ОКБ

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Эксплуатационная документация на «Защищенный терминал с поддержкой загрузки по сети на базе микро-компьютера МКТ-card long»

Quick Start

Руководство по быстрому старту

Москва
2019

АННОТАЦИЯ

Настоящий документ является руководством по быстрому старту защищенного терминала с поддержкой загрузки по сети на базе микрокомпьютера МКТ-card long (далее – Терминал, Защищенный терминал) и содержит описание процедур настройки Терминала, необходимых и достаточных для начала его эксплуатации.

1. Первая загрузка Терминала

При первой загрузке Защищенного терминала каждому пользователю необходимо осуществить вход в ОС, используя установленные при производстве логин и пароль. Логины и пароли пользователей, установленные при производстве, представлены в таблице 1.

Таблица 1 – Логины и пароли пользователей, установленные при производстве

Пользователь Терминала	**Логин пользователя**	**Пароль пользователя**
Администратор БИ	securityadmin	securityadmin
Администратор	admin	admin
Пользователь	user	user

После загрузки ОС необходимо запустить утилиту MKGearTool. При первом запуске утилиты появляется запрос на установку пароля. Каждому пользователю нужно установить пароль, следуя указаниям ПО.

Теперь установленный пароль пользователя может использоваться для входа в ОС, аутентификации в утилите MKGearTool и смены пароля.

2. Настройка Терминала

2.1. Настройка Терминала для работы в режиме локальной загрузки функционального ПО

После успешного прохождения Администратором БИ процедуры аутентификации в утилите MKGearTool появляется окно, изображенное на рисунке 1.

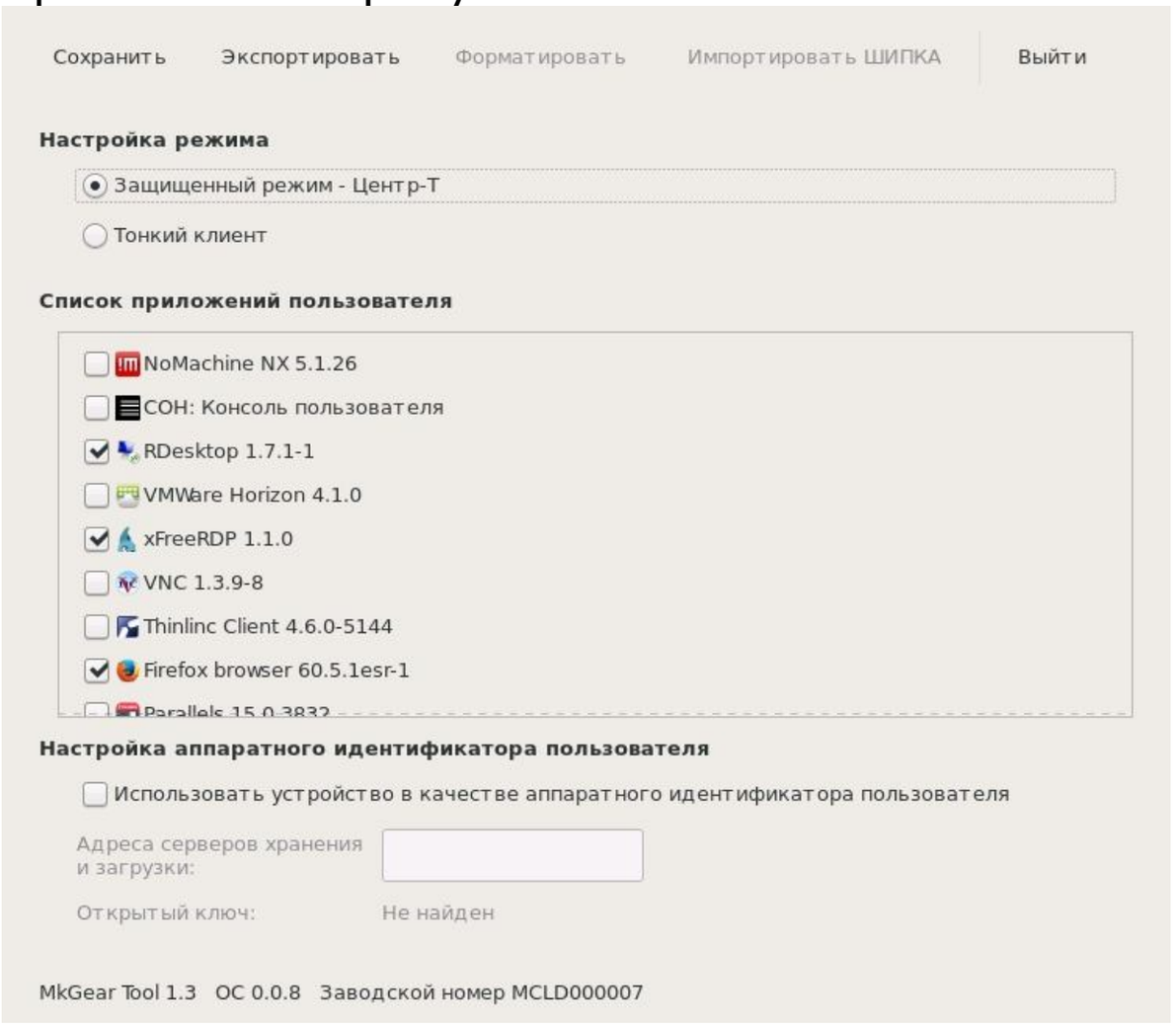

Рисунок 1 – Окно настроек Администратора БИ

Администратору БИ необходимо выбрать режим работы «Тонкий клиент» и указать разрешенные пользователю приложения для доступа к терминальному серверу.

Для сохранения настроек Администратору БИ необходимо нажать кнопку <Сохранить>. Если процедура выполнена успешно, на экране появляется соответствующее сообщение, а ярлыки доступных пользователю приложений появляются в панели инструментов, расположенной в нижней части рабочего стола.

По завершении настроек следует нажать кнопку <Выйти>.

2.2. Настройка Терминала для работы в режиме сетевой загрузки функционального ПО

До использования Терминала в режиме сетевой загрузки должны быть произведены процедуры, указанные в документах:

– «ПАК СЗИ НСД «Центр-Т». Руководство администратора АРМ «Центр» (11443195.4012.042 90):

– предварительная инициализация всех персональных идентификаторов ШИПКА;

– выработка ключевой пары на АРМ «Центр»;

– установка кодов аутентификации для контроля целостности и подлинности образов ПО ТС;

– инициализация СХСЗ;

– формирование начального набора образов на СХСЗ;

– «ПАК СЗИ НСД «Центр-Т». Руководство администратора СХСЗ» (11443195.4012.042 91):

– создание пользователей «Администратор» и «Администратор БИ»;

– настройка сетевых параметров СХСЗ;

– импорт образов ПО ТС на СХСЗ;

– создание учетных записей пользователей;

– сопоставление пользователям Клиентских устройств;

– сопоставление пользователям образов ПО ТС (пользователям защищенных терминалов соответствует образ MKTrust01);

– управление сетевыми настройками СХСЗ и Клиента.

ВНИМАНИЕ! В рамках технологии «Центр-Т» для Терминала выполнение процедур создания шаблона образа ПО ТС, платформы ТС, сбора образа ПО ТС из шаблона не требуется. Образ ПО ТС для Терминала уже собран и добавлен в ПО АРМ «Центр» при производстве.

После успешного прохождения Администратором БИ процедуры аутентификации в утилите MKGearTool появляется окно, изображенное на рисунке 1. Администратору БИ необходимо выбрать режим работы «защищенный режим «Центр-Т» и нажать кнопку <Сохранить>.

По завершении настроек следует нажать кнопку <Выйти>.

После успешного прохождения Администратором процедуры аутентификации в утилите MKGearTool появляется окно, изображенное на рисунке 2.

