертификаты для проверки подписи. Значение по умолчанию: «certs\client».

Секция [TLS Connection Settings]

Секция содержит параметры соединения:

- **ServerHandShakeScheme** – поддерживаемая схема аутентификации. Возможные значения:
 - «1» – аутентификация по сертификату;
 - «2» – аутентификация в домене;
 - «4» – аутентификация по имени и паролю;
 - «7» (по умолчанию) – поддерживаются все схемы, кроме «8» (восстановление пароля);
 - «8» – восстановление пароля;
 - «32» – аутентификация внутри домена (по доменному имени пользователя).

При поддержке нескольких схем значение настройки задается в виде суммы значений, соответствующих поддерживаемым схемам.

- **UsedHandShakeSchemePrefer** – предпочтительная схема аутентификации. Выбирается, если у клиента выбран режим «0» (определяется сервером). Возможные значения:



- «1» – аутентификация по сертификату;
- «2» – аутентификация в домене по логину и паролю;
- «4» (по умолчанию) – аутентификация по имени и паролю;
- «8» – восстановление пароля;
- «32» – аутентификация внутри домена (по доменному имени пользователя).
- **SSLProtocols** – список допустимых к подключению версий протокола TLS через запятую. Возможные значения:
 - «TLSv1.0»;
 - «TLSv1.1»;
 - «TLSv1.2».
- **CA** – путь к директории, содержащей корневые сертификаты. Значение по умолчанию: «certs\ca».
- **CRL** – путь к директории, содержащей списки отозванных сертификатов (CRL). Значение по умолчанию: «certs\crl».
- **spn_sspi** – SPN сервера для Windows. Значение по умолчанию: «» (пусто).
- **spn_gss** – SPN сервера для Linux. Значение по умолчанию: «» (пусто).

5.5 Настройка MultiPurpose

Криптопровайдер MP используется только для ОС Windows.

Для проверки ЭЦП на компьютерах, где расположены сервер QUIK и серверной части QUIK Administrator, должны быть установлены все необходимые корневые сертификаты УЦ. Файлы с данными сертификатами загружаются из внешних источников и могут быть в формате .p7b, .pfx, .pem, .cer.

Криптопровайдер MultiPurpose (далее MP) предоставляет сервисы для использования электронной цифровой подписи (ЭЦП) и шифрования по протоколу SSL (TLS), полностью опираясь на встроенные в операционную систему Windows интерфейсы и протоколы.

Работа с ЭЦП осуществляется с помощью соответствующих криптопровайдеров (CSP), встроенных в ОС пользователя.

При использовании шифрования по протоколу SSL (TLS) процедура аутентификации и установления защищенного канала происходит с помощью интерфейса SSPI (Security Support Provider Interface) ОС Windows. Данный интерфейс позволяет использовать различные алгоритмы шифрования, поддерживаемые установленными в ОС провайдерами безопасности.

При необходимости возможна установка дополнительного ПО, реализующего алгоритмы, которые отсутствуют в базовом наборе ОС. Например, установив провайдер КриптоПро CSP, пользователь получает следующие возможности:



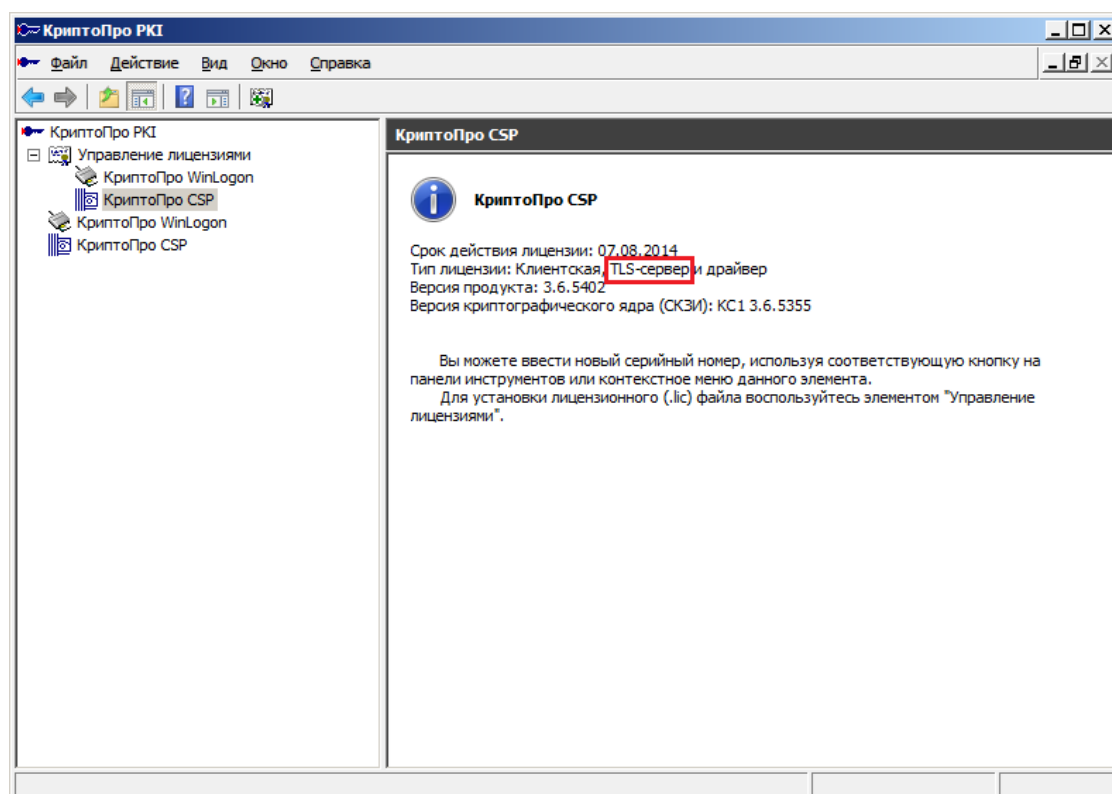
- Использовать для создания и проверки ЭЦП соответствующие ГОСТ алгоритмы для работы в режиме ЭЦП;
- Работать по защищенному SSL (TLS) каналу с использованием соответствующих ГОСТ алгоритмов.

Криптопровайдер МР предоставляет весь необходимый функционал для построения SSL (TLS) защищенных каналов и создания / проверки ЭЦП, а именно:

- Создание ключевых пар (public/private key). Если в качестве носителя ключевого контейнера используются брелоки JaCarta или eToken Pro (ГОСТ), то ключи создаются в неизвлекаемой памяти.
- Создание запросов на сертификаты, соответствующие созданным ключам.
- Установка выпущенных по запросу сертификатов в соответствующее хранилище сертификатов ОС.
- Аутентификация пользователя по сертификату, по имени и паролю, по имени и паролю через контроллер домена.

5.5.1 Установка и настройка программы

При использовании провайдеров КриптоПро CSP и Сигнал-КОМ CSP убедитесь, что установленное ПО провайдеров имеет серверную лицензию.



1. Поместите в рабочий каталог сервера QUIK файлы, необходимые для работы программы:

— mp_pr.dll;



— mp_pr.ini.

2. Укажите в файле qcrypto.cfg следующие настройки провайдера:

— В секцию [CryptoProviders] добавьте ключ mp=1:

```
[CryptoProviders]
...
mp=1
```

— Добавьте в файл секцию [mp] следующего вида:

```
[mp]
Module=mp_pr.dll          полный или относительный путь до исполняемого файла;
IniFile=mp_pr.ini         полный или относительный путь до файла с настройками
```

— Для использования ЭЦП укажите следующие ключи в секции [auth]:

```
[auth]
...
sign=secprov.dll
sign_provider=MP
```

3. В зависимости от используемого режима работы (шифрование или ЭЦП) пропишите соответствующие настройки в файле [mp_pr.ini](#). Следующие настройки являются обязательными к выполнению пользователем:

— Укажите в секции [CUSTOM_STORE] путь к файлу с хранилищем сертификатов .sto:

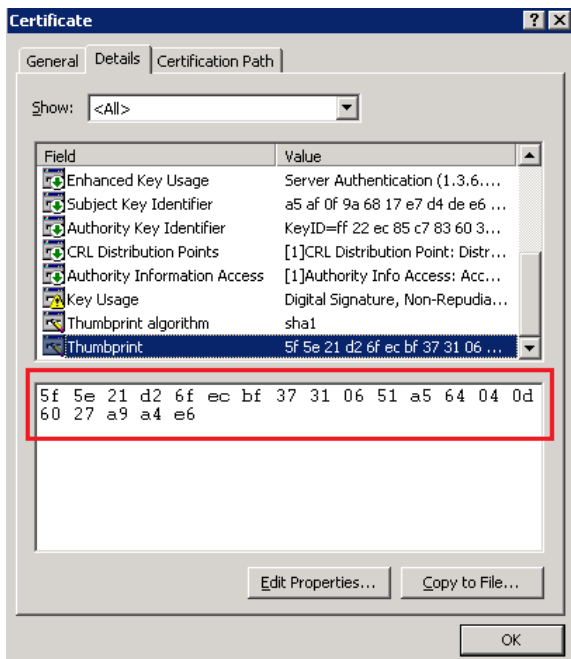
```
[CUSTOM_STORE]
...
LOCATION=.\usersto          полный или относительный путь до файла
хранилища
```

— Укажите в секции [TLS Connection Settings] значение ключа CSPCertHash:

```
[TLS Connection Settings]
...
CSPCertHash = хеш сертификата сервера
```

Для получения значения хеша сервера откройте созданный сертификат, искомое значение находится на вкладке Details в поле Thumbprint:





Скопируйте данное значение для ключа CSPCertHash, после чего обязательно уберите все пробелы.

4. В файле quik.ini сервера QUIK в секции [usend_module] добавьте ключ crypto_provider_ini_file:

```
[usend_module]
...
crypto_provider_ini_file=mp_pr.ini
```

полный или относительный путь до файла с настройками

Если провайдеров несколько, тогда для задания настроек нужно использовать настройку «crypto_provider_ini_file_mp» – ключ для задания криптопровайдера MP.

5. Запустите сервер QUIK и убедитесь в наличии следующих строк в файле events.log:

```
Crypto provider 'MP' initied           при использовании режима шифрования
Sign provider 'MP' initialized successfully  при использовании режима ЭЦП
```

6. [Зарегистрируйте ключи пользователей](#) в программе QUIK Administrator.

5.5.2 Регистрация ключей пользователей

Регистрация ключей пользователей выполняется в программе QUIK Administrator.



Для просмотра списка зарегистрированных ключей выберите пункт меню **Сервер QUIK / Безопасность / Ключи CSP SSPI**. Список зарегистрированных ключей отображается в таблице справа.

Выберите пункт «Добавить» в контекстном меню таблицы, чтобы открыть окно регистрации нового ключа CSP SSPI со следующими параметрами:

Редактирование (Ключи CSP SSPI)

Пользователь

Пользователь: Петров Петр Петрович

Из организации с кодом: ИК "Петрович"

Имеет ключ

Владелец сертификата:

№ сертификата:

Удостоверяющий центр:

Действует с: По:

Ключ присвоен:

Ключ отозван:

Доступные ключи

Номер сертификата	Удостоверяющий центр	Владелец сертификата	Алгоритм подписи
615C B602 0000 0000 0000 0014	/CN=PC-AGAR-TEST2-CA	/CN=Test client/C=RU	

Выбор ключа

☒ Использовать для подписи транзакций

☒ Использовать для шифрования потока данных

☐ Отозван

Редактирование (Ключи CSP SSPI) | Фильтры (Ключи CSP SSPI)

1. «Пользователь»:

- «Пользователь» – ручной ввод UID пользователя или выбор из справочника нажатием кнопки «...». В поле справа отображаются фамилия, имя и отчество пользователя;
- «Из организации с кодом» – информационное поле, отображающее номер организации в справочнике. В поле справа отображается название организации.

