Тонкий клиент (Thinclient). Руководство Администратора

19. янв. 2018

mailto:nilstarsoft@mail.ru

Оглавление

1 Используемые сокращения и термины

- ККМ — контрольно-кассовая машина (в этом документе это сокращение относится к мобильному ПТК IRAS 900K);
- Управляющая система — система, взаимодействующая с ККМ в режиме тонкого клиента (подразумевается, что на ККМ запущен программный комплекс «Тонкий Клиент»;
- Серверный режим — подразумевается что ККМ является серверной стороной соединения по сети;
- Клиентский режим — подразумевается что ККМ является клиентской стороной соединения по сети.

2 Введение

В документе приведена правила установки программного обеспечения и его настройки.

Программное обеспечение предназначено для установки и эксплуатации на ККМ оснащенной фискальным регистратором.

Программный комплекс состоит из трех компонент:

- Программа «Тонкий клиент» (thinclient.aip);
- Модуль обслуживания фискального регистратора (KKTIras.aip);
- Модуль обслуживания платежных карт (Сбербанк «UPOS» или Инпас «UniPOS»).

В этом документе подробно рассматриваются правила настройки/установки и эксплуатации программы «Тонкий клиент». Про правила настройки/установки и эксплуатации других модулей комплекса смотрите в соответствующих документах и описаниях.

Внимание: В случае использования режима приема только наличных платежей, модуль обслуживания платежных карт не устанавливается.

3 Назначение программного обеспечения

Приложение «Тонкий клиент» предназначено для предоставления управляющей системе следующих интерфейсов (сетевых протоколов):

- Работа с фискальным регистратором по искра-совместимому протоколу (протокол ПРИМ);
- Работа с модулем обслуживания платежных карт через протокол клиента отображаемых форм (используется SA протокол);
- Работа с отображаемыми формами по простому протоколу на базе xml (смотрите «Протокол клиента отображаемых форм»).

Управляющая система детектирует наличие ККМ с установленным ПО «Тонкий клиент» и подключается к ККМ как к серверу, управляя им. То есть ККМ является удаленным устройством ввода/вывода с точки зрения управляющей системы.

Оператор ККМ может осуществлять ввод запрашиваемых данных, получать чеки и отчеты, а также осуществлять сервисные операции над ККМ (смотрите «Руководство Оператора»).

4 Установка программного обеспечения

Установка программного обеспечения производится программой TermAssist (под Windows). Сама процедура установки приводится в руководстве по TermAssist (требуйте руководство у производителя).

Одновременно должны быть установлены три компоненты программного комплекса, каждая компонента устанавливается в свой подраздел (т. е. параметры для каждой компоненты загружаются раздельно и не доступны другим компонентам).

Перечень компонент для установки:

№	Наименование модуля	Имя раздела	Описание
1	thinclient.aip	MAINAPP	Основное приложение «Тонкий клиент».
2	KKTIras.aip	KKTIRAS	Подчиненное приложение для обслуживания фискального регистратора (используется сотрудниками ЦТО).
3а	S900.aip	SBER	Подчиненное приложение для обслуживания платежных карт (Сбербанк UPOS)
3б	UNIPOS.aip	UNIPOS	Подчиненное приложение для обслуживания платежных карт (Инпас UniPOS)

4.1 Загрузка дополнительных параметров к приложению

Приложение «Тонкий клиент» может иметь следующие дополнительные данные:

- Файл настроек параметров приложения [settings.xml] – смотри раздел 5;
- Файл лицензии [license.xml] – лицензия, дающая право на использование приложения;
- Файлы изображений - используются в запросах, как элементы оформления.

Эти дополнительные файлы должны быть загружены как дополнительные данные к приложению с помощью программы TermAssist (под Windows). Сама процедура загрузки дополнительных файлов данных приводится в руководстве по TermAssist.

5 Настройка параметров (файл settings.xml)

Параметры приложения «Тонкий клиент» хранятся в файле **settings.xml** и загружаются отдельно от приложения (загрузка файла параметров должна осуществляться в раздел MAINAPP).

Файл представляет собой xml-форматированный файл. Этот файл имеет основной раздел **SETTINGS** и в нем подразделы согласно группам настроек.

Структура файла:

```
<?xml … ?>
<SETTINGS>
     <CONNECTION>[параметры 1-го соединения]</CONNECTION>
     ...
     <CONNECTION>[параметры n-го соединения]</CONNECTION>
     <UDPSERVICE>[параметры]</UDPSERVICE>
     <FISCAL>[параметры]</FISCAL>
     <CLIENT>[параметры]</CLIENT>
     <BACKMENU>[параметры]</BACKMENU>
     <PAYCARD>[параметры]</PAYCARD>
</SETTINGS>
```

В файле должны быть следующие группы настроек:

- **CONNECTION** – параметры соединения, в файле настроек может быть одна или несколько групп параметров соединения (раздел 5.1);
- **UDPSERVICE** – настройка широковещательных сообщений (раздел 5.2);
- **FISCAL** – настройка протокола фискального регистратора (раздел 5.3);
- **CLIENT** – настройка протокола клиента отображаемых форм (раздел 5.4);
- **BACKMENU** – настройка сервисного меню (раздел 5.5);
- **PAYCARD** - настройка протокола модуля обслуживания платежных карт (раздел 5.6).

5.1 Параметры соединения <CONNECTION>

Подраздел описывающие параметры соединения.

На текущий момент поддерживаются два способа описания соединений:

- Новый способ — рекомендуется к использованию.
  Параметры соединения описываются ввиде аттрибутов к разделу, значение параметра эквивалентно значению атрибута (название атрибутов должно быть в нижнем регистре). Например:
  <CONNECTION name=”[имя пункта меню]” type=”[тип соединения]” mode=”[режим соединения]” … timeout=”10000” />
- Старый способ — исключительно для поддержки уже находящихся в эксплуатации ККМ. Параметры соединения описываются ввиде подразделов, значение параметра включены в подраздел. Например:
  <CONNECTION>
  <TYPE>[тип соединения]<TYPE>
  …

```
  <TIMEOUT>10000<TIMEOUT>
</CONNECTION>
```

Внимание: В описании названия разделов и их содержимое приводится для нового способа описания. Дополнительно приводится примеры, как для нового способа, так и для старого.

Внимание: Названия и формат значений параметров идентичны, но нужно учитывать, что названия параметров отличаются в регистре букв (для нового способа — нижний регистр букв, для старого — верхний регистр).

Формат описания соединения:

- новый способ:
```
<CONNECTION
  type="[тип соединения]"
  name="[название для отображения в меню]"
  mode="[режим соединения]"
  [параметры настройки оборудования]
  [параметры настройки TCPIP сети]
  [параметры настройки шифрования SSL] />
```
- старый способ:
```
<CONNECTION>
 <TYPE>[тип соединения]</TYPE>
 <NAME>[название для отображения в меню]</NAME>
 [параметры настройки оборудования]
 [параметры настройки TCPIP сети]
 <SSL>
 [раздел параметров SSL]
 </SSL>
</CONNECTION>
```

Базовые параметры:

- **type** - служит Для задания типа соединения (обязательный параметр**)**. Текущая версия ПО поддерживает следующие типы соединения:
  - **GPRS** – соединение с использованием встроенного GPRS/GSM модема ККМ;
  - **WIFI**[1] – соединение с использованием встроенного WiFi модуля ККМ;
  - **ETH** – соединение с использованием внешнего переходника USB в Ethernet.
- **mode** – режим соединения, может принимать следующие значения:
  - **SERVER**[2] – ККМ является серверной стороной соединения (по умолчанию);
  - **CLIENT** – ККМ является клиентской стороной соединения.
- **name** – строка: используется для отображения названия соединения (имя пункта меню) в меню выбора.

5.1.1 Параметры настройки оборудования для WiFi соединения

При WiFi соединении для инициализации оборудования могут использоваться следующие параметры:

1 Наличие модуля WiFi на ККМ зависит от комплектации модели ККМ (уточняйте у производителя).
2 Надо учитывать, что ККМ в этом случае должен быть в прямом доступе (без использования NAT).

- **apn** – строка: имя точки доступа;
- **pass** – строка: пароль к точке доступа;
- **auth** – режим аутентификации точки доступа (необязательный параметр):
  - **AUTO** – автоматическое определение режима (по умолчанию). В этом режиме параметры аутентификации и шифрования определяются автоматически;
  - **WPA** – WPA режим;
  - **WPA_WPA2** – WPA или WPA2 режим;
  - **WPA2** — WPA2 режим.
- **encrypt** – тип шифрования точки доступа (необязательный параметр):
  - **NONE** – без шифрования (по умолчанию);
  - **WEP** – WEP шифрование;
  - **TKIP** — TKIP шифрование;
  - **AES** — AES шифрование.

Внимание: Для работы со скрытыми WiFi точками доступа, параметры **auth** и **encrypt** должны быть установлены обязательно. Со скрытой WiFi точки невозможно получить параметры аутентификации и шифрации автоматически.

Пример настройки (новый способ):

```
<CONNECTION type="WIFI" apn="AndroidAP" auth="WPA2" encrypt="AES" pass="12345678" dhcp="1"
timeout="60000" />
```

Пример настройки (старый способ):

```
<CONNECTION>
  <TYPE>WIFI</TYPE>
  <APN>WIFINET</APN>
  <PASS>123456</PASS>
  <AUTH>WPA2</AUTH>
  <ENCRYPT>AES</ENCRYPT>
  <DHCP>1</DHCP>
</CONNECTION>
```

5.1.2 Параметры настройки оборудования для GPRS/GSM соединения (работа с операторами мобильной связи)

Для настройки GSM|GPRS соединения используются следующие параметры:

- **pin** – цифровая строка: пин-код от SIM-карты (используется для типов оборудования GPRS). Для SIM-карт, не использующих пин, определять атрибут не нужно;
- **apn** – строка: имя точки доступа в сеть;
- **login** – строка: логин для входа в сеть;
- **pass** – строка: пароль для входа в сеть;

Внимание: Параметры настройки GPRS соединения для операторов мобильной связи следует узнавать непосредственно от соответствующего оператора.

Ниже приведены параметры настройки для распространенных операторов мобильной связи.

Оператор мобильной связи	Пример настройки
Мегафон	`<conn name="MegaFon" type="GPRS" apn="internet" login="gdata" pass="gdata" ... />`
МТС	`<conn name="MTS" type="GPRS" apn="internet.mts.ru" login="mts" pass="mts" ... />`
Билайн	`<conn name="BeeLine" type="GPRS" apn="internet.beeline.ru" login="beeline" pass="beeline" ... />`
TELE2	`<conn name="TELE2" type="GPRS" apn="internet.tele2.ru" ... />` **Внимание:** не нужно указывать атрибуты **login** и **pass -** для этого оператора мобильной связи они не используются.

5.1.3 Параметры настройки TCPIP сети

Параметры служат для настройки TCPIP сети.

Внимание: Как правило для соединения мобильной связи (**type**=”GPRS”) эти настройки не используются (кроме параметра **timeout**).

Для настройки TCPIP сети используются следующие параметры:

- **dhcp** – значение 0: не использовать DHCP при инициализации соединения, 1: использовать DHCP (DHCP – автоматическое получение настроек IP);
- **ip** – значение IP адреса ККМ (если не используется DHCP);
- **mask** – значение маски сегмента сети ККМ (если не используется DHCP);
- **gateway** – значение шлюза для ККМ (если не используется DHCP);
- **dns** – сервер DN для ККМ (если не используется DHCP);
- **timeot** – таймаут поиска сети и инициализации соединения: число (в миллисекундах). Необязательный параметр, значение по умолчанию: 10000.

Внимание: Параметр **timeout** регулирует все процессы соединения, которые требуют ожидания (например: поиск сети, определение адреса по DHCP, получение ответа от мобильной сети).

Пример настроек WiFi соединения со статическим адресом (новый способ):

```
<CONNECTION type="WIFI" apn="AndroidAP" auth="WPA2" encrypt="AES" pass="12345678" dhcp="1"
timeout="60000" dhcp="0" ip="192.168.1.4" mask="255.255.255.0" gateway="192.168.1.1"
dns="192.168.1.1" />
```

Пример настроек WiFi соединения со статическим адресом (старый способ):

```
<CONNECTION>
  <TYPE>WIFI</TYPE>
  <APN>WIFINET</APN>
  <PASS>123456</PASS>
  <AUTH>WPA2</AUTH>
  <ENCRYPT>AES</ENCRYPT>
  <DHCP>0</DHCP>
  <IP>192.168.1.4</IP>
  <MASK>255.255.255.0</MASK>
  <GATEWAY>192.168.1.1</GATEWAY>
  <DNS>192.168.1.1</DNS>
```

```
  <TIMEOUT>30000</TIMEOUT>
</CONNECTION>
```

5.1.4 Параметры защиты соединения <SSL>

Подраздел используется для описания параметров защиты соединения (SSL).

Формат описания данных:

При новом способе описания нужно установить параметр **ssl**=”1” и затем добавить атрибуты с другими параметрами:

```
<CONNECTION type=”[тип соединения]” … ssl=”1” [атрибуты защиты соединения] />
```

При старом способе описания параметров нужно созадять подраздел **SSL** в разделе описания соединения:

```
<CONNECTION>
  <TYPE>[тип соединения]</TYPE>
  <SSL>
    [параметры защиты соединения]
  </SSL>
</CONNECTION>
```

Атрибуты защищенного соединения (в скобках приведены названия разделов при старом способе описания):

- **ssl_type (TYPE)** — тип протокола защищенного соединения, может принимать следующие значения:
  - **SSL23** – протокол SSL2 или SSL3;
  - **SSL3** – протокол строго SSL3;
  - **TLS1** — протокол TLS 1.0;
  - **TLS11** – протокол TLS 1.1;
  - **TLS12** – протокол TLS 1.2;
  - **DTLS1** – протокол DTLS 1.0.
- **ssl_servercert (SERVERCERT)** – имя файла[3] сертификата сервера (сертификат загружается, как параметр, вместе с файлом параметров);
- **ssl_serverkey (SERVERKEY)** – имя файла[4] закрытого ключа сервера (файл ключа загружается, как параметр, вместе с файлом параметров);
- **ssl_verifyclient (VERIFYCLIENT)** – значение 0: не использовать проверку клиентского сертификата, 1: проверять клиентский сертификат. Необязательный параметр, по умолчанию 0.
- **ssl_cacert (CACERT)** – имя файла[5] корневого сертификата, используемого для проверки клиентского сертификата (сертификат загружается, как параметр, вместе с файлом параметров).

Пример (новый способ описания):

3 **Внимание:** Операционная система ККМ чувствительна к регистру букв указанных в имени файла.
4 **Внимание:** Операционная система ККМ чувствительна к регистру букв указанных в имени файла.
5 **Внимание:** Операционная система ККМ чувствительна к регистру букв указанных в имени файла.

```
<CONNECTION ... ssl="1" ssl_type="TLS1" ssl_cacert="ca.crt"
ssl_servercert="server.crt" ssl_serverkey="server_private.pem"
ssl_verifyclient="1" />
```

Пример (старый способ описания):

```
<CONNECTION>
  <SSL>
    <TYPE>TLS1</TYPE>
    <SERVERCERT>server.crt</SERVERCERT>
    <SERVERKEY>server_private.pem</SERVERKEY>
    <VERIFYCLIENT>1</VERIFYCLIENT>
    <CACERT>ca.crt</CACERT>
  </SSL>
</CONNECTION>
```

Пример команд для генерации сертификатов и ключей с помощью OpenSSL:

1. Генерация ключей (RSA):
   ```
   openssl genrsa -out ssl\ca_private.pem

   openssl genrsa -out ssl\client_private.pem

   openssl genrsa -out ssl\server_private.pem
   ```
2. Создание самоподписанного (корневого) сертификата:
   ```
   openssl req -new -x509 -key ssl\ca_private.pem -out ssl\ca.crt -config
   ./openssl
   ```
3. Подготовка шаблона клиентского и серверного сертификата:
   ```
   openssl req -new -key ssl\server_private.pem -out ssl\server.csr
   -config ./openssl.cnf -subj
   /C=RU/ST=Msk/L=Msk/O=Inc/OU=Develop/CN=server/emailAddress=server@test.ru

   openssl req -new -key ssl\client_private.pem -out ssl\client.csr
   -config ./openssl.cnf -subj
   /C=RU/ST=Msk/L=Msk/O=Inc/OU=Develop/CN=client/emailAddress=client@test.ru
   ```
4. Создание клиентского и серверного сертификата. Подпись шаблонов корневым сертификатом:
   ```
   openssl x509 -req -days 365 -CA ssl\ca.crt -CAkey ssl\ca_private.pem
   -set_serial 01 -extfile ./openssl_client.cnf -extensions req_ext -in
   ssl\server.csr -out ssl\server.crt

   openssl x509 -req -days 365 -CA ssl\ca.crt -CAkey ssl\ca_private.pem
   -set_serial 02 -extfile ./openssl_client.cnf -extensions req_ext -in
   ssl\client.csr -out ssl\client.crt
   ```

Внимание: Сертификаты и ключи должны быть загружены на терминал Iras, в качестве параметров в раздел MAINAPP.

5.2 Параметры отправки широковещательных сообщений <UDPSERVICE>

Параметры этого раздела отвечают за отправку широковещательных (broadcast) UDP сообщений с информацией о терминале Iras управляющей системе. Формат сообщения описан в документе «Протокол клиента отображаемых форм».

Внимание: Начиная с версии ThinClientFN 2.0.9, если этого раздела нет в файле настроек, то сообщения рассылаться не будут.

Может иметь следующие подразделы:

- **TIMEOUT** - таймаут промежутка между отправкой UDP сообщений: число (в миллисекундах). Необязательный раздел, значение по умолчанию: 2000 (2 секунды);
- **PORT** – номер порта: число. Номер порта куда отправляется UDP сообщение. Необязательный раздел, значение по умолчанию: 2000;
- **IP** – адрес принимающей стороны: адрес. Необязательный раздел, по умолчанию 255.255.255.255 (broadcast).

Пример:

```
<UDPSERVICE>
  <PORT>2000</PORT>
  <TIMEOUT>2000</TIMEOUT>
</UDPSERVICE>
```

5.3 Параметры протокола фискального регистратора <FISCAL>

Параметры этого раздела отвечают за настройку протокола фискального регистратора.

Может иметь следующие подразделы:

- **IP —** адрес сервера внешней системы для подсоединения, используется и обязателен только в клиентском режиме работы. Для серверного режима работы — не используется.
- **PORT** – номер серверного порта: число. Необязательный раздел, значение по умолчанию: 4000.
    - **В серверном режиме:** Номер серверного порта для работы по протоколу фискального регистратора.
    - **В клиентском режиме:** Номер серверного порта на стороне сервера внешней системы, для работы по протоколу фискального регистратора.

Пример:

```
<FISCAL>
  <IP>195.168.1.7</IP>
  <PORT>4000</PORT>
</FISCAL>
```

5.4 Параметры протокола клиента отображаемых форм <CLIENT>

Параметры этого раздела отвечают за настройку протокола клиента отображаемых форм. Описание протокола смотрите в документе «Протокол клиента отображаемых форм».

Может иметь следующие подразделы:

- **IP —** адрес сервера внешней системы для подсоединения, используется и обязателен только в клиентском режиме работы. Для серверного режима работы — не используется.
- **PORT** – номер серверного порта: число. Необязательный раздел, значение по умолчанию: 4001;
    - **В серверном режиме:** Номер серверного порта для работы по протоколу клиента отображаемых форм.
    - **В клиентском режиме:** Номер серверного порта на стороне сервера внешней

системы, для работы по протоколу клиента отображаемых форм.

- **BACKMENUKEY –** маска клавиш для входа в сервисное меню: число. Определяет комбинацию клавиш для входа в сервисное меню (смотри раздел 6.1). Необязательный раздел, значение по умолчанию: x222 (сочетание клавиш [1]+[5]+[9]).
- **TIMEOUT** — время в миллисекундах. Необязательный раздел, значение по умолчанию: 10000 (10 секунд);
  - таймаут ожидания восстановления доступа к беспроводной сети, если в течении этого времени доступ не восстановлен — осуществляется переход в меню выбора сети;
  - в клиентском режиме — используется как время ожидания соединения с сервером, если в течении этого времени присоединиться не удалось — осуществляется переход в меню выбора сети.
- **REQMSG_TIMEOUT** — время в миллисекундах. Необязательный раздел, значение по умолчанию 2000. Определяет время задержки вывода сообщения «ОЖИДАНИЕ ЗАПРОСА» после завершения работы с формой.

Пример:

```
<CLIENT>
  <IP>pos.nilstar.ru</IP>
  <PORT>4001</PORT>
  <TIMEOUT>10000</TIMEOUT>
  <REQMSG_TIMEOUT>2000</REQMSG_TIMEOUT>
  <BACKMENUKEY>x222</BACKMENUKEY>
</CLIENT>
```

5.5 Параметры сервисного меню <BACKMENU>

Параметры этого раздела отвечают за настройку сервисного меню.

Может иметь следующие подразделы:

- **INSPECTOR** – пароль для входа в меню инспектора: строка;
- **BANKMODULE** – пароль для входа в меню обслуживания банковского модуля: строка.

Пример:

```
<BACKMENU>
  <INSPECTOR>9999</INSPECTOR>
  <BANKMODULE>9999</BANKMODULE>
</BACKMENU>
```

5.6 Параметры модуля обслуживания банковских карт <PAYCARD>

Параметры этого раздела отвечают за настройку модуля обслуживания банковских карт.

Может иметь следующие подразделы:

- **PROTO** – протокол, на текущий момент может использоваться только одно значение SA.

Пример:

```
<PAYCARD>
```

```
  <PROTO>SA</PROTO>
</PAYCARD>
```

5.7 Параметры настроек терминала <TERMINAL>

Параметры этого раздела позволяют установить значения для переменных настройки терминала (IRAS Pax S900).

Может иметь любое количество переменных.

Структура раздела:

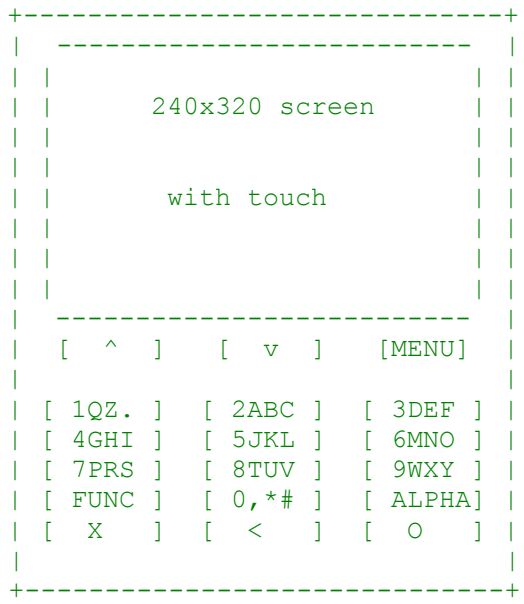
```
<TERMINAL>
      <[название] var=”[имя переменной]”>[значение]</[название]>
      …
</TERMINAL>
```