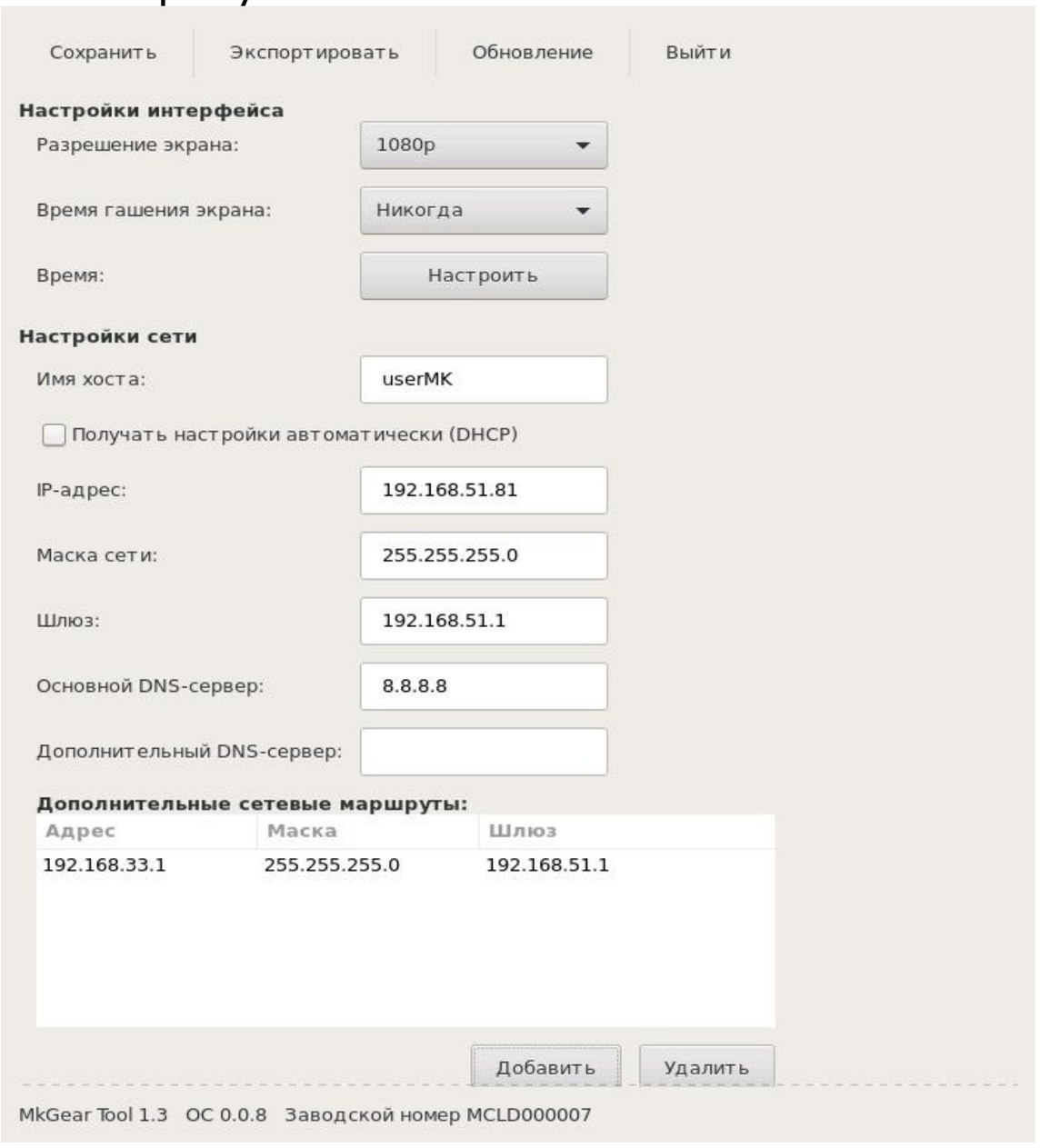

Рисунок 2 – Окно настроек Администратора

Для настройки даты и времени необходимо нажать кнопку <Настроить> в строке «Время». При этом появляется окно, которое показано на рисунке 3.