2. «Имеет ключ CSP SSPI» – поля заполняются автоматически при выборе ключа в таблице «Доступные ключи»:

- «Владелец сертификата» – данные о владельце сертификата;
- «Номер сертификата» – серийный номер сертификата, присвоенный данному пользователю;
- «Удостоверяющий центр» – данные об удостоверяющем центре, выпустившем сертификат.
- «Действует с ... по ...» – дата начала и окончания действия сертификата.



3. «Доступные ключи» – перечень идентификаторов ключей, содержащихся в выбранном файле и доступных для использования. Информация представлена в виде таблицы, в столбцах отображаются следующие параметры:

Параметр	Назначение
Номер сертификата	Серийный номер сертификата
Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат
Владелец сертификата	Имя владельца сертификата
Алгоритм подписи	Наименование алгоритма, используемого для формирования ЭЦП
Алгоритм шифрования	Наименование алгоритма, используемого для потокового шифрования данных
Email	Email
Дата начала	Срок начала действия сертификата (выдачи)
Дата окончания	Срок окончания действия сертификата

— «Выбор ключа» – выбор файла с ключами.

4. «Использовать для подписи транзакций» – признак использования ключа из указанного сертификата для формирования электронной цифровой подписи на поручениях клиента.
5. «Использовать для шифрования потока данных» – признак использования сертификата для шифрования данных, передаваемых между пользователем и сервером брокера.

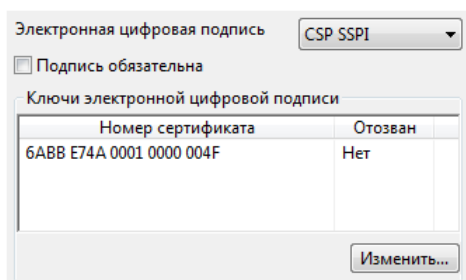
Перед использованием данного свойства обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

6. «Отозван» – при установленном флажке сертификат сохраняется в базе, но его использование запрещено.

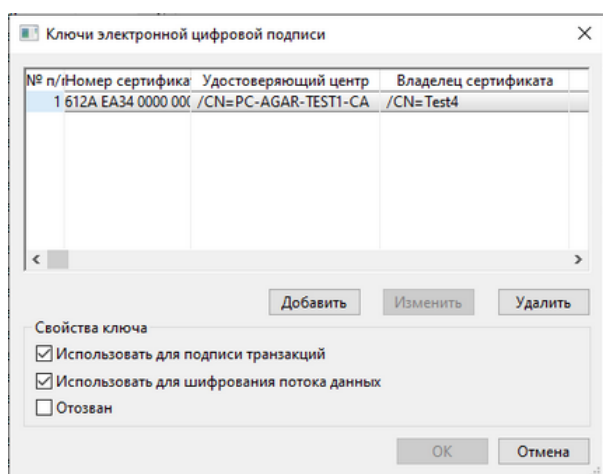
Нажатием кнопки «Сохранить» настройки пользователя сохраняются. Кнопка «Отменить» служит для выхода из окна регистрации сертификатов.

После регистрации ключа выберите пункт меню **Сервер QUIK / Пользователи** и в открывшемся справочнике найдите пользователя, которому вручен ключ.





В окне редактирования выберите из выпадающего списка тип электронной цифровой подписи «CSP SSPI», включите флажок «Подпись обязательна» и настройте выбранный ключ ЭЦП, нажав на кнопку «Изменить...»:



Сохраните настройки нажатием кнопки «Сохранить».

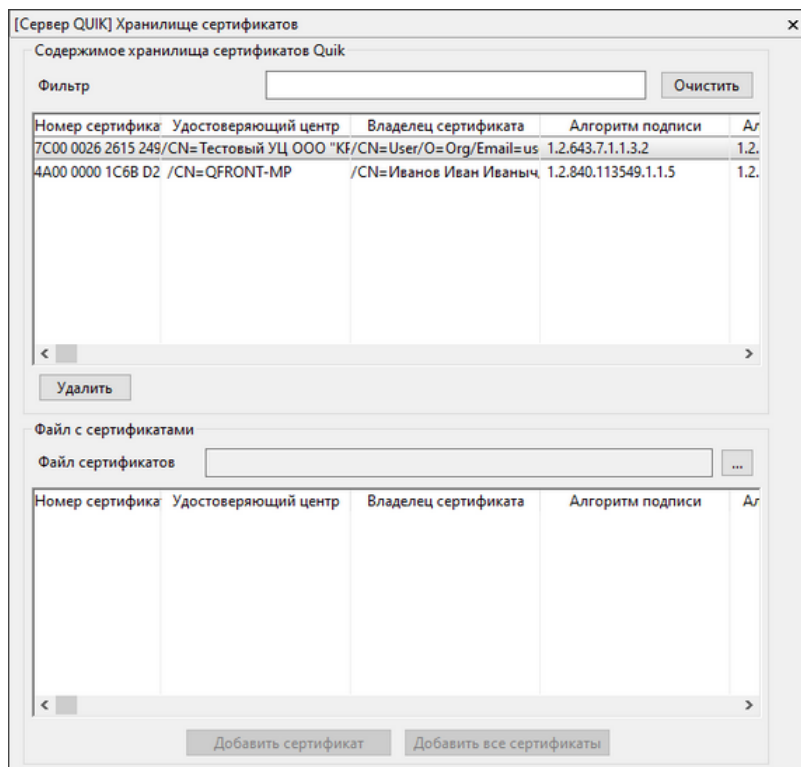
Чтобы настроить сертификаты **CryptoPro** через QUIK Administrator, необходимо прописать путь к .sto файлу, содержащему сертификаты клиентов. Как правило, это файл userstore.sto, который находится в директории с сервером QUIK. Для этого в файле настроек экземпляра сервера QUIK (по умолчанию: «mainbase.ini») добавьте в секцию [QuikCryptoProvider] параметр Storage. Например:

```
[QuikCryptoProvider]
CryptoType=CryptoPro
Storage=..\quik1\server\userstore.sto
```

полный или
относительный путь до файла хранилища



В случае использования сертификата не только для шифрования трафика, но и для подписи транзакций, добавьте сертификат пользователя в **Сервер QUIK / Безопасность / Сертификаты CryptoPro**:

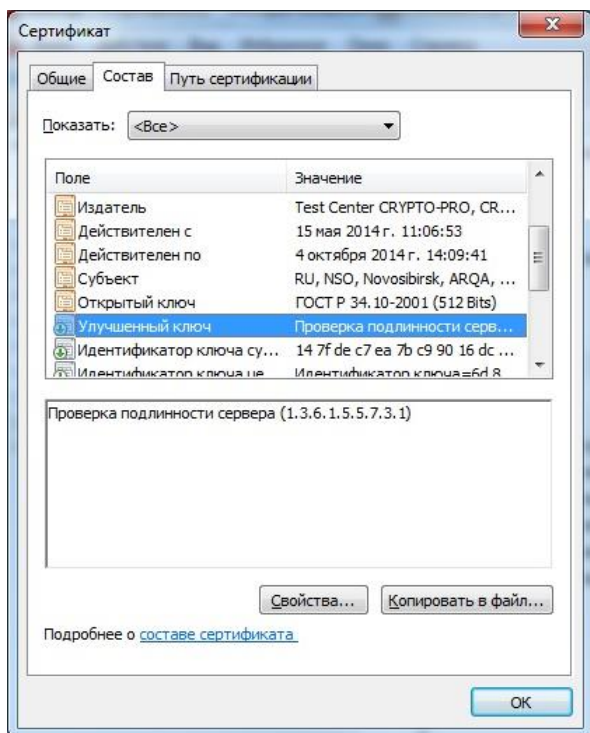


В поле «Файл сертификатов» укажите путь к сертификату клиента и выберите «Добавить сертификат».

5.5.3 Проверка подлинности сервера

Если сертификат формируется через web-интерфейс удостоверяющего центра, то для работы по протоколу SSL (TLS) расширение «Улучшенный ключ» сертификата сервера должно содержать цель «Проверка подлинности сервера». Это необходимо для подтверждения подлинности сервера клиентами:





5.5.4 Формат файла настроек шифрования MP

В файле mp_pr.ini задаются настройки шифрования средствами библиотеки криптографии MP.

Секция [Crypto Provider Settings]

Секция содержит описание настроек криптопровайдера, необходимых для проверки ЭЦП.

Для работы ЭЦП укажите ключевой контейнер одним из следующих способов:

1. Указание параметров контейнера:

- **CSPName** – имя провайдера CSP (Cryptographic Service Provider), используемого сертификатом.
- **CSPContainerName** – имя ключевого контейнера.
- **CSPType** – тип провайдера CSP.

Если не указан параметр CSPName, система предоставляет провайдера CSP, назначенного по умолчанию для указанного типа криптопровайдера.

2. Указание файла сертификата, связанного с ключевым контейнером:

- **CSPCertFileName** – путь к файлу сертификата.

3. Указание хеша сертификата, связанного с ключевым контейнером:

- **CSPCertHash** – хеш установленного сертификата.

Для получения хеша сертификата:

- Откройте файл сертификата;



- _ Перейдите на вкладку «Состав»;
- _ Скопируйте значение поля «Отпечаток», удалите пробелы.

Дополнительные параметры настройки ЭЦП (необязательные):

- **CSPUseInService** – признак работы криптопровайдера в тихом режиме. Возможные значения:

- _ «0» – криптопровайдер работает в интерактивном режиме;
- _ «1» – криптопровайдер работает в тихом режиме.

При работе в тихом режиме криптопровайдер не взаимодействует с пользователем, и при необходимости интерактивного взаимодействия (например, для ввода пароля доступа к контейнеру) возникнет ошибка.

- **CachKeyAndCertificates** – признак кеширования ключей и сертификатов для ускорения последующего доступа к ним. Возможные значения:

- _ «0» – не кешировать;
- _ «1» – кешировать.

- **CSPUseLocalMachineStore** – место расположения секретного ключа. Возможные значения:

- _ «0» (по умолчанию) – ключ находится в хранилище текущего пользователя;
- _ «1» – ключ находится в локальном хранилище компьютера.

- **CheckRevocation** – признак проверки сертификата на отзыв. Возможные значения:

- _ «0» – проверка не проводится;
- _ «1» – проверка проводится.

- **UseLocalCA** – признак использования локального хранилища сертификатов. Возможные значения:

- _ «0» – локальное хранилище не используется.
- _ «1» (по умолчанию) – локальное хранилище используется.

- **CA** – путь к локальному хранилищу сертификатов CA. Значение по умолчанию: «certs\ca».

- **CRL** – путь к локальному хранилищу списка отозванных сертификатов (CRL). Значение по умолчанию: «certs\crl».

Секция [Certificate Stores]

Секция содержит описание хранилища сертификатов, в котором осуществляется поиск сертификатов для настройки режимов шифрования и ЭЦП:

Необходимо указать как минимум одно хранилище сертификатов.



- **MY** – признак использования стандартного личного хранилища сертификатов пользователя. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.
- **CA** – признак использования стандартного хранилища сертификатов центров сертификации. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.
- **ROOT** – признак использования стандартного корневого хранилища. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.
- **SPC** – признак использования стандартного хранилища сертификатов производителей ПО. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.
- **CUSTOM_STORE** – признак использования стороннего внешнего хранилища. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.
- **CUSTOM_DIR** – признак использования директории для хранения сертификатов. Возможные значения:
 - _ «0» – не используется;
 - _ «1» – используется.

Каждое хранилище описывается отдельной секцией вида [[<хранилище>](#)].

Секция [[<хранилище>](#)]

- **HOST** – хост, на котором располагается хранилище. Значение: «.» (точка).
- **LOCATION** – физическое расположение хранилища.
- **TYPE** – тип хранилища. Возможные значения:
 - _ «1» – системное хранилище;
 - _ «2» – внешнее хранилище, расположенное в определенном файле;
 - _ «3» – директория с файлами сертификатов.
- **UPDATABLE** – признак обновляемого хранилища. Возможные значения:
 - _ «0» – запрещено обновлять;
 - _ «1» – разрешено обновлять.
- **PRIORITY** – приоритет. Значение: «1».



Пример:

```
[CUSTOM_STORE]
HOST=.
LOCATION=D:\quik\server\cpstorage\userstore.sto
TYPE=2
UPDATABLE=1
PRIORITY=1
```

Секция [TLS Connection Settings]

Секция содержит настройки TLS-соединения.

- **SSLProtocols** – список используемых версий протоколов (через запятую). Возможные значения:

- _ TLSv1;
- _ TLSv1.1;
- _ TLSv1.2 (по умолчанию).

Для работы в режиме шифрования необходимо указать закрытый ключ. Для этого указывается сертификат, привязанный к закрытому ключу одним из следующих способов:

1. Указание параметров контейнера:

- _ **CSPName** – имя CSP (Cryptographic Service Provider) провайдера, используемого сертификатом.
- _ **CSPContainerName** – имя ключевого контейнера.
- _ **CSPType** – тип CSP-провайдера.

Если не указан параметр CSPName, система предоставляет CSP-провайдера, назначенного по умолчанию для указанного типа криптопровайдера.

2. Указание файла сертификата:

- _ **CSPCertFileName** – путь и имя файла сертификата.

3. Указание хеша сертификата, связанного с ключевым контейнером:

- _ **CSPCertHash** – хеш сертификата.

Параметры настройки аутентификации:

- **UsedHandShakeScheme** – схема, используемая для аутентификации. Возможные значения:

- _ «1»* – аутентификация по сертификату (проверка по сертификату, предоставленному клиентом во время установки SSL/TLS-соединения);
- _ «2»* – аутентификация в домене по логину и паролю;



- «4» (по умолчанию)* – аутентификация по имени пользователя и паролю;
- «8» – восстановление пароля;
- «32»* – аутентификация внутри домена (по доменному имени пользователя).

(*) Совместимость схем аутентификации на сервере и у клиента:

- 1. Если на сервере настроена схема «1», то клиент может использовать схемы «1» и «4».**
- 2. Если на сервере настроена схема «2», то клиент может использовать схемы «2» и «4».**
- 3. Если на сервере настроена схема «4», то клиент может использовать только схему «4».**
- 4. Если на сервере настроена схема «32», то клиент может использовать только схему «32».**

Дополнительные параметры настройки режима шифрования (необязательные):

- **CSPUseInService** – признак работы криптопровайдера в тихом режиме. Возможные значения:

- «0» – криптопровайдер работает в интерактивном режиме;
- «1» – криптопровайдер работает в тихом режиме.

При работе в тихом режиме криптопровайдер не взаимодействует с пользователем, и при необходимости интерактивного взаимодействия (например, для ввода пароля доступа к контейнеру) возникает ошибка.

- **CSPUseLocalMachineStore** – место расположения секретного ключа. Возможные значения:
 - «0» (по умолчанию) – ключ находится в хранилище текущего пользователя;
 - «1» – ключ находится в локальном хранилище компьютера.
- **CheckRevocation** – признак проверки сертификата криптопровайдером по списку отозванных сертификатов. Возможные значения:
 - «0» – проверка не проводится;
 - «1» – проверка проводится.
- **IOBufferMaxSize** – размер буфера (в байтах) данных для шифрования. Значение по умолчанию: «65536».
- **CheckClientCert** – признак проверки сертификата клиента дополнительными средствами ОС Windows.
- **spn_sspi** – SPN сервера для Windows. Значение по умолчанию: «» (пусто).



Секция [TLS Extra Parameters]

Секция содержит настройки для плановой смены сертификатов сервера (необязательные).

Настройки для плановой смены сертификата должны быть заданы до истечения срока действия текущего сертификата. После смены сертификата настройки удаляются.

- **NewServerCertHash** – замена сертификата сервера через хеш. Возможные значения:
 - хеш нового сертификата сервера – после замены сертификата это значение записывается в настройку ServerCertHash файла клиента mp_pr_client.ini, а значение настройки NewServerCertHash удаляется.
 - «DELETE» – отмена процедуры замены сертификата.
 - «» (пусто, по умолчанию) – значение не задано.
- **NewServerCertDomainName** – смена сертификата сервера через доменное имя. Возможные значения:
 - доменное имя нового сертификата – после замены сертификата это значение записывается в настройку ServerCertDomainName файла клиента mp_pr_client.ini, а значение настройки NewServerCertDomainName удаляется.
 - «DELETE» – отмена процедуры замены сертификата.
 - «» (пусто, по умолчанию) – значение не задано.

5.5.5 Пример файла mp_pr.ini

```
[Crypto Provider Settings]
CSPName=Microsoft Enhanced Cryptographic Provider v1.0
CSPCertHash=2c3c48279695e2f058ba2acee9e75403bbc34b97
CSPContainerName=Test_Container
CSPType=1
CSPUseInService=0
CachKeyAndCertificates=1

[Certificate Stores]
MY=1
CA=1
ROOT=1
SPC=1
CUSTOM_STORE=1

[MY]
HOST=.
LOCATION=MY
TYPE=1
```



```

[CA]
HOST=.
LOCATION=CA
TYPE=1
UPDATABLE=1
PRIORITY=1

[ROOT]
HOST=.
LOCATION=ROOT
TYPE=1
UPDATABLE=1
PRIORITY=1

[SPC]
HOST=.
LOCATION=SPC
TYPE=1
UPDATABLE=1
PRIORITY=1

[CUSTOM_STORE]
HOST=.
LOCATION=D:\QUIK\Server\CPCerts\userstore.sto
TYPE=2
UPDATABLE=1
PRIORITY=1

[TLS Connection Settings]
CSPCertFileName=enhanced_cert.cer
UsedHandShakeScheme=1

[TLS Extra Parameters]
NewServerCertHash=2c3c48279695e2f058ba2acee9e75403bbc34b97
NewServerCertDomainName=DELETE

```

5.6 Настройка КриптоПро

Убедитесь, что установлено ПО КриптоПро на компьютерах, где расположены сервер QUIK и серверная часть QUIK Administrator.

Для проверки ЭЦП на компьютерах, где расположены сервер QUIK и серверной части QUIK Administrator, должны быть установлены все необходимые корневые сертификаты УЦ. Файлы с данными сертификатами загружаются из внешних источников и могут быть в формате .p7b, .pfx, .pem, .cer.

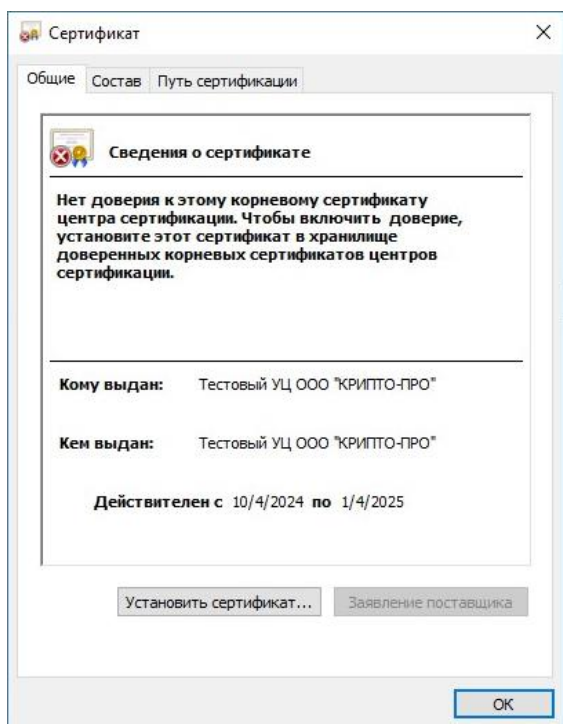


5.6.1 Установка сертификатов УЦ на сервере QUIK при работе на Windows

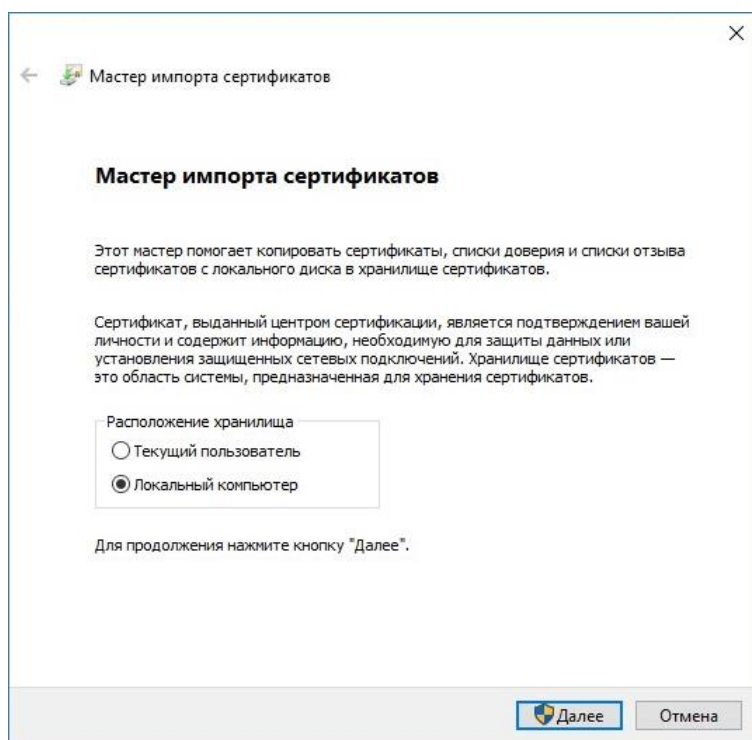
При работе на Windows сертификаты УЦ должны быть установлены в системное хранилище корневых доверенных сертификатов той системной записи, под которой работает сервис ПО сервера QUIK или серверная часть QUIK Administrator. Обычно используется аккаунт определенного пользователя, для которого нужно устанавливать сертификаты, работая через аккаунт данного пользователя. Если ПО работает через системную учетную запись, сертификаты устанавливаются в хранилище локального компьютера.

Установка сертификата УЦ в хранилище «Локальный компьютер»/«Доверенные корневые центры сертификации»

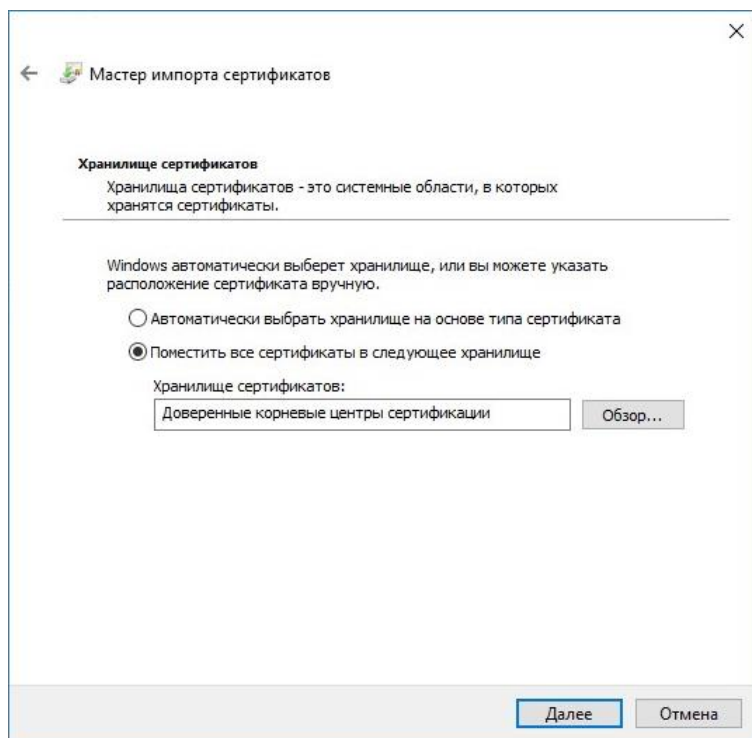
1. Откройте полученный файл с сертификатом УЦ. Нажмите кнопку «Установить сертификат...».



2. В открывшемся окне «Мастер импорта сертификатов» установите флажок «Локальный компьютер» и нажмите «Далее».



3. В открывшемся окне «Хранилище сертификатов» выполните следующие действия:



- _ Установите флажок «Поместить все сертификаты в следующее хранилище»;
- _ Выберите хранилище «Доверенные корневые центры сертификации»;
- _ Нажмите «Далее».



Проверка установки сертификата УЦ в хранилище «Локальный компьютер» / «Доверенные корневые центры сертификации»

1. Нажмите «Пуск».
2. Наберите «certlm.msc».
3. Выберите предложенную программу.
4. Убедитесь, что сертификат УЦ установлен в «Доверенные корневые центры сертификации» в открывшемся окне «certlm – [Сертификаты – Локальный компьютер]».

5.6.2 Установка сертификатов УЦ на сервере QUIK при работе на Linux

Настройка производится при наличии файла, в котором находится корневой сертификат полученный от УЦ.

Установка сертификатов под пользователем arqasrv

При работе на Linux используется пользователь с определенным именем. ПО QUIK устанавливается от пользователя с именем – arqasrv.

1. Скопируйте полученный от УЦ файл с корневым сертификатом, например, в папку /opt/arqasrv/quik/quik/CryptoPro (где расположен сервер QUIK). Например: «certnew.p7b».
2. Выполните команду в каталоге с «certnew.p7b»:

```
sudo chmod 777 ./certnew.p7b
```

3. Проверьте владельца файла сертификатов «certnew.p7b» командой:

```
ls -l ./certnew.p7b
```

Если владелец файла «certnew.p7b» отличается от пользователя arqasrv, выполните команду:

```
sudo chown -R arqasrv: *
```

Если система работает под пользователем, отличным от arqasrv (например, arqa), то для смены пользователя на arqasrv выполните следующие команды:

- Выполните команду для настройки прав пользователя:

```
sudo su -
```



```
[sudo] пароль для arqa: (введите пароль от root для пользователя arqa)
```

- Смените пользователя на arqasrv командой:

```
su - arqasrv
```

4. Установите сертификаты:

- Перейдите в место расположения хранилища «certnew.p7b», где он был сохранен (/opt/arqasrv/quik/quik/CryptoPro);
- Установите корневые сертификаты командой (сертификатов может быть несколько в контейнере формата PKCS7):

```
/opt/cprosp/bin/amd64/certmgr -install -store root -file certnew.p7b
```

Где:

- «/opt/cprosp/bin/amd64/certmgr» – менеджер сертификатов;
- «-install» – команда установки сертификатов;
- «-store root» – хранилище корневых доверенных сертификатов;
- «-file certnew.p7b» – имя файла контейнера, содержащее корневые сертификаты.

Пример:

- В результате выполнения команды, отобразится список сертификатов, которые находятся в указанном контейнере. Под номером 1 сертификат «УЦ», который необходимо поставить в «Доверенные корневые центры сертификации».

```
1-----
Издатель           : ОГРН=1234567890123, ИНН=001234567890, STREET=ул.
Сущевский вал д. 18, C=RU, S=г. Москва, L=Москва, O="ООО ""КРИПТО-ПРО""",
CN="Тестовый УЦ ООО ""КРИПТО-ПРО""
Субъект            : ОГРН=1234567890123, ИНН=001234567890, STREET=ул.
Сущевский вал д. 18, C=RU, S=г. Москва, L=Москва, O="ООО ""КРИПТО-ПРО""",
CN="Тестовый УЦ ООО ""КРИПТО-ПРО""
Серийный номер      : 0x3AF80A1332834D994C4E6F0AD07C8FAD
SHA1 отпечаток      : 41dcbff2ae102339bcdd0d5100ffb8e6018353d
Идентификатор ключа : e4c08096e4b47834123c22b975cd96204330b023
Алгоритм подписи    : ГОСТ Р 34.11-2012/34.10-2012 256 бит
Алгоритм откp. кл.  : ГОСТ Р 34.10-2012 256 бит (512 бит)
Выдан               : 04/10/2024 12:22:02 UTC
Истекает            : 04/01/2025 12:32:02 UTC
```



Ссылка на ключ : Нет

- Нажмите «1» и «Enter».
- Для контейнеров сертификатов УЦ с паролем, например, в формате <PKCS12>, используется следующая команда установки:

```
«/opt/cprocsp/bin/amd64/certmgr -store root -file ./test_user_криптопро.pfx -pfx  
-pin 12345»
```

Где:

- «-pin» – пароль от контейнера .pfx.

Проверка установки сертификата УЦ для пользователя arqasrv

Все сертификаты КриптоПро хранятся по указанному пути:

```
/var/opt/cprocsp/users
```

Сертификаты arqasrv хранятся по указанному пути:

```
/var/opt/cprocsp/users/arqasrv/stores
```

Проверить владельца сертификатов можно командой:

```
ls -l
```

Проверить установленные корневые сертификаты можно командой:

- Для Windows:

```
Certutil -store root
```

- Для Linux:

```
/opt/cprocsp/bin/amd64/certmgr -list -store root
```



5.6.3 Файл настроек qcrypto.cfg на сервере QUIK

- Добавьте в файл qcrypto.cfg на Windows следующие настройки:

```
[CryptoProviders]
cryptopro=1

[cryptopro]
Module=.\cpcsp_pr.dll
IniFile=.\cpcsp_pr.ini
```

- Добавьте в файл qcrypto.cfg на Linux следующие настройки:

```
[CryptoProviders]
cryptopro=1

[cryptopro]
Module=./libcpcsp_pr.so
IniFile=./cpcsp_pr.ini
```

5.6.4 Файл настроек qadminsrv.ini серверной части QUIK Administrator

- Добавьте в файл qadminsrv.ini серверной части QUIK Administrator на Windows следующие настройки:

```
CryptoProviders]
cryptopro=1

[cryptopro]
Module=.\cpcsp_pr.dll
IniFile=.\cpcsp_pr.ini
```

- Добавьте в файл qadminsrv.ini серверной части QUIK Administrator на Linux следующие настройки:

```
[CryptoProviders]
cryptopro=1

[cryptopro]
Module=./libcpcsp_pr.so
IniFile=./cpcsp_pr.ini
```



5.6.5 Файл настроек cpcsp_pr.ini сервера QUIK

Укажите в секции [Certificate Stores] следующие значения:

```
[Certificate Stores]
CA=1
ROOT=1
CUSTOM_STORE=1
```

Где:

- «CA» – промежуточные сертификаты УЦ. Путь к данному хранилищу указывается в секции [CA] файла «cpcsp_pr.ini»:

```
[CA]
HOST=.
LOCATION=CA
TYPE=1
UPDATABLE = 1
PRIORITY = 1
```

- «ROOT» – корневые сертификаты УЦ. Путь к данному хранилищу указывается в секции [ROOT] файла «cpcsp_pr.ini»:

```
[ROOT]
HOST=.
LOCATION=ROOT
TYPE=1
UPDATABLE = 1
PRIORITY = 1
```

- «CUSTOM_STORE» – локальное хранилище сертификатов пользователей в виде файла. Путь к данному хранилищу указывается в секции [CUSTOM_STORE] файла «cpcsp_pr.ini»:

```
[CUSTOM_STORE]
HOST=.
LOCATION=./userstore.sto
TYPE=2
UPDATABLE = 1
PRIORITY = 1
```



Файл «userstore.sto» должен быть создан заранее, в него с помощью QUIK Administrator добавляются сертификаты пользователей, которые отправляют подписанные транзакции на сервер QUIK. Владелец должен быть пользователь arqasrv.

5.6.6 Файл настроек cpcsp_pr.ini серверной части QUIK Administrator

Укажите в секции [Certificate Stores] следующие значения:

```
[Certificate Stores]
CA=1
ROOT=1
CUSTOM_STORE=1
```

Где:

- «CA» – промежуточные сертификаты УЦ. Путь к данному хранилищу указывается в секции [CA] файла «cpcsp_pr.ini»:

```
[CA]
HOST=.
LOCATION=CA
TYPE=1
UPDATABLE = 1
PRIORITY = 1
```

- «ROOT» – корневые сертификаты УЦ. Путь к данному хранилищу указывается в секции [ROOT] файла «cpcsp_pr.ini»:

```
[ROOT]
HOST=.
LOCATION=ROOT
TYPE=1
UPDATABLE = 1
PRIORITY = 1
```

- «CUSTOM_STORE» – локальное хранилище сертификатов пользователей в виде файла. Путь к данному хранилищу указывается в секции [CUSTOM_STORE] файла «cpcsp_pr.ini»:

```
[CUSTOM_STORE]
HOST=.
LOCATION=/opt/arqasrv/quik/quik/userstore.sto
TYPE=2
```



```
UPDATABLE = 1  
PRIORITY = 1
```

Хранилище сертификатов «userstore.sto» для сервера QUIK и серверной части QUIK Administrator – общее.

5.6.7 Проверка инициализации провайдера КриптоПро

1. Запустите сервер QUIK.
2. Откройте «events.log».

**При успешной установке отобразится следующая диагностика:
«Sign provider “CryptoPro” initialized successfully».**

5.6.8 Миграция серверной части с ОС Windows на ОС Linux

1. Установите ПО КриптоПро на сервере Linux и настройте сервер QUIK на ЭЦП КриптоПро по инструкции установки ЭЦП.
2. Перенесите sto-файл с хранилищем сертификатов пользователей сервера QUIK под Windows в сервер QUIK под Linux. Для этого скопируйте данный файл в требуемое место хранения в Linux и укажите данный путь в ini-файле настроек криптопровайдера (секция [CUSTOM_STORE], параметр LOCATION).

Владельцем sto-файла должен быть пользователь arqasrv.

3. Настройте сервер QUIK под Linux на работу с БД, которая используется на сервере QUIK под Windows.

Если используется база данных под управлением СУБД Microsoft SQL Server, то предварительно необходимо выполнить миграцию данных из Microsoft SQL Server в PostgreSQL.

Если сервер, установленный на Windows, настроен на ЭЦП через криптопровайдер МР (в файле crypto.cfg находится ссылка на файл mp_pr.dll вместо cspcsp_pr.dll), то дополнительно необходимо модифицировать данные в БД, меняя в таблицах dbo.users.crypto_type и dbo.crypto_pro_key строку «cspsspi» на «cryptopro». Для этого необходимо выполнить следующие запросы к БД:

```
update dbo.USERS set CRYPTO_TYPE='cryptopro' where CRYPTO_TYPE='cspsspi'
```



```
update dbo.CRYPTO_PRO_KEY set CRYPTO_TYPE='cryptopro' where CRYPTO_TYPE='cspsspi'
```

5.7 Настройка Сигнал-КОМ

Убедитесь, что установлено ПО Сигнал-КОМ на компьютерах, где расположены сервер QUIK и серверная часть QUIK Administrator.

Для проверки ЭЦП на компьютерах, где расположены сервер QUIK и серверной части QUIK Administrator, должны быть установлены все необходимые корневые сертификаты УЦ. Файлы с данными сертификатами загружаются из внешних источников и могут быть в формате .p7b, .pfx, .pem, .cer.

Криптопровайдер **SSLAndMessagePro** предоставляет возможность работы с двумя криптографическими библиотеками: Message-Pro и SSL-Pro.

5.7.1 Настройка шифрования для Основного сервера QUIK для Windows

1. Проверьте наличие и при необходимости скопируйте в рабочий каталог Основного сервера QUIK файлы, необходимые для работы программы:
 - «sslpro.dll» – библиотека SSL-Pro, предоставляется компанией «Сигнал-КОМ»;
 - «signalcom_pr.dll» – модуль объединенного провайдера библиотек SSL-Pro и Message-Pro;
 - «signalcom_pr.ini» – файл с общими настройками провайдера, параметрами соединения пользователя и настройками ЭЦП.
2. Для шифрования серверу понадобится набор ключевых файлов и сертификатов. Нужно до запуска поместить файлы ключей и сертификаты в соответствующий подкаталог каталога ключевого носителя программы. Описание рекомендуемого формата ключевого носителя см. в п. [«Описание рекомендуемого формата ключевого носителя для библиотек SSL-Pro и Message-Pro»](#).

Функционирование системы с использованием шифрования с помощью библиотеки SSL-Pro требует наличия у каждой из сторон (сервера и Рабочих мест QUIK) секретного ключа, соответствующего ему сертификата, а также необходимого набора сертификатов удостоверяющих центров. В текущих версиях ключ сервера не должен быть защищен паролем, иначе при попытке запросить пароль сервер зависнет. Для генерации ключей и сертификатов используется ПО, не входящее в состав стандартного комплекта поставки системы QUIK. Вопрос его приобретения решается с компанией «Сигнал-КОМ».

3. В соответствии с описанием структуры файла [signalcom_pr.ini](#) укажите необходимые настройки шифрования в файле signalcom_pr.ini ОС QUIK. В данном случае в файле signalcom_pr.ini будут указаны и общие настройки криптопровайдера, и настройки, которые будут использоваться именно для шифрования.



4. Укажите в файле qcrypto.cfg следующие настройки провайдера:

- В секцию [CryptoProviders] добавьте настройку SignalComMessageAndSSLPro=1:

```
[CryptoProviders]
...
SignalComMessageAndSSLPro=1
```

- Добавьте в файл секцию [SignalComMessageAndSSLPro] следующего вида:

```
[SignalComMessageAndSSLPro]
Module=.\signalcom_pr.dll ;полный или относительный путь до исполняемого файла
IniFile= .\signalcom_pr.ini ;полный или относительный путь до файла с
настройками
```

5. Укажите путь для настроенного ранее файла signalcom_pr.ini с настройками шифрования посредством библиотеки SSL-Pro, которые сервер будет использовать при подключении пользователей. Для этого в секции [usend_module] файла настроек сервера quik.ini создайте настройку crypto_provider_ini_file=.\signalcom_pr.ini:

```
[usend_module]
...
crypto_provider_ini_file=.\signalcom_pr.ini
```

Если Основной сервер QUIK использует только один криптопровайдер шифрования, то для задания его настроек можно использовать настройку crypto_provider_ini_file в секции [usend_module].

Если провайдеров несколько, тогда для задания настроек нужно использовать настройку «crypto_provider_ini_file_sslpro» – ключ для задания криптопровайдера SSL-Pro.

6. Запустите Основной сервер QUIK и убедитесь в наличии следующих строк в файле events.log:

```
Crypto provider 'SignalComMessageAndSSLPro' initied
```

5.7.2 Настройка ЭЦП для Основного сервера QUIK для Windows

1. Проверьте наличие и при необходимости скопируйте в рабочий каталог Основного сервера QUIK файлы, необходимые для работы программы:

- mespro.dll – библиотека Message-Pro, предоставляется компанией «Сигнал-КОМ»;
- signalcom_pr.dll – модуль объединенного провайдера библиотек SSL-Pro и Message-Pro;



— signalcom_pr.ini – файл с общими настройками провайдера и настройками ЭЦП.

2. Поместите файлы с сертификатами пользователей, которые будут присылать транзакции с ЭЦП в соответствующий подкаталог каталога ключевого носителя программы. Описание рекомендуемого формата ключевого носителя см. в п. [«Описание рекомендуемого формата ключевого носителя для библиотек SSL-Pro и Message-Pro»](#).

Функционирование системы с использованием ЭЦП с помощью библиотеки Message-Pro требует наличия у Рабочих мест QUIK секретного ключа, соответствующего ему сертификата, а также необходимого набора сертификатов удостоверяющих центров. Со стороны сервера требуется наличие справочника клиентских сертификатов и необходимого набора сертификатов удостоверяющих центров. Для генерации ключей и сертификатов используется ПО, не входящее в состав стандартного комплекта поставки системы QUIK. Вопрос его приобретения решается с компанией «Сигнал-КОМ». Поддержка серверного справочника сертификатов в актуальном состоянии (удаление отозванных и просроченных сертификатов) также осуществляется сторонним ПО.

3. В соответствии с описанием структуры файла [signalcom_pr.ini](#) укажите необходимые настройки ЭЦП в файле signalcom_pr.ini ОС QUIK. В данном случае в файле signalcom_pr.ini будут указаны и общие настройки криптопровайдера, и настройки, которые будут использоваться именно для проверки ЭЦП.
4. Укажите в файле crypto.cfg следующие настройки провайдера:

— В секцию [CryptoProviders] добавьте настройку SignalComMessageAndSSLPro=1:

```
[CryptoProviders]
...
SignalComMessageAndSSLPro=1
```

— Добавьте в файл секцию [SignalComMessageAndSSLPro] следующего вида:

```
[SignalComMessageAndSSLPro]
Module=.\signalcom_pr.dll ;полный или относительный путь до исполняемого файла
IniFile= .\signalcom_pr.ini ;полный или относительный путь до файла с
настройками
```

— В случае отсутствия укажите в секции [auth] следующие настройки:

```
[auth]
...
sign=secprov.dll
```

5. Запустите Основной сервер QUIK и убедитесь в наличии следующих строк в файле events.log:



```
Sign provider 'SignalComMessageAndSSLPro' initialized successfully
```

5.7.3 Настройка шифрования для Основного сервера QUIK для Astra Linux

1. Проверьте наличие и при необходимости скопируйте в рабочий каталог Основного сервера QUIK файлы необходимые для работы программы:
 - libsslprox.so.0 – библиотека SSL-Pro, предоставляется компанией «Сигнал-КОМ»;
 - libsignalcom_pr.so – модуль объединенного провайдера библиотек SSL-Pro и Message-Pro;
 - signalcom_pr.ini – файл с общими настройками провайдера.
2. Для шифрования серверу понадобится набор ключевых файлов и сертификатов, нужно до запуска поместить файлы ключей и сертификаты в соответствующий подкаталог каталога ключевого носителя программы. Описание рекомендуемого формата ключевого носителя см. в п. [«Описание рекомендуемого формата ключевого носителя для библиотек SSL-Pro и Message-Pro»](#).

Функционирование системы с использованием шифрования с помощью библиотеки SSL-Pro требует наличия у каждой из сторон (сервера и клиентских рабочих мест QUIK) секретного ключа, соответствующего ему сертификата, а также необходимого набора сертификатов удостоверяющих центров. В текущих версиях ключ сервера не должен быть защищен паролем, иначе при попытке запросить пароль сервер зависнет. Для генерации ключей и сертификатов используется ПО, не входящее в состав стандартного комплекта поставки системы QUIK. Вопрос его приобретения решается с компанией «Сигнал-КОМ».

3. В соответствии с описанием структуры файла [signalcom_pr.ini](#) пропишите необходимые настройки шифрования в файле signalcom_pr.ini ОС QUIK. В данном случае в файле signalcom_pr.ini будут указаны и общие настройки криптопровайдера, и настройки, которые будут использоваться именно для шифрования.
4. Укажите в файле crypto.cfg следующие настройки провайдера:
 - В секцию [CryptoProviders] добавьте настройку SignalComMessageAndSSLPro=1:

```
[CryptoProviders]
...
SignalComMessageAndSSLPro=1
```

- Добавьте в файл секцию [SignalComMessageAndSSLPro] следующего вида:

```
[SignalComMessageAndSSLPro]
Module=../libsignalcom_pr.so ;полный или относительный путь до
исполняемого файла
```



```
IniFile= ./signalcom_pr.ini      ;полный или относительный путь до файла с
настройками
```

5. Укажите путь для уже настроенного ранее файла signalcom_pr.ini с настройками шифрования посредством библиотеки SSL-Pro, которые сервер будет использовать при подключении пользователей. Для этого в секции [usend_module] файла настроек сервера quik.ini создайте настройку crypto_provider_ini_file=./signalcom_pr.ini:

```
[usend_module]
...
crypto_provider_ini_file=./signalcom_pr.ini
```

Если Основной сервер QUIK использует только один криптопровайдер шифрования, то для задания его настроек можно использовать настройку crypto_provider_ini_file в секции [usend_module].

Если провайдеров несколько, тогда для задания настроек нужно использовать настройку «crypto_provider_ini_file_sslpro» – ключ для задания криптопровайдера SSL-Pro.

6. Запустите Основной сервер QUIK и убедитесь в наличии следующих строк в файле events.log:

```
Crypto provider 'SignalComMessageAndSSLPro' initied
```

5.7.4 Настройка ЭЦП для Основного сервера QUIK для Astra Linux

1. Проверьте наличие и при необходимости скопируйте в рабочий каталог Основного сервера QUIK файлы, необходимые для работы программы:
 - libmesprox.so.0 – библиотека Message-Pro, предоставляется компанией «Сигнал-КОМ»;
 - libsignalcom_pr.so – модуль объединенного провайдера библиотек SSL-Pro и Message-Pro;
 - signalcom_pr.ini – файл с общими настройками провайдера и настройками ЭЦП.
2. Поместите файлы с сертификатами пользователей, которые будут присылать транзакции с ЭЦП, в соответствующий подкаталог каталога ключевого носителя программы. Описание рекомендуемого формата ключевого носителя см. в п. [«Описание рекомендуемого формата ключевого носителя для библиотек SSL-Pro и Message-Pro»](#).

Функционирование системы с использованием ЭЦП с помощью библиотеки Message-Pro требует наличия у клиентских Рабочих мест QUIK секретного ключа, соответствующего ему сертификата, а также необходимого набора сертификатов удостоверяющих центров. Со стороны сервера требуется



наличие справочника клиентских сертификатов и необходимого набора сертификатов удостоверяющих центров. Для генерации ключей и сертификатов используется ПО, не входящее в состав стандартного комплекта поставки системы QUIK. Вопрос его приобретения решается с компанией «Сигнал-КОМ». Поддержка серверного справочника сертификатов в актуальном состоянии (удаление отозванных и просроченных сертификатов) также осуществляется сторонним ПО.

3. В соответствии с описанием структуры файла [signalcom_pr.ini](#) пропишите необходимые настройки ЭЦП в файле signalcom_pr.ini ОС QUIK. В данном случае в файле signalcom_pr.ini будут указаны и общие настройки криптопровайдера, и настройки, которые будут использоваться именно для проверки ЭЦП.

4. Укажите в файле crypto.cfg следующие настройки провайдера:

- В секцию [CryptoProviders] добавьте настройку SignalComMessageAndSSLPro=1:

```
[CryptoProviders]
...
SignalComMessageAndSSLPro=1
```

- Добавьте в файл секцию [SignalComMessageAndSSLPro] следующего вида:

```
[SignalComMessageAndSSLPro]
Module=libsignalcom_pr.so ;полный или относительный путь до исполняемого файла
IniFile= ./signalcom_pr.ini ;полный или относительный путь до файла с
настройками
```

- В случае отсутствия укажите в секции [auth] следующие настройки:

```
[auth]
...
sign=libsecprov.so
```

5. Запустите Основной сервер QUIK и убедитесь в наличии следующих строк в файле events.log:

```
Sign provider 'SignalComMessageAndSSLPro' initialized successfully
```

5.7.5 Настройка шифрования для Сервера доступа QUIK

Настройка шифрования для канала связи с клиентами осуществляется аналогично настройке Основного сервера QUIK (см. пункт настройки для [Windows](#) или [Astra Linux](#)) по шагам 1-5.



Для канала связи Сервера доступа с вышестоящими в иерархии серверами или Основного сервера QUIK в типовой конфигурации используется библиотека Qcrypto32, поэтому настраивать шифрование с помощью библиотеки SSL-PRO для защиты канала связи между Сервером доступа и вышестоящими в иерархии серверами или Основного сервера QUIK не требуется.

1. Библиотека SSL-Pro при работе требует больших, чем Qcrypto32, вычислительных ресурсов, поэтому достаточность уровня производительности системы обязательно нужно проверить до запуска комплекса в боевую эксплуатацию.
2. В процессе работы библиотеки SSL-Pro на Сервера доступа возможно использование ключа и сертификата, используемых на вышестоящие в иерархии серверами, – это снижает безопасность, но упрощает процедуру администрирования ключей.

5.7.6 Настройка ЭЦП для Сервера доступа QUIK

В типовой конфигурации настройки ЭЦП для Сервера доступа не требуется, так как генерация ЭЦП выполняется Рабочим местом QUIK клиентов при отправке транзакций, а проверка ЭЦП осуществляется Основным сервером QUIK.

Настройка ЭЦП для Сервера доступа требуется только в случае, когда клиенты, подключающиеся через Сервер доступа, не используют ЭЦП (то есть транзакции поступают на Сервер доступа без ЭЦП), и при этом есть требование, что все пользовательские транзакции, поступающие на Основной сервер, должны быть с ЭЦП и должны проверяться Основным сервером QUIK. В этом случае Сервер доступа настраивается так, чтобы все входящие транзакции пользователей подписывались ключом Сервера доступа. При этом:

1. Если Сервер доступа с настроенной генерацией ЭЦП получает транзакцию клиента, уже подписанную ЭЦП, сделанной тем же самым ПО, которое настроено для ЭЦП на Сервере доступа, то данная транзакция пересылается на Основной сервер QUIK без ЭЦП Сервера доступа.
2. Если криптопровайдер, на котором сделана ЭЦП транзакции клиента, и криптопровайдер, настроенный для создания ЭЦП на Сервере доступа, разные, то транзакция подписывается с помощью ЭЦП Сервера доступа и отправляется на Основной сервер QUIK.

Настройка ЭЦП на Сервере доступа осуществляется аналогично настройке Основного сервера QUIK (см. пункт настройки для [Windows](#) или [Astra Linux](#)) по шагам 1-5.

Дополнительно произведите следующие настройки:

1. В файл настроек [signalcom_pr.ini](#) добавьте секцию [Signal_Com_Message_Pro_Sign_Settings] и укажите в ней следующие настройки:



- «sign_cert_file_name» – путь и наименование файла с сертификатом пользователя, с помощью которого осуществляется ЭЦП;
- «pse_path» – путь к каталогу корневого ключевого носителя.

Пример:

```
[Signal_Com_Message_Pro_Sign_Settings]
sign_cert_file_name=./certs/pse/cert/cert.cer
pse_path=./certs/pse
```

2. В файле настроек Сервера доступа quik.ini добавьте в секцию [dwell_module] настройку sign_provider:

- «sign_provider» – тип криптопровайдера, используемого при генерации ЭЦП. Значение по умолчанию: «SignalComMessageAndSSLPro» (генерация ЭЦП с помощью библиотеки Message-Pro).

Пример:

```
[dwell_module]
...
sign_provider=SignalComMessageAndSSLPro
```

3. Запустите Сервер доступа и убедитесь в наличии следующей строки в файле events.log:

```
Sign provider 'SignalComMessageAndSSLPro' initialized successfully
```

5.7.7 Формат файла signalcom_pr.ini

Описание настроек шифрования

- Секция [SIGNAL_COM_SSL_PRO_COMMON_SETTINGS] содержит описание глобальных настроек криптопровайдера.
- Секция [SIGNAL_COM_SSL_PRO_CIPHER_SETTINGS] содержит описание настроек криптопровайдера, необходимых для корректного создания контекста шифрования:
 - «PSE_PATH» – путь к корневому каталогу ключевого носителя СКЗИ. Обязательный параметр.
 - «TRUSTED_CA_CERTS_DIR» – путь к каталогу сертификатов корневых удостоверяющих центров. Обязательный параметр, если путь к файлу с сертификатом корневого удостоверяющего центра не указан в ключе «TRUSTED_CA_CERT_FILE_NAME».
 - «TRUSTED_CA_CERT_FILE_NAME» – путь к файлу с сертификатом корневого удостоверяющего центра. Обязательный параметр, если путь к каталогу сертификатов корневого удостоверяющего центра не указан в ключе «TRUSTED_CA_CERTS_DIR».
 - «UNTRUSTED_CA_CERTS_DIR» – путь к каталогу сертификатов промежуточных удостоверяющих центров. Опциональный параметр.



- «UNTRUSTED_CA_CERT_FILE_NAME» – путь к файлу с сертификатом промежуточного удостоверяющего центра. Опциональный параметр.
- «CRL_FILES_DIR» – путь к каталогу со списком отозванных сертификатов. Опциональный параметр.
- «CRL_FILE_NAME» – путь к файлу со списком отозванных сертификатов. Опциональный параметр.
- «CIPHER_CERT_FILE_NAME» – имя файла с сертификатом, соответствующим секретному ключу, на котором шифруются данные в процессе сеанса связи. Обязательный параметр.
- «CIPHER_KEY_FILE_NAME» – имя файла с секретным ключом, на котором шифруются данные в процессе сеанса связи. Опциональный параметр.
- Секция [SignalComCommonSettings]:
 - «DefaultNewKeyAlgorithm» – алгоритм шифрования данных асимметричным ключом. Значение по умолчанию: «ECR3410».

Для генерации ключей в соответствии с ГОСТ 2012 в качестве значения настройки DefaultNewKeyAlgorithm укажите «GOST3410-2012-512-A-ParamSet».

Описание настроек проверки ЭЦП

Секция [signal_com_message_pro_common_settings] содержит описание настроек криптопровайдера, необходимых для проверки ЭЦП:

- «certificates_path» – путь к каталогу используемых сертификатов. Обязательный параметр.
- «CRLs_path» – путь к каталогу используемых списков отозванных сертификатов. Обязательный параметр.
- «CAs_path» – путь к каталогу сертификатов удостоверяющих центров. Обязательный параметр.
- «input_data_format» – формат входных данных. В типовой конфигурации пользователем не настраивается (использует значение по умолчанию). Возможные значения:
 - «FORMAT_ASN1»;
 - «FORMAT_PEM» (по умолчанию).
- «output_data_format» – формат выходных данных. В типовой конфигурации пользователем не настраивается (использует значение по умолчанию). Возможные значения:
 - «FORMAT_ASN1»;
 - «FORMAT_PEM» (по умолчанию).
- «cert_storage_validation» – проверка загружаемых сертификатов на актуальность. При включенной настройке сертификаты с истекшим сроком действия не загружаются. Возможные значения:
 - «0» – отключено;



— «1» (по умолчанию) – включено.

- «cert_operation_approach» – добавления сертификатов в промежуточное хранилище для дальнейшей сверки на наличие сертификатов в библиотеке mespro.dll. Позволяет значительно сократить время поиска нужного сертификата и проверки ЭЦП. Возможные значения:

— «0» – отключено;

— «1» (по умолчанию) – включено.

Описание рекомендуемого формата ключевого носителя для библиотек SSL-Pro и Message-Pro

- «SignalCom» – корневой каталог, в котором находятся все необходимые файлы (ключи, сертификаты, списки отозванных сертификатов и другое).
- «PSE» – подкаталог каталога «SignalCom», в котором находятся ключи.
- «CERTS» – подкаталог каталога «SignalCom», в котором находятся файлы сертификатов пользователей. Имя и местоположения данного каталога можно изменять, внося также соответствующие изменения в файл настроек провайдера «signalcom_pr.ini».
- «KEYS» – подкаталог каталога «PSE», в котором находятся файлы ключей шифрования пользователя. Имя и местоположения данного каталога относительно корневого каталога «PSE» изменять нельзя.
- «TrustedCA» – подкаталог каталога «SignalCom», в котором находятся файлы сертификатов корневых удостоверяющих центров. Имя и местоположения данного каталога можно изменять, внося также соответствующие изменения в файл настроек провайдера.
- «CA» – подкаталог каталога «SignalCom», в котором находятся файлы сертификатов корневых удостоверяющих центров. Местоположения данного каталога, как правило, совпадает с местоположением каталога «TrustedCA».
- «CRLs» – подкаталог каталога «SignalCom», в котором находятся файлы со списками отозванных сертификатов. Имя и местоположения данного каталога можно изменять, внося также соответствующие изменения в файл настроек провайдера.

При использовании рекомендованного формата ключевого носителя файл настроек криптопровайдера signalcom_pr.ini имеет следующий вид:

```
[SIGNAL_COM_SSL_PRO_COMMON_SETTINGS]

[SIGNAL_COM_SSL_PRO_CIPHER_SETTINGS]
PSE_PATH=./signalcom/pse
TRUSTED_CA_CERTS_DIR=./signalcom/trustedca
CRL_FILES_DIR=./signalcom/crls
CIPHER_CERT_FILE_NAME=./signalcom/certs/cert.cer

[SIGNAL_COM_MESSAGE_PRO_COMMON_SETTINGS]
CERTIFICATES_PATH=./signalcom/certs
CRLS_PATH=./signalcom/crl
CAS_PATH=./signalcom/ca
```



```
INPUT_DATA_FORMAT=FORMAT_ASN1
OUTPUT_DATA_FORMAT=FORMAT_ASN1
```

```
[SIGNAL_COM_MESSAGE_PRO_SIGN_SETTINGS] ;секция присутствует при настройке ЭЦП через
Сервер доступа
```

```
SIGN_CERT_FILE_NAME=./signalcom/certs/cert.cer
```

```
PSE_PATH=./signalcom/pse
```

Файлы .orq и .db3 должны соответствовать тому контейнеру, с которым были сгенерированы.

5.8 Хранимая процедура для стоп-заявок

Для снятия стоп-заявки выполните хранимую процедуру **withdrawstoporder** со следующими параметром:

Параметр	Тип данных в MS SQL / PostgreSQL		Описание
@StopOrderID	BIGINT	BIGINT	Номер стоп-заявки, статус которой будет изменен на «Снята» в результате выполнения хранимой процедуры

5.9 Перенос стоп-заявок

Особенности переноса стоп-заявок между серверами, объединенными в контур, в том числе между основным и резервным сервером. Описание приведено как для аварийного, так и для планового переноса.

5.9.1 Сценарий переноса стоп-заявок, когда один из серверов вышел из строя

- Через программный интерфейс QMonitor на работающем сервере выполнить команду «Process all stop orders». На запрос идентификатора (с которого необходимо перенести стоп-заявки) выбрать метку сервера, который аварийно завершил работу.
- Сервер, который аварийно завершил свою работу, необходимо запустить с ключом -removestops (допустима комбинация с ключами -clean, -new и -loadlimits). Именно при первом запуске после сбоя сервера последующие штатные запуски выполняются без ключа -removestops.

5.9.2 Сценарии планового переноса

Любой плановый перенос рекомендуется делать исключительно в неторговое время.



Выполнение переноса в один шаг

1. Обеспечить выполнение следующих условий:

- Оба сервера запущены;
- К данным серверам подключен Репликатор;
- К данным серверам подключены все торговые интерфейсы.

2. Подключиться Программным интерфейсом QMonitor к серверу, на который необходимо перенести стоп-заявки и выполнить команду «Process all stop orders» (на запрос идентификатора указать метку сервера, с которого нужно перенести стоп-заявки).

При выполнении переноса в один шаг выполнение условий обязательно, иначе будут коллизии с метками принадлежности.

Выполнение переноса в два шага

1. Подключиться Программным интерфейсом QMonitor к серверу, с которого необходимо перенести стоп-заявки, и выполнить команду «Remove all stop orders» (альтернативный вариант запуска с ключом -removestops).

2. Подключиться Программным интерфейсом QMonitor к серверу, на который необходимо перенести стоп-заявки, и выполнить команду «Process all stop orders» (на запрос идентификатора указать метку сервера, с которого нужно перенести стоп-заявки).

Требования:

- Если сервер, на который переносятся стоп-заявки, был запущен с ключом -clean или -new, то возможна ситуация, когда Программный интерфейс QMonitor не будет отображать стоп-заявки. В этом случае нужно дождаться обработки стоп-заявок сервером QUIK из базы данных. Обычный порядок времени ожидания от 30 секунд до нескольких минут. Критерий успешного окончания обработки стоп-заявок из базы данных – появление списка в таблице Stop Orders (в Программном интерфейсе QMonitor). По этой причине не рекомендуется запуск сервера, на который переносятся стоп-заявки с ключами -clean или -new.
- Подключение Репликатора и торговых интерфейсов в сценарии «Выполнение переноса в два шага» необязательно.
- Плановый перенос необходимо делать в неторговое время. Если есть необходимость сделать плановый перенос в торговое время, то через Программный интерфейс QMonitor действия, описанные в «[Выполнение переноса в два шага](#)», нужно делать последовательно и быстро (чтобы не было двойного срабатывания и задержек срабатывания).

При возникновении иных вопросов отправьте файл events.log и полное описание событий в Службу технической поддержки QUIK:
quiksupport@argatech.com.



5.10 Регламент ежедневного обслуживания сервера QUIK

5.10.1 Остановка и запуск сервисов

При возникновении вопросов обратитесь в Службу технической поддержки QUIK: quiksupport@arqatech.com.

Сервер QUIK и интерфейсы к торговым системам нужно перезагружать ежедневно, так как перезапуск торговых площадок выполняется ежедневно.

Отсутствие настроенного расписания перезапуска сервисов может привести к некорректному определению даты текущей торговой сессии и проблемам с подключением торговых интерфейсов. Остановку сервисов рекомендуется выполнять после завершения торгов на соответствующих площадках, а запуск – утром, перед началом торгов.

Расписание запуска сервисов должно быть согласовано со значением параметра [ClearingTime](#) в секции [trade_date] файла настроек quik.ini, которое должно соответствовать времени, когда сервис гарантированно остановлен. Например, если сервер QUIK останавливается в 02:30, а запускается в 05:30, значение может быть следующим:

```
[trade_date]
ClearingTime=040000
```

Параметр ClearingTime может также присутствовать в настройках других сервисов и модулей системы QUIK. Информацию о настройке этого параметра см. в Руководстве по администрированию соответствующего модуля.

Сервер QUIK может быть запущен с [ключами](#) или [без ключей](#).

Рекомендуемое расписание

Время	Событие
До 05:30	Запуск сервера QUIK (сервис QuikServer)
05:35	Запуск Модуля формирования кросс-курсов (CrossRateTW)
05:40	Запуск Репликатора (RepITW)
05:45	Запуск Модуля рассылки уведомлений (SMS)
05:47	Запуск Серверов доступа и Модулей web2QUIK



Время	Событие
05:50	Запуск шлюзов МБ AstsBridge или DFServer (Фондовый, Валютный рынок, клиринговая система)
05:53	Запуск шлюза торговой системы SPECTRA Срочного рынка МБ (SpectraCGate)
05:55	Запуск Торгового интерфейса Валютного рынка МБ (AstsCurrGate) и Программного интерфейса Клиринговой системы Валютного рынка МБ (AstsCurrRiskGate)
05:57	Запуск Торгового интерфейса Фондового рынка МБ (AstsGate) и Программного интерфейса Клиринговой системы Фондового рынка МБ (AstsRiskGate)
06:00	Запуск Торгового интерфейса Срочного рынка МБ (FortsGate)
05:45	Запуск Торгового интерфейса Санкт-Петербургской Биржи (SpbExchangeGate)
08:55	Запуск шлюза МБ AstsBridge или DFServer (денежный рынок)
09:05	Запуск Торгового интерфейса Денежного рынка МБ (AstsGKO)
21:05	Остановка Торгового интерфейса Денежного рынка МБ (AstsGKO)
21:10	Остановка шлюза МБ (AstsBridge, DFServer) для Денежного рынка МБ
00:00	Остановка Торговых интерфейсов Фондового и Валютного рынка МБ (AstsGate, AstsCurrGate) и Программных интерфейсов Клиринговой системы Фондового и Валютного рынка (AstsRiskGate, AstsCurrRiskGate)
00:35	Остановка Торгового интерфейса Срочного рынка МБ (FortsGate)
00:10	Остановка шлюзов МБ (AstsBridge, DFServer) для Фондового и Валютного рынка и клиринговой системы МБ
00:40	Остановка шлюза торговой системы SPECTRA Срочного рынка МБ (SpectraCGate)
00:05	Остановка Торгового интерфейса Санкт-Петербургской Биржи (SpbExchangeGate)
02:25	Остановка Модуля формирования кросс-курсов (CrossRateTW)
02:25	Остановка Серверов доступа и Модулей web2QUIK
02:27	Остановка Модуля рассылки уведомлений (SMS)
02:27	Остановка Репликатора (RepITW)
02:30	Остановка сервера QUIK (сервис QuikServer)



Запуск сервера QUIK без ключей

При запуске без ключей сервер QUIK загружает рыночную информацию, а также информацию о заявках и сделках из файлов хранилищ. Эта информация доступна всем пользователям, подключенным к серверу QUIK, что позволяет, например, выгрузить с утра информацию о сделках за предыдущий торговый день. Очистка данных за предыдущую торговую сессию происходит в момент подключения к серверу QUIK первого торгового интерфейса.

5.10.2 Загрузка позиций и профилей клиентов

Позиции и профили клиентов должны загружаться на сервер QUIK ежедневно до начала торгов, так как позиции и профили не переносятся на следующий день, и вся информация о них на момент окончания торгов удаляется при перезапуске сервера QUIK.

В большинстве случаев загрузка позиций и профилей выполняется при помощи .lim файла, в котором каждая строка содержит информацию о позиции или профиле клиента. Файл можно получить следующими способами:

- из Рабочего места QUIK с правами менеджера после окончания предыдущего торгового дня, выбрав пункт основного меню **Брокер / Сохранить позиции в файл**;
- с помощью Программы для загрузки лимитов на сервер QUIK FillLimits;
- из учетной системы брокерской компании или банка (рекомендуется).

Загрузить позиции и профили на сервер QUIK можно следующими способами:

- При [запуске сервера QUIK](#) с ключом -loadlimits.
- В программе для загрузки лимитов на сервер QUIK [FillLimits](#).
- В программе [QMonitor](#).
- Вручную из [Рабочего места QUIK](#).
- С помощью Программного интерфейса управления лимитами QuikLimit.

Запуск сервера QUIK с ключом -loadlimits

Этот способ рекомендуется как наиболее быстрый.

1. Скопируйте подготовленный файл .lim в директорию, которая доступна серверу QUIK.
2. Запустите сервер QUIK с параметрами -clean -loadlimits <путь к файлу с позициями>. Например:

```
sc start QuikServer -clean -loadlimits C:\quik\limits.lim
```

Вместо ключа [-clean](#) может использоваться ключ [-new](#) за исключением ситуаций, когда на сервер загружены некорректные позиции по деньгам и инструментам и необходимо загрузить корректный файл с позициями.



Программа для загрузки лимитов на сервер QUIK FillLimits

Программа подключается к серверу QUIK как обычный пользователь, но ее запуск можно автоматизировать при помощи файлов .bat или .cmd, которые могут запускать ее по заранее установленному расписанию. Запуск программы должен выполняться после подключения торговых интерфейсов и загрузки на сервер QUIK необходимых инструментов.

Программа QMonitor

Способ используется, если файл с позициями не был подготовлен вовремя и его необходимо загрузить после запуска сервера QUIK.

1. Укажите путь к файлу с позициями в файле настроек сервера quik.ini:

```
[ctl_module]
loadlimits_file=C:\quik\server\positions.lim
```

Если эта настройка не указана, позиции будут загружены из файла «qmonitor.lim», который должен находиться в директории с сервером QUIK.

2. В программе QMonitor выберите пункт меню **Actions / Load limits from file**, чтобы загрузить позиции.

Рабочее место QUIK

Файл с позициями можно загрузить из Рабочего места QUIK с правами менеджера, выбрав пункт основного меню **Брокер / Загрузить позиции из файла**.

Недостатки:

- выполнение операции вручную менеджером;
- позиции могут быть загружены только после подключения торговых интерфейсов и получения списка доступных инструментов.

Информационный интерфейс Holiday

Интерфейс можно использовать для загрузки статической информации на сервер QUIK в неторговые дни. Например, если клиенты совершают торговые операции через систему QUIK на западных рынках, то такая необходимость возникает в дни, которые являются выходными в Российской Федерации, но рабочими на западе. Интерфейс позволяет загрузить на сервер QUIK:

- описание инструментов в отдельном режиме торгов и цен для оценки стоимости позиций клиентов;
- информацию о срочных инструментах, позициях и ограничениях по клиентским счетам для клиентов, использующих Модуль единой денежной позиции.



5.10.3 Создание резервных копий файлов

Сервер QUIK не хранит файлы в системных директориях и не прописывает в реестр Windows настройки. Файлы, необходимые для работоспособности сервера, находятся в директории, в которой установлен сервер QUIK.

Чтобы не потерять важные файлы настроек, рекомендуется перед установкой обновления версии:

- создать резервную копию директории с сервером QUIK и QUIK Administrator;
- создать резервные копии .ini файлов всех установленных торговых и информационных интерфейсов;
- сохранить логи сервера QUIK (events.log, deallib.log), логи интерфейсов и модулей минимум за последние 10 дней. Также желательно сохранить .ik файлы от сервера QUIK.

Можно использовать встроенные механизмы ротации логов, имеющиеся в сервере QUIK и других модулях.

Для всех используемых баз данных рекомендуется настроить автоматическое создание резервных копий в нерабочее время, а также процедуру реиндексации на еженедельной основе в выходные дни.

5.10.4 Синхронизация локального времени

Синхронизация локального времени с сервером времени на машинах с сервисами QUIK должна производиться в момент, когда все сервисы QUIK остановлены. Рекомендуется производить синхронизацию не чаще одного раза в сутки.

5.10.5 Восстановление после системного сбоя

При возникновении системного сбоя в процессе торгов обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

В случае сбоя в работе системного ПО или оборудования, на котором установлен сервер QUIK, может возникнуть проблема с сохранением данных в файлы хранилищ, а запуск сервера QUIK будет завершаться ошибкой.

Общий порядок остановки и запуска сервисов

1. Остановка интерфейсов/модулей, подключенных к серверу QUIK.

Остановка обязательна для следующих сервисов:

- Интерфейсы Asts* (например: Торговый интерфейс Фондового рынка Московской Биржи (сектор «Основной рынок») (AstsGate), Торговый интерфейс Валютного рынка Московской Биржи (AstsCurrGate), Программный интерфейс Клиринговой системы Фондового рынка Московской биржи (AstsRiskGate), Программный интерфейс Клиринговой системы Валютного рынка Московской биржи (AstsCurrRiskGate).



- Торговый интерфейс Срочного рынка Московской Биржи (FortsGate).
- Система брокерских котировок.
- Модуль мультиброкерского обслуживания (Multihub) (если есть в конфигурации).

Необходимость остановки этих сервисов зависит от условий:

- Торговый интерфейс СПБ Биржи (Рынок иностранных ценных бумаг) (SpbExchangeGate), Торговый интерфейс СПБ Биржи (Рынок российских ценных бумаг) (SpbExchangeRuGate) – только в случае сбоя в торговой системе СПБ Биржи, из-за которого на сервер QUIK загружена некорректная информация.

Остановка не требуется для следующих сервисов:

- Клиентские приложения.
- Технологические приложения (например, сервер доступа, Модуль экспорта биржевой информации, Программный интерфейс FIX adapter).
- Исключение: Сервис Q2Q (см. [особенности](#)).

2. Остановка сервера QUIK.

3. Запуск сервера QUIK с ключом [-clean](#) (может комбинироваться с [-loadlimits](#)) или [-new](#).

4. Запуск интерфейсов/модулей, имеющих в конфигурации и использующихся совместно с одним из остановленных интерфейсов/модулей).

Рекомендуемый временной промежуток между запусками торговых интерфейсов – 1-3 минуты.

Интерфейсы Asts*, Торговый интерфейс СПБ Биржи (Рынок иностранных ценных бумаг) и Торговый интерфейс СПБ Биржи (Рынок российских ценных бумаг) запускаются только с ключом [-clean](#).

Особенности запуска Торгового интерфейса Срочного рынка Московской Биржи (FortsGate) см. [ниже](#).

Особенности запуска с ключами **-new** и **-clean**

Запуск сервера QUIK с ключом **-new** или **-clean** может использоваться в следующих случаях:

- при обновлении сервера QUIK (ключ **-new** или **-clean**);
- на сервер загружены некорректные данные (например, из-за сбоя на бирже или нарушения регламента запуска сервисов QUIK):
 - кроме позиций и новостей (ключ **-new**);
 - в том числе позиции по деньгам и инструментам (ключ **-clean**).
- при возникновении системного сбоя (отсутствие свободного места на диске, аппаратная проблема, внезапное отключение питания), который привел к повреждению файлового хранилища:
 - кроме хранилищ с позициями и новостями (ключ **-new**);



— в том числе хранилища с позициями или новостями (ключ -clean).

В этом случае сервер не запускается, а тип поврежденного хранилища сохраняется в файл events.log сервера QUIK.

Для проведения диагностики по файлу events.log обратитесь в Службу технической поддержки QUIK: quiksupport@argatech.com.

Остановка и запуск Сервиса Q2Q

Порядок остановки и запуска сервисов при использовании Сервиса Q2Q отличается от [Общего порядка](#) и должен быть следующим:

1. Остановка master-сервера.
2. Запуск master-сервера с ключом [-new](#) или [-clean](#).
3. Остановка Сервиса Q2Q и интерфейсов/модулей (см. шаг 1 [Общего порядка](#)).
4. Остановка slave-сервера.
5. Запуск slave-сервера с ключом [-new](#) или [-clean](#).
6. Запуск Сервиса Q2Q и интерфейсов/модулей (см. шаг 4 [Общего порядка](#)).

Запуск Торгового интерфейса Срочного рынка МБ

В течение дневной торговой сессии клиенты выставляют заявки, которые после основного клиринга переносятся на вечернюю сессию. Остальные заявки снимаются торговой системой. Торговый интерфейс Срочного рынка Московской Биржи (FortsGate) анализирует состояние сессии и при наступлении вечернего клиринга снимает заявки, срок действия которых ограничен текущей сессией.

Если в ходе основной торговой сессии произошел сбой, и сервер QUIK перезапускается с ключом -new или -clean после начала вечерней сессии на Срочном рынке МБ (после 19:00 МСК), то Интерфейс необходимо запустить с ключом -new -send_esp, чтобы загрузить на сервер QUIK заявки и сделки основной торговой сессии, а также входящие позиции для корректной работы Модуля единой денежной позиции.

5.11 Список кодов ошибок сервера QUIK

Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637216	Вам запрещена работа по данному инструменту	No right to trade in this instrument
8637217	Цена заявки должна быть положительна	Order price should be positive



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637218	Цена заявки <Значение3> не соответствует установленному диапазону от <Значение1> до <Значение2>	Order price <Value3> is out of set interval from <Value1> to <Value2>
8637219	Не задана позиция по инструменту	You have no position for this instrument
8637220	Превышена позиция по инструменту	Position for the instrument is exceeded
8637221	Ошибка при изменении позиции по инструменту	Error in changing position for the instrument
8637222	Неверно указан финансовый инструмент	Incorrect name of financial instrument
8637223	Рыночная заявка для клиентского счета запрещена	Market order for the client account is forbidden
8637224	Не задана позиция пользователя по деньгам	Money-position for the client is missed
8637225	Вам запрещена работа по данному торговому счету	No right for this trading account
8637226	Превышена позиция по деньгам	Money-position is exceeded
8637227	Ошибка при изменении позиции по деньгам	Error while changing money-position
8637231	Превышено максимально возможное количество инструментов	Securities amount exceed tolerable one
8637232	Заявка периода закрытия запрещена	Close period order is forbidden
8637233	Количество в заявке должно быть положительно	Order depth should be positive
8637236	Подача заявок по данному торговому счету и финансовому инструменту запрещена	Orders for this trading account and financial instrument are prohibited
8637237	Превышен общий лимит кредитования	Common limit is exceeded
8637238	Операции по данному клиентскому коду запрещены	Operations on this client code are prohibited



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637239	Превышен максимальный лимит кредитования	Maximum limit is exceeded
8637240	Данный инструмент запрещен для операции шорт	Security is restricted for short operation
8637242	Достигнут минимальный уровень клиентского обеспечения	Minimal level of client assets
8637243	Запрещена операция с указанным контрагентом	Operations are not allowed for the specified counterparty
8637244	Запрещена операция с указанным кодом расчетов	Operations are not allowed for the specified settlement code
8637245	Не определено ГО по инструменту	Initial margin of contract is undefined
8637247	Объем заявки не может быть меньше <Значение1>	The order value cannot be less than <Value1>
8637248	По данному инструменту разрешено только закрытие позиции	Order volume is out of range
8637249	Превышен общий лимит инструментов обеспечения	Total limit for collateral securities exceeded
8637250	Для выбранного финансового инструмента нижний дисконт не может быть меньше начального дисконта более чем на <Значение1>	Low discount for the selected security must not be smaller than the initial discount by more than <Value1>
8637251	Для выбранного финансового инструмента верхний дисконт не должен превышать начальный дисконт более чем на <Значение1>	High discount for the selected security must not exceed the initial discount by more than <Value1>
8637252	Объем заявки <Значение1> превышает заданное ограничение <Значение2> от среднедневного оборота <Значение3>	The order volume <Value1> exceeds the limit in <Value2> from the average daily turnover <Value3>
8637253	Вам запрещены операции в классе <Значение1> с указанными параметрами заявки	Operations in <Value1> class with the specified parameters are not allowed
8637254	Вам запрещено заключение сделок РЕПО по <Значение1> с указанной направленностью и/или сроком РЕПО	REPO transactions on <Value1> of the specified direction and/or REPO term are prohibited



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637255	Вам запрещены операции с инструментом <Значение1>	Operations with <Value1> instrument are prohibited
8637256	Рыночная заявка на продажу по инструменту <Значение1> в классе <Значение2> запрещена	Placing a market order to sell <Value1> in <Value2> class is prohibited
8637257	Рыночная заявка на продажу в шорт по инструменту <Значение1> в классе <Значение2> запрещена	Placing a market short order to sell <Value1> in <Value2> class is prohibited
8637258	Превышен максимально допустимый объем заявки <Значение1>	Maximum order value <Value1> exceeded
8637259	Заявка может привести к недопустимому размеру длинной позиции <Значение1> для <Значение2> (максимальная позиция <Значение3>)	An order can lead to an unacceptable long position size <Value1> in <Value2> (max. position <Value3>)
8637260	Заявка может привести к недопустимому размеру короткой позиции <Значение1> для <Значение2> (максимальная позиция <Значение3>)	An order can lead to an unacceptable short position size <Value1> in <Value2> (max. position <Value3>)
8637261	Превышено максимальное количество транзакций <Значение1> в интервале <Значение2> сек	Maximum transactions quantity <Value1> on interval <Value2> exceeded
8637262	Количество в заявке не может превышать <Значение1>	The order quantity must not exceed <Value1>
8637263	Количество в заявке не может быть меньше <Значение1>	The order quantity cannot be less than <Value1>
8637264	Цена не может быть больше <Значение1>	The order price cannot be higher than <Value1>
8637265	Цена не может быть меньше <Значение1>	The order price cannot be lower than <Value1>
8637266	Скорректированное значение НПП1 <Значение1> меньше 0	The corrected RCS1 <Value1> is less than 0



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637267	Скорректированное значение НПП1 меньше 0. Непокрытая позиция по неликвидному инструменту	The corrected RCS1 is less than 0. The short position in non-liquid instrument
8637268	Не найдено описание инструмента валюты расчетов	Security of settle currency is not found
8637269	Операция запрещена: недопустимый CFI код	The operation is not allowed. CFI code is not valid
8637270	Непокрытая позиция <Значение1> по <Значение2> с учетом обязательств	Short position <Value1> in <Value2> less liabilities
8637271	Операция запрещена из-за наличия короткой позиции по опциону <Значение1>. Допускается только закрытие позиций	Operation is prohibited due to a short in the option <Value1>. Only position closing is allowed
8637272	В классе <Значение1> запрещено заключение сделок РЕПО, в срок которых попадает дата фиксации списка держателей облигации для выплаты купона	REPO trades with a term that includes the record date for coupon payment are not allowed for the class <Value1>
8637319	Цена заявки должна быть меньше <Значение1>	The order price must be lower than <Value1>
8637320	Цена заявки должна быть больше <Значение1>	The order price must be higher than <Value1>
8637326	Максимальный размер обязательств превышен на <Значение1> <Значение2>	The maximum size of liabilities was exceeded by <Value1> <Value2>
8637336	Операции запрещены	Operations are prohibited
8637337	Операции с инструментами <Значение1> запрещены	Operations with <Value1> instruments are prohibited
8637338	Операции с датой расчетов <Значение1> и позднее запрещены	Operations with settlement date <Value1> or greater are prohibited
8637339	Операции с датой расчетов <Значение1> и позднее запрещены для инструментов <Значение2>	Operations with settlement date <Value1> or greater are prohibited for <Value2> instruments
8637340	Ввод заявки по <Значение1> запрещен: недопустимый ISIN-код инструмента	You cannot enter an order for <Value1>. The instrument ISIN code is not allowed



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637341	Ввод заявки по инструменту <Значение1> запрещен. Для совершения операций с <Значение2> для неквалифицированных инвесторов обязательно прохождение тестирования на тип сложного финансового продукта <Значение3>	You cannot enter an order for instrument <Value1>. Operations with <Value2> are available for unqualified investors successfully tested on complex financial product type <Value3>
8637342	Превышен лимит для срока <Значение1> на <Значение2> <Значение3>	The limit is exceeded for the period <Value1> by <Value2> <Value3>
8637343	Недостаточно денежных средств для передачи в депозит	Insufficient funds to deposit
8637346	Запрещены операции покупки	Buy operations are prohibited
8637347	Запрещены операции продажи	Sell operations are prohibited
8637348	Запрещены операции покупки с инструментами <Значение1>	Buy operations are prohibited for <Value1> instruments
8637349	Запрещены операции продажи с инструментами <Значение1>	Sell operations are prohibited for <Value1> instruments
8637350	Запрещены операции покупки с датой расчетов <Значение1> и позднее	Buy operations with settlement date <Value1> or greater are prohibited
8637351	Запрещены операции продажи с датой расчетов <Значение1> и позднее	Sell operations with settlement date <Value1> or greater are prohibited
8637352	Запрещены операции покупки для инструментов <Значение2> с датой расчетов <Значение1> и позднее	Buy operations with settlement date <Value1> or greater are prohibited for <Value2> instruments
8637353	Запрещены операции продажи для инструментов <Значение2> с датой расчетов <Значение1> и позднее	Sell operations with settlement date <Value1> or greater are prohibited for <Value2> instruments
8637354	Недостаточно <Значение1> для выставления заявки	The available quantity of <Value1> is not sufficient to enter an order
8637355	Ошибка при получении фьючерсного лимита по бумагам	Error while receiving a futures limit for securities



Десятичный код ошибки	Текст ошибки в интерфейсе на русском языке	Текст ошибки в интерфейсе на английском языке
8637356	Ошибка при получении фьючерсного лимита по деньгам	Error while receiving a futures limit for cash
8637357	Ошибка при установке лимита по бумагам	Error while setting securities limit
8637358	Ошибка при установке лимита по деньгам	Error while setting cash limit