Пример:

```
<TERMINAL>
  <BACKLIGHTTIME var="persist.sys.backlighttime">0</BACKLIGHTTIME>
  <SLEEPTIME var="persist.sys.sleeptime">0</SLEEPTIME>
  <SLEEPWAITING var="persist.sys.sleepwaiting">0</SLEEPWAITING>
</TERMINAL>
```

6 Приложение

6.1 Коды и значения клавиш терминала IRAS



Клавиша	Код[6]	Маска[7]	Значение
[^]	x67	x00020000	Перемещение на предыдущий пункт меню или перемещение к предыдущему активному объекту.
[v]	x6C	x00040000	Перемещение на следующий пункт меню или перемещение к следующему активному объекту.
[MENU]	x8B	x00080000	
[1QZ.]	x31	x00000002	Ввод 1. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[2ABC]	x32	x00000004	Ввод 2. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[3DEF]	x33	x00000008	Ввод 3. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[4GHI]	x34	x00000010	Ввод 4. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[5JKL]	x35	x00000020	Ввод 5. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[6MNO]	x36	x00000040	Ввод 6. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[7PRS]	x37	x00000080	Ввод 7. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.

6 Код клавиши используется для идентификации клавиши при одиночном нажатии клавиши (смотри «Протокол клиента отображаемых форм»).

7 Маска клавиши используется для идентификации клавиши при одновременном нажатии нескольких клавиш.

[8TUV]	x38	x00000100	Ввод 8. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[9WXY]	x39	x00000200	Ввод 9. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[0,*#]	x30	x00000001	Ввод 0. В режиме ввода нецифровых значений — ввод дополнительных символов при повторном нажатии.
[FUNC]	x66	x00002000	Переключение между дробной и целой частью вводимых чисел. **Внимание:** В случае режима ввода шестнадцатеричных чисел, включает режим ввода цифры A-F (при условии нажатия затем соответственно клавиши 1-6).
[ALPHA]	x45	x00004000	
[X]	x1B	x00000400	Отмена (Cancel).
[<]	x08	x00001000	Удаление последнего введенного символа.
[O]	x0D	x00000800	Подтверждение (OK).

7 История изменений

19.01.2018:

- Добавлено описание атрибута **mode** (серверный или клиентский режим работы ККМ) в разделе «Параметры соединения <CONNECTION>» 5.1;
- Добавлено описание параметра **IP** для работы по протоколу фискального регистратора в разделе «Параметры протокола фискального регистратора <FISCAL>» 5.3;
- Добавлено описание параметров **IP, REQMSG_TIMEOUT** для работы по протоколу отображаемых форм в разделе «Параметры протокола клиента отображаемых форм <CLIENT>» 5.4.

12.07.2017:

- Добавлено описание нового способа параметров раздела **CONNECTION** в разделе «Параметры соединения <CONNECTION>» 5.1;
- Добавлено описание **GPRS** раздел «Параметры настройки оборудования для GPRS/GSM соединения (работа с операторами мобильной связи)» 5.1.2;

27.12.2016:

- Добавлено описание параметров **AUTH** и **ENCRYPT** в разделе «Параметры соединения <CONNECTION>» 5.1.

23.12.2015:

- Добавлен раздел «Параметры настроек терминала <TERMINAL>» 5.7;
- Добавлен раздел «Загрузка дополнительных параметров к приложению» 4.1.