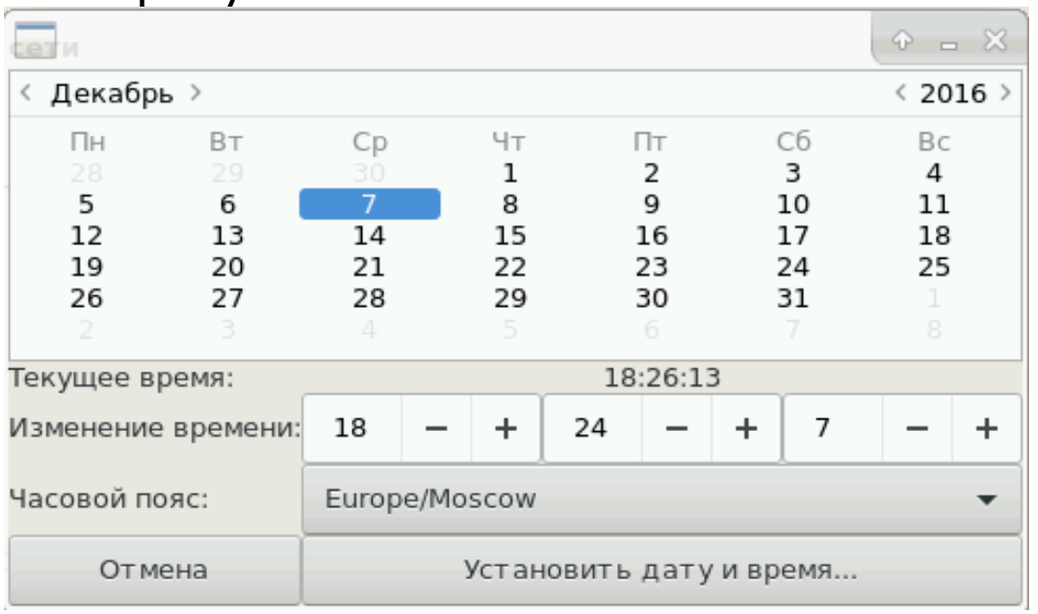

Рисунок 3 – Окно настройки даты и времени

Администратору нужно указать текущую дату, время и часовой пояс, после чего нажать кнопку <Установить дату и время…>.

После редактирования всех необходимых настроек интерфейса и сетевых настроек для их сохранения Администратору следует нажать кнопку <Сохранить>.

Если процедура выполнена успешно, на экране появляется соответствующее сообщение.

Настройки, выполненные Администратором, можно сохранить на внешнее устройство. Для этого следует нажать кнопку <Экспортировать>. При этом на экране появляется окно

экспорта настроек в файл, в котором нужно указать место сохранения файла настроек и его имя. После успешного завершения процедуры появляется сообщение: «Настройки успешно записаны на устройство».

По завершении настроек Администратору следует нажать кнопку <Выйти>.

2.3. Настройка Терминала в качестве аппаратного идентификатора пользователя

В любом режиме работы Защищенный терминал может использоваться в качестве аппаратного идентификатора пользователя на терминальном сервере. Для установки Терминала в качестве аппаратного идентификатора следует в окне, изображенном на рисунке 1, установить флаг «Использовать устройство в качестве аппаратного идентификатора пользователя». После установки флага становится доступной функция импорта настроек клиентской ШИПКИ из состава ПАК «Центр-Т», а внизу окна появляется серийный номер идентификатора Терминала.

Идентификатор Терминала имеет свой PIN-код для авторизации пользователя. Менять PIN-код может только пользователь Защищенного терминала. Если пользователь забыл PIN-код, Администратору БИ следует выполнить форматирование идентификатора.

В процессе инициализации клиентского устройства в его память копируются, в том числе, адрес (адреса) СХСЗ и

открытый ключ, необходимый для проверки целостности образа ПО ТС после его получения по сети. Эти данные необходимо хранить также на Защищенном терминале для возможности его применения в режиме сетевой загрузки. Для этого Администратору БИ следует подключить устройство, назначенное ему как пользователю ПАК «Центр-Т», и нажать кнопку <Импортировать ШИПКА>.

При этом на экране последовательно появляются сначала окно для ввода PIN-кода идентификатора с поддержкой загрузки по сети на базе микрокомпьютера МКТ-card long, а затем – окно для ввода PIN-кода подключенного клиентского устройства. В результате успешного завершения процедуры появляется соответствующее сообщение, а в окне настроек Администратора БИ отображаются импортированные настройки (рисунок 4).

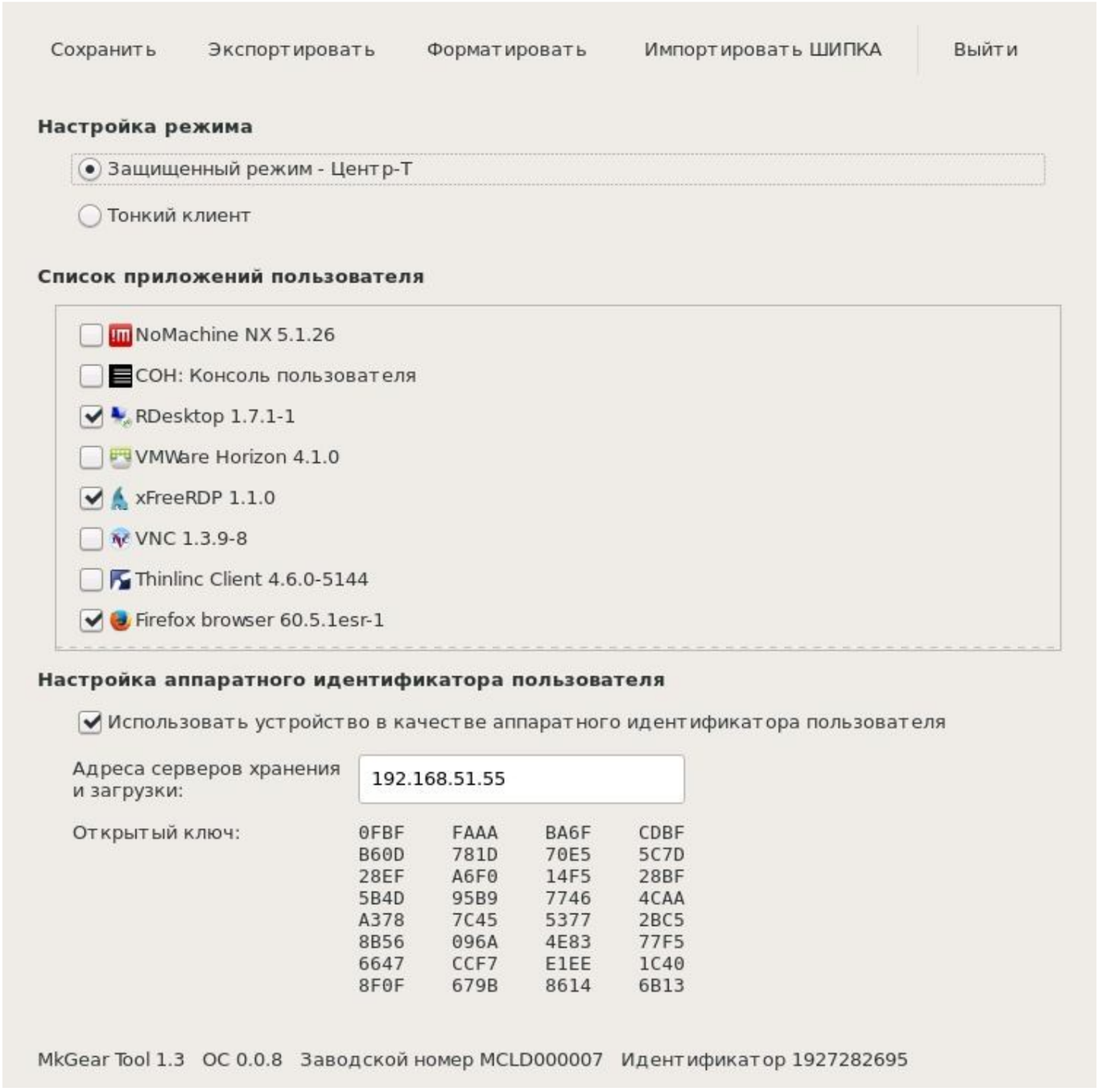

Рисунок 4 – Окно настроек Администратора БИ после выполнения процедуры импорта

Если Администратор Терминала установил для пользователя возможность использования Защищенного терминала в качестве аппаратного идентификатора на терминальном сервере, то до первого его использования пользователю необходимо сменить PIN-код, установленный по умолчанию. По умолчанию установлен PIN-код OKBSAPR_.

Рисунок 5 – Окно настроек пользователя

Для смены PIN-кода следует авторизоваться в утилите MKGearTool от имени пользователя и в окне, показанном на рисунке 5, нажать кнопку <Сменить PIN-код>.

3. Использование Терминала

3.1. Использование Терминала в режиме локальной загрузки функционального ПО

После включения Защищенного терминала начинается загрузка ОС из защищенного от записи раздела памяти микрокомпьютера МКТ-card long.

После загрузки ОС Пользователь может получить доступ к терминальному серверу, используя различные установленные приложения.

Порядок работы с клиентским ПО для доступа к терминальному серверу зависит от вида используемого клиентского ПО и описан в документации на программное решение по доставке приложений на удаленную рабочую станцию.

3.2. Использование Терминала в режиме сетевой загрузки функционального ПО

Если Администратором БИ установлен режим сетевой загрузки ФПО, клиентское устройство ШИПКА Пользователя должно быть подключено до включения Терминала.

После включения Защищенного терминала начинается загрузка ОС из защищенного от записи раздела памяти микрокомпьютера МКТ-card long.

После загрузки ОС запускается ПО Клиента «Центр-Т», на экране отображается окно аутентификации пользователя (рисунок 6).

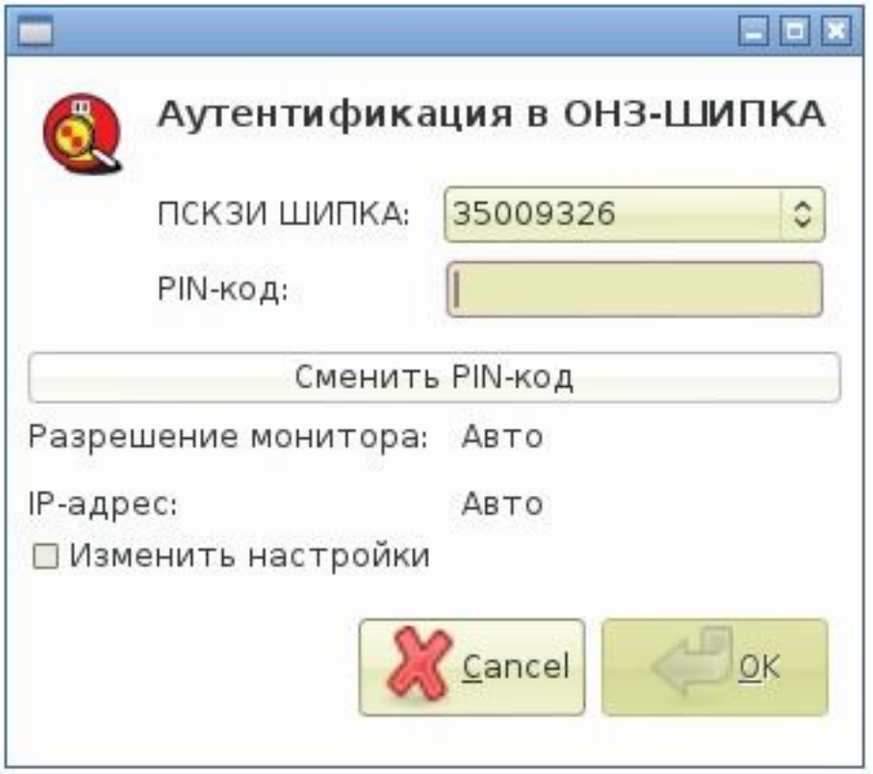

Рисунок 6 – Окно аутентификации пользователя

При первом запуске Терминала в режиме сетевой загрузки ФПО пользователю необходимо установить адрес Citrix-брокера. Для этого нужно установить флаг «Изменить настройки» (рисунок 6).

В поле «ПСКЗИ ШИПКА» следует выбрать серийный номер подключенного клиентского устройства ШИПКА, в поле «PIN - код» ввести соответствующий PIN–код и нажать кнопку <ОК> для подтверждения операции или кнопку <Cancel> для ее отмены.

По нажатии кнопки <ОК> на экране появляется окно дополнительных настроек.

Пользователю нужно ввести адрес Citrix-брокера в строке «Адрес терминального сервера» в виде http://ip_server, где ip_server – адрес Citrix-брокера, и нажать кнопку <Применить>.

По нажатии кнопки <Применить> адрес Citrix-брокера автоматически сохраняется.

Затем посылается запрос СХСЗ на получение образа с ПО терминальной станции (ТС). Сервер обрабатывает запрос и передает Терминалу нужный образ ПО ТС.

В случае успешного завершения проверки образа ПО ТС производится его загрузка в оперативную память МКТ-card long и ему передается дальнейшее управление ресурсами микрокомпьютера.

ПО, запущенное из полученного образа, инициирует соединение с Citrix-брокером с помощью браузера.