ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство по эксплуатации

37222406.26.20.14.070 РЭ

Листов 41

Москва

2019

АННОТАЦИЯ

Настоящий документ является руководством по эксплуатации защищенного терминала с поддержкой загрузки по сети на базе микрокомпьютера «МКТ-card long» (далее – Терминал, Защищенный терминал) и содержит сведения о характеристиках Терминала и указания, необходимые для его правильной и безопасной эксплуатации.

Перед эксплуатацией продукта рекомендуется внимательно ознакомиться с настоящим Руководством.

Использование защитных мер Терминала должно дополняться общими мерами предосторожности и физической безопасности.

СОДЕРЖАНИЕ

1 Общие сведения 5
1.1 Назначение и область применения 5
1.2 Технические условия применения 6
1.3 Организационные меры 6
1.4 Роли пользователей 7
2 Предварительная настройка 8
3 Содержание работы Администратора БИ 10
3.1 Установка пароля 10
3.2 Установка режима работы Терминала 11
3.3 Настройка Терминала в качестве аппаратного идентификатора пользователя 13
3.3.1 Настройка возможности использования Терминала в качестве аппаратного идентификатора пользователя 13
3.3.2 Импорт настроек клиентского устройства из состава ПАК «Центр-Т» 14
3.3.3 Форматирование Терминала в качестве аппаратного идентификатора 16
3.4 Смена пароля 17
4 Содержание работы Администратора 18
4.1 Установка пароля 18
4.2 Редактирование настроек интерфейса и сетевых настроек 18
4.3 Смена пароля 22
5 Содержание работы Пользователя 23
5.1 Установка пароля 23
5.2 Смена PIN-кода Терминала в качестве аппаратного идентификатора 23
5.3 Использование Терминала в режиме сетевой загрузки функционального ПО 24
5.3.1 Начало работы 24

5.3.2 Работа Пользователя в соответствии с функциональными обязанностями 27
5.4 Использование Терминала в режиме локальной загрузки функционального ПО 28
5.4.1 Начало работы 28
5.4.2 Работа Пользователя в соответствии с функциональными обязанностями 29
5.4.3 Сброс настроек функционального ПО 29
5.5 Смена пароля 30
6 Завершение работы и выход из системы 31
7 Обновление Терминала 32
8 Перечень принятых сокращений и обозначений 35
Приложение А. Инструкция по настройке Citrix для работы с Терминалом (образ версии 0.0.6) 36
Приложение Б. Методы устранения неполадок в работе терминала на базе МКТ-card long в режиме сетевой загрузки 38

1 Общие сведения

1.1 Назначение и область применения

Операционная система (ОС) МКТ-card long размещена в памяти с правами доступа read only (RO), что исключает возможность её несанкционированного изменения. На этапе производства в память микрокомпьютера может быть установлено любое программное обеспечение (ПО).

МКТ-card long с предустановленным функциональным ПО (ФПО), обеспечивающим доступ к терминальному серверу, называется терминалом на базе МКТ-card long.

Терминал предоставляет возможность работы в одном из двух режимов, определяющих способ загрузки ФПО:

- защищенный режим «Центр-Т» (сетевая загрузка ФПО);
- тонкий клиент (локальная загрузка ФПО).

При работе в первом режиме используется технология защищенного хранения и сетевой загрузки «Центр-Т». ФПО (в рамках концепции «Центр-Т» называется «образ ПО терминальной станции» (ТС)) загружается по сети с компонента программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Центр-Т» (далее – ПