



Двухфакторная аутентификация QUIK

Руководство пользователя

Версия 15.3



Содержание

1. Двухфакторная аутентификация QUIK	3
2. Настройка двухфакторной аутентификации QUIK	3
2.1 Настройки в файле quik.ini	3
2.1.1 Секция [mail]	3
2.1.2 Секция [mobile_terminals]	4
2.1.3 Секция [quik_auth]	4
2.2 Настройки в программе QUIK Administrator	9
3. Отчет по параметрам двухфакторной аутентификации QUIK	10
4. Первичное получение / восстановление пароля	12
5. Вход в систему с помощью двухфакторной аутентификации QUIK	13
Приложение. Макрокоманды для текстовых шаблонов	14

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



1. Двухфакторная аутентификация QUIK

Двухфакторная аутентификация на сервере QUIK – это дополнительный уровень безопасности, позволяющий защитить терминал пользователя от несанкционированного доступа.

Несанкционированный доступ возможен из-за утери или кражи ключей доступа к системе злоумышленниками и может повлечь за собой нанесение финансового ущерба пользователю.

Использование двухфакторной авторизации предполагает, что пользователь при входе в систему наряду с обычными параметрами (имя и пароль для защиты секретного ключа) вводит пароль доступа (далее – ПАРОЛЬ), полученный через канал связи, который не может быть перехвачен злоумышленниками. ПАРОЛЬ можно получить:

- по SMS – на номер мобильного телефона, указанный пользователем;
- по электронной почте – на адрес, указанный пользователем;
- от представителя организации-брокера (далее БРОКЕР), через которого работает пользователь (например, по телефону).

Необходимость ввода нового ПАРОЛЯ возникает при попытке установки связи с устройства, с которого пользователь ни разу не устанавливал связь (потенциально возможная ситуация, если ключи и пароль были украдены). Для обнаружения такой ситуации сервер системы QUIK идентифицирует и запоминает параметры каждого подключения пользователя, использующего новую схему двухфакторной аутентификации и, при подозрении на изменение параметров подключения, запрашивает ПАРОЛЬ. Данный ПАРОЛЬ сообщается пользователю по заранее определенному каналу связи.

2. Настройка двухфакторной аутентификации QUIK

2.1 Настройки в файле quik.ini

Откройте для редактирования файл **quik.ini** в каталоге QUIK\Server\ с настройками сервера QUIK.

Настройте следующие параметры в секциях:

2.1.1 Секция [mail]

- **FromAddress** – адрес отправителя писем, связанных с двухфакторной аутентификацией и восстановлением пароля.



2.1.2 Секция [mobile_terminals]

- **System** – операционные системы мобильных терминалов. Значение по умолчанию: «Android,iPhone». Для мобильных устройств возможна настройка отправки PIN-кода двухфакторной аутентификации в момент подключения к серверу QUIK. При получении значения параметра, которое включает одну из строк данной настройки, сервер идентифицирует мобильный терминал и запрашивает PIN-код только после полной проверки прав на разрешение работы терминала.

2.1.3 Секция [quik_auth]

Параметры двухфакторной аутентификации

- **retry** – количество дополнительных попыток ввода PIN-кода после неверного ввода. При исчерпании попыток ввода PIN-кода второго фактора, производится отключение пользователя от сервера без его блокировки. Значение по умолчанию: «0». Параметр не обязателен для заполнения.
- **Quik_Auth_Wait_TMO** – период ожидания ввода пользователем PIN-кода в секундах. Значение по умолчанию: «75».
- **BlockTypeOnUnsuccessAuth** – тип блокировки в результате ввода неверного пароля при аутентификации заданное количество раз. Возможные значения:
 - «0» – не блокировать;
 - «1» (по умолчанию) – блокировать пользователя на время, заданное в настройках;
 - «2» – сбросить пароль пользователя.

Настройка используется, если настройка [UnsuccessAuthMaxAttempts](#) содержит значение, отличное от «0».

Общий параметр

- **PinCodeDefaultTransport** – способ доставки PIN-кода. Возможные значения:
 - «sms» (по умолчанию);
 - «email»;
 - «no» – используются оба способа.

Если выбранный способ недоступен, сервер использует альтернативный канал при его наличии.

Например, у пользователя указана только почта (номер телефона отсутствует), и используется:

```
PinCodeDefaultTransport = sms
```

Тогда PIN-код отправляется пользователю по email.



Параметры восстановления пароля

- **RetrievePassword** – режим восстановления пароля. Возможные значения:

- «0» (по умолчанию) – выключен;
- «1» – включен.

Если на сервере аутентификация по имени и паролю не используется или не включен режим двухфакторной аутентификации, то независимо от значения настройки, считается, что режим выключен.

- **RetrievePasswordOnLockedUsers** – режим восстановления пароля для заблокированных пользователей. Возможные значения:

- «0» (по умолчанию) – выключен;
- «1» – включен.

- **RetrievePasswordOnTerminalTypes** – список кодов типов терминалов через разделитель «|», для которых разрешено восстановление паролей. Возможные значения:

- «ALL» (по умолчанию) – все типы терминалов. Если указан этот код, то все прочие коды игнорируются;
- «DESKTOP» – Рабочее место QUIK;
- «IQUIKX» – Рабочее место iQUIK X;
- «QUIKANDROIDX» – Рабочее место QUIK Android X;
- «WEBQUIK» – Рабочее место webQUIK.

- **UseEmailOnRetrievePassword** – признак отправки пароля по e-mail при восстановлении пароля. Возможные значения:

- «0» – выключено. Пароль отправляется по SMS. Возможно только при использовании SMS в качестве второго фактора авторизации;
- «1» (по умолчанию) – включено.

- **SendMsgOnChangePassword** – признак отправки оповещения при изменении пароля, если включена двухфакторная аутентификация. Возможные значения:

- «0» – не отправлять;
- «1» (по умолчанию) – отправлять.

Исходя из соображений безопасности, не рекомендуется отключение отправки оповещения об изменении пароля.

- **NewRetrieveCodeTimeOut** – список временных интервалов через запятую до запроса нового кода подтверждения. Интервалы задаются в секундах. Значение 0 означает, что запрос нового кода доступен немедленно. Количество значений в списке соответствует максимальному количеству попыток запроса нового кода подтверждения. Например, значение «0, 60, 120, 240» говорит о том, что пользователь может запросить новый код подтверждения 4 раза, не включая код, который высылается автоматически. При этом



запрос первого кода доступен сразу, следующий – через минуту, далее через 2 и 4 минуты. Значение по умолчанию: «0, 0, 0, 0, 0» (5 запросов нового кода без ожидания).

- **NewRetrieveCodeMaxAttempts** – максимальное количество попыток ввода кода подтверждения. Значение по умолчанию: «0» – число попыток не ограничено.
- **RetrieveCodeProcessingTimeOut** – максимальное время (в секундах) ожидания ответа после отправки кода подтверждения. Значение по умолчанию: 0 (без ограничений).
- **TemporaryPasswordLength** – длина временного пароля для аутентификации по логину и паролю. Целое число в интервале от 8 до 32. Если задано число, не входящее в указанный интервал, то используется ближайшая граница интервала. Значение по умолчанию: «8».
- **TemporaryPasswordSymbols** – список наборов символов, допустимых во временном пароле. Значения в списке задаются через разделитель «|». Возможные значения:
 - _ «Number» – цифры (0-9);
 - _ «Lowercase» – прописные буквы латинского алфавита (a-z);
 - _ «Uppercase» – строчные буквы латинского алфавита (A-Z);
 - _ «Underline» – символ подчеркивания («_»);
 - _ «Minus» – минус («-»);
 - _ «Space» – пробел (« »).

Обязательно должно быть указано одно из значений: «Number», «Lowercase», «Uppercase». Значение по умолчанию: «Lowercase|Number».

- **TemporaryPasswordMaxAttempts** – максимальное количество попыток восстановления пароля в день. Значение по умолчанию: «0» (ограничение отсутствует).
- **TemporaryPasswordValidityPeriod** – срок, в течение которого временный пароль действителен, в минутах. Значение по умолчанию: «0» (пароль имеет срок действия постоянного пароля). Максимальное значение: «1440».
- **AddInfoOnRetrievePassword** – тип дополнительной информации, требуемой для начала процедуры восстановления пароля. Возможные значения:

- _ «0» – не запрашивается;
- _ «1» – адрес электронной почты для двухфакторной аутентификации;
- _ «2» – номер телефона для двухфакторной аутентификации;

Значение по умолчанию:

- _ «1» (адрес электронной почты), если [UseEmailOnRetrievePassword=1](#);
- _ «0» (не запрашивается), если [UseEmailOnRetrievePassword=0](#)).

- **CheckLastDigitsInPhoneNumber** – количество последних цифр в номере телефона, проверяемых на совпадение. Используется, если в качестве дополнительной информации запрашивается номер телефона ([AddInfoOnRetrievePassword=2](#)). Значение «0» соответствует полной проверке номера на соответствие. Значение по умолчанию: «10».
- **UnsuccessAuthMaxAttempts** – максимальное число попыток аутентификации за торговую сессию. Значение «0» соответствует отсутствию ограничения на число попыток. Значение по умолчанию: «10».



- **AlertOnUnsuccessAuth** – оповещение пользователя при вводе неверных данных для аутентификации заданное количество раз. Возможные значения:

- «0» – не оповещать;
- «1» (по умолчанию) – оповещать.

Настройка используется, если настройка [UnsuccessAuthMaxAttempts](#) содержит значение, отличное от «0».

- **BlockPeriodOnUnsuccessAuth** – время в секундах, на которое блокируется пользователь в результате ввода неверных данных для аутентификации заданное количество раз. Значение по умолчанию: «10».

Настройка используется, если [BlockTypeOnUnsuccessAuth](#)=1.

- **Template<Язык><Код типа шаблона>FileName** – путь к файлу, содержащему шаблон сообщения о восстановлении пароля или код для двухфакторной аутентификации. Для каждого типа шаблона создается отдельный файл шаблона. Тексты шаблонов могут содержать макрокоманды (подробнее см. [Приложение](#)).

Где:

- <Язык> – язык сообщения. Возможные значения:
 - «Ru» – русский;
 - «En» – английский;
 - «Def» – язык не определен. Может использоваться для шаблонов типа «2ndFactorAuthSubject» и «2ndFactorAuthText».
- <Код типа шаблона> – тип сообщения. Возможные значения:

Шаблоны текстов, используемых для процедуры восстановления пароля:

 - «RetrievingNotSupported» – текст, отображаемый, если в данной конфигурации Сервер QUIK не поддерживает процедуру восстановления пароля вообще или для данного пользователя.
 - «MaxRetrievingAttempts» – текст, отображаемый при попытке восстановления пароля, если превышено число попыток восстановления пароля.
 - «UserUnknown» – текст, отображаемый, если пользователь указал неверный логин или неверный e-mail при запросе восстановления пароля.
 - «UnknownError» – текст, отображаемый в случае недоступности Модуля рассылки уведомлений или при возникновении любой другой ошибки при отправке SMS-сообщения.
 - «IncorrectCode» – текст, отображаемый, если пользователь указал неверный код, отправленный ему для подтверждения восстановления пароля.
 - «TooMuchErrorsForCode» – текст, отображаемый, если пользователь превысил максимальное число попыток ввода кода подтверждения.
 - «TooMuchErrors» – текст, отображаемый, если при запросе нового пароля возникло большое количество ошибок.



- «RetrievingInfo» – текст, отображаемый в диалоге «Идентификация пользователя». Этот текст отображается в диалоге с полями для ввода логина и e-mail. Длина не более 700 символов. Может быть не задан (в этом случае текст не отображается).
- «InfoDescription» – ссылка на правила восстановления пароля. Отображается в диалоге «Идентификация пользователя». Длина не более 100 символов. Может быть не задан (в этом случае текст не отображается).
- «InfoText» – текст правил восстановления пароля. Отображается при нажатии на ссылку в диалоге «Идентификация пользователя». Длина не более 4 КБайт. Формат текста: обычный (plain text). Обязательно для настройки, если задан «InfoDescription».
- «WaitForCode» – текст сообщения о том, что пользователю направлен код для подтверждения процедуры создания нового пароля. Отображается в диалоге «Подтверждение сброса пароля» и в уведомлении, которое появляется при нажатии на ссылку «Выслать код повторно».
- «PasswordSent» – текст сообщения о том, что для пользователя создан новый пароль, который отправлен на адрес электронной почты.
- «AddInfoTitle» – наименование дополнительного поля.
- «BlockOnUnsuccseccAuth» – текст оповещения, отображаемого при блокировке учетной записи пользователя в результате ввода неверных данных для аутентификации заданное количество раз.

Шаблоны оповещений об изменении пароля:

- «PasswordChangedSubject» – тема письма, отправляемого по электронной почте при изменении пароля.
- «PasswordChangedText» – текст сообщения, отправляемого при изменении пароля. Отправляется тем же способом, что и второй фактор при двухфакторной аутентификации типа QUIK.

Если шаблоны не настроены, и задана настройка

SendMsgOnChangePassword, то при изменении пароля по умолчанию рассылается следующий текст уведомления: «Ваш пароль был успешно изменён. Ранее использовавшийся пароль более не действителен».

Шаблоны текстов (также в виде ссылки на файл с текстом шаблона), используемых для отправки сообщений пользователям по SMS и электронной почте:

- «Code» – текст сообщения с кодом подтверждения. Отправляется с одноразовым кодом подтверждения, используемым для начала процедуры восстановления пароля. Отправляется тем же способом, что и второй фактор при двухфакторной аутентификации типа QUIK (обычно SMS). Длина не более 280 символов (4 SMS).
- «NewPasswordSubject» – тема письма с временным паролем, отправляемого по электронной почте. Длина не более 128 символов.



- «NewPasswordText» – текст письма с временным паролем. Сервер QUIK отправляет письмо с одноразовым кодом подтверждения, используемым для начала процедуры восстановления пароля, по электронной почте. Формат текста: обычный (plain) или HTML. Длина не более 4 Кбайт.

Шаблоны, с помощью которых задаются тема письма и текст с кодом для двухфакторной аутентификации:

- «2ndFactorAuthSubject» – тема письма со вторым фактором. Отправляется при прохождении аутентификации с использованием второго фактора. Длина не более 128 символов.
- «2ndFactorAuthText» – текст письма со вторым фактором. Отправляется при прохождении аутентификации с использованием второго фактора, а также при восстановлении пароля. Длина не более 4 Кбайт. Формат текста: обычный (plain) или HTML. Если отправка PIN-кода двухфакторной аутентификации производится посредством SMS, то настройка игнорируется.

Например:

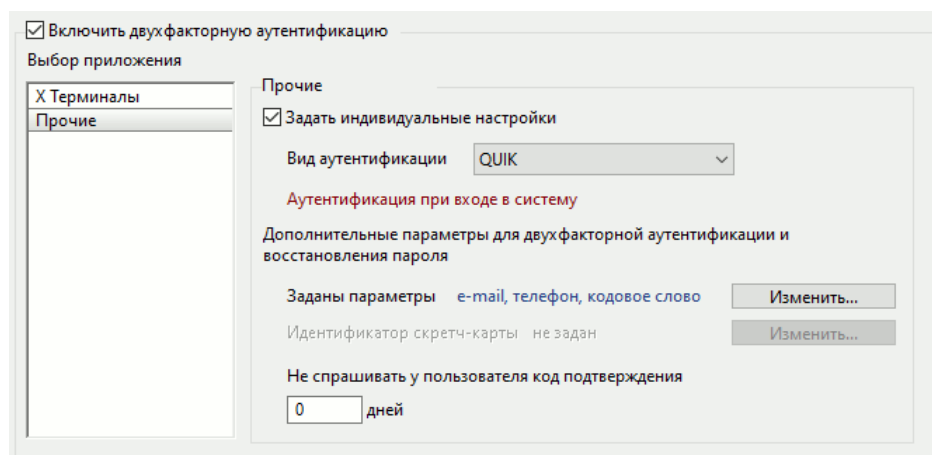
```
TemplateRuInfoTextFileName=Templates\ru\InfoText
```

- **Template<Тип шаблона>Type** – формат файла шаблона. Поддерживается для типов шаблона «NewPasswordText» и «2ndFactorAuthText». Возможные значения:
 - «plain» (по умолчанию) – обычный текст;
 - «html» – текст в HTML-формате.

2.2 Настройки в программе QUIK Administrator

В программе QUIK Administrator выполните следующие действия:

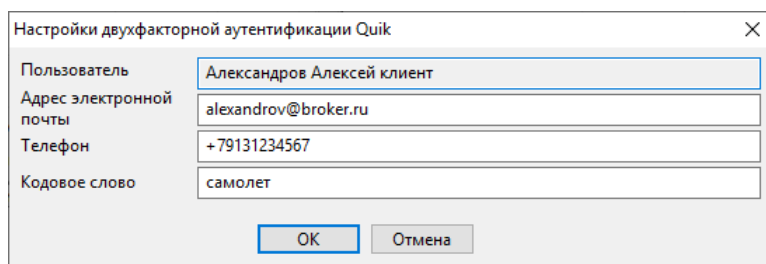
1. В диалоге настройки прав пользователя на вкладке «Безопасность» установите опцию «Включить двухфакторную аутентификацию» и выберите вид аутентификации «QUIK».



- Поле «Не спрашивать у пользователя код подтверждения ... дней» – количество дней, в течение которых не будет запрашиваться дополнительный пароль для двухфакторной аутентификации при условии, что пользователь не изменяет параметры подключения. Допустимые значения: целые числа от 1 до 365. Доступно для редактирования при выбранном виде аутентификации «QUIK».

При изменении параметров подключения дополнительный пароль запрашивается снова. Если поле не заполнено или указано значение «0», то новый дополнительный пароль запрашивается при каждом сеансе связи пользователя.

2. При нажатии на кнопку «Изменить...» появляется форма, в которой доступно заполнение следующих полей для разных способов доставки пароля до клиента:



- Поле «Адрес электронной почты» – электронный адрес клиента, на который отправляется письмо с паролем.
- Поле «Телефон» – номер мобильного телефона клиента, на который отправляется SMS. Для работы этого способа доставки пароля брокеру требуется провести интеграцию с сервисом отправки SMS-сообщений.
- Поле «Кодовое слово» – секретное слово, которое идентифицирует пользователя при сообщении ему пароля.

Способы доставки пароля пользователю могут использоваться как по отдельности, так и вместе.

3. Отчет по параметрам двухфакторной аутентификации QUIK

Отчет служит для создания списка паролей пользователей, которые устанавливают связь с помощью двухфакторной аутентификации QUIK. В отчете отображаются только те пользователи, у которых заполнено поле «кодовое слово» в настройках пользователя.

Отчет используется, например, если клиент звонит брокеру и просит назвать его пароль для установления связи. В этом случае брокеру следует создать отчет по данному клиенту и спросить у клиента кодовое слово. Отчет вызывается из программы QUIK Administrator (меню **Сервер QUIK / Отчеты / Кодовые слова...**).



Кодовые слова

Пользователь

☐ по всем пользователям ☒ по одному пользователю

Гусева 01 Елена

OK Отмена

Если кодовое слово названо верно, клиенту в ответ сообщается пароль для прохождения двухфакторной авторизации.

Отчет по параметрам двухфакторной аутентификации Quik

Главный отчет

Дата создания отчета : 29.05.2019 13:31

Отчет по параметрам двухфакторной аутентификации Quik

Идентификатор пользователя :	100101
Пользователь:	Гусева 01 Елена
Пароль сервера :	71939
Кодовое слово:	лето

Номер текущей страницы: 1 Количество страниц: 1 Коэффициент масштабирования: 100%

Отчет можно построить сразу по всем клиентам, которым требуется сообщить пароль. Для этого выберите опцию «по всем пользователям».



4. Первичное получение / восстановление пароля

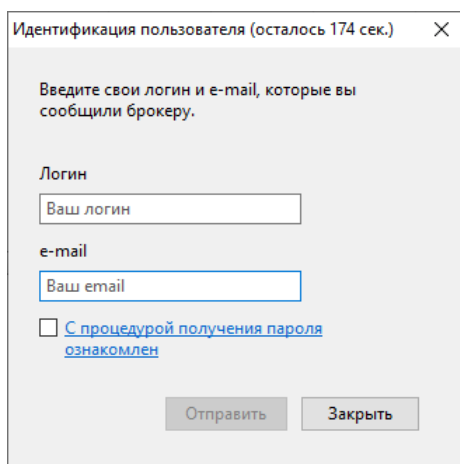
Если пароль для аутентификации пользователю неизвестен (пользователь еще не получил пароль или пароль был утерян), он может получить его без личного визита к брокеру и без участия сотрудников брокера.

Работа сервиса восстановления пароля возможна при одновременном выполнении следующих условий:

- Для пользователя используется аутентификация по логину и паролю.
- Включена двухфакторная аутентификация типа «QUIK» с отправкой второго фактора аутентификации по SMS.
- У пользователя в настройках заданы телефон и e-mail для двухфакторной аутентификации.
- Включена настройка [RetrievePassword](#) в секции [quik_auth] файла quik.ini.

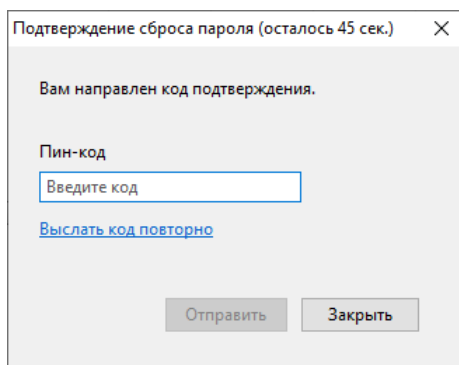
При прохождении процедуры первичного получения / восстановления пароля пользователю отображаются диалоги, наполнение которых настраивается брокером с помощью [шаблонов](#). Ниже приведены варианты диалогов, основанных на шаблонах, поставляемых по умолчанию.

- В диалоге «Вход в систему» пользователь нажимает «Получить пароль». Открывается диалог «Идентификация пользователя».



- Пользователь вводит логин и e-mail и подтверждает, что ознакомился с процедурой восстановления пароля, установив соответствующий флажок.
- Сервер проверяет, что для пользователя включена двухфакторная аутентификация, и срок доверенности не истек. Если проверка выполнена успешно, сервер отправляет пользователю код подтверждения по SMS.
- В окне «Подтверждение сброса пароля» пользователь вводит полученный код.





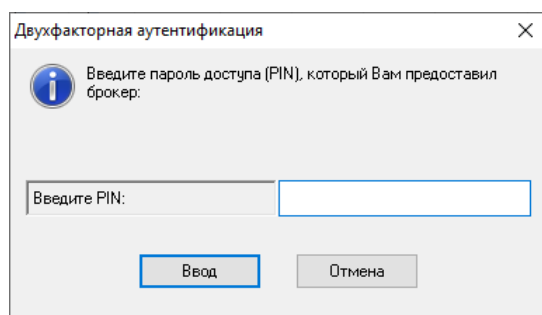
- Сервер проверяет код, генерирует временный пароль и отправляет его пользователю по e-mail.

5. Вход в систему с помощью двухфакторной аутентификации QUIK

Первая часть процедуры аутентификации (с использованием ключей доступа из файлов `pubring.txk` и `secring.txk` или логина и пароля) происходит в обычном режиме – вводятся имя и пароль, и сервер проверяет соответствие введенных параметров. Если первая часть аутентификации прошла успешно, сервер QUIK начинает вторую часть аутентификации по следующему регламенту:

1. Сервер QUIK проверяет параметры подключения, с которого устанавливается связь.
2. Если информация о подключении серверу известна, далее проверяется, является ли это подключение подтвержденным на сервере QUIK (пройдена ли двухфакторная аутентификация при предыдущем установлении связи).
3. Контролируется, не истек ли период экспирации подключения (период экспирации устанавливается в настройках пользователя в программе QUIK Administrator, см. [п. 2.2](#)).

Если все проверки пройдены успешно, то двухфакторная аутентификация QUIK считается завершенной, и пользователю начинают поступать данные с сервера. Если хотя бы одна из проверок не пройдена, то пользователю предлагается подтвердить параметры нового подключения вводом нового ПАРОЛЯ.



В момент появления формы для ввода пароля, клиенту отправляется пароль по заранее определенному каналу связи – по электронной почте, по SMS или с помощью звонка брокеру. В последнем случае для получения пароля клиент должен назвать брокеру кодовое слово. Если пароль, введенный в поле, совпадает с требуемым паролем, то новое подключение считается подтвержденным.

Если время ожидания ввода ПАРОЛЯ истекло, то требуется повторно пройти первую часть аутентификации (ввод имени и пароля для защиты секретного ключа).

Количество попыток ввода пароля ограничено. После использования всех попыток пользователь временно блокируется или сбрасывается пароль. Информация о временной блокировке пользователя, а также возможность снять блокировку доступны в QUIK Administrator в диалоге редактирования пользователя на вкладке «Безопасность».

Приложение. Макрокоманды для текстовых шаблонов

В шаблоны текстов, используемых для различных оповещений при восстановлении пароля, могут входить макрокоманды.

Все макрокоманды имеют вид: «{CMD}», где CMD – команда на вставку некоторого текстового параметра. В тексте может использоваться произвольное количество таких команд, одна и та же команда может использоваться несколько раз. При необходимости использования символов «{» или «}» в тексте они должны записываться как «{{» или «}}» соответственно.

Допустимые команды:

- DATE – текущая дата в формате <ДД.ММ.ГГГГ>.
- TIME – текущее время в формате <ЧЧ:ММ:СС>.
- UID – идентификатор пользователя (UID), для которого производится восстановление пароля.
- USERNAME – ФИО пользователя.
- PASSWORD – текст временного пароля.
- CODE – код подтверждения. Доступен только в шаблоне типа «Code».
- EMAIL – e-mail, указанный для двухфакторной аутентификации.
- BLOCKEDTILL – дата и время окончания периода блокировки (по времени сервера QUIK) пользователя в формате <ДД.ММ.ГГГГ ЧЧ:ММ:СС>. Используется, если [BlockTypeOnUnsuccessAuth](#)=1 и значение [BlockPeriodOnUnsuccessAuth](#) отлично от 0.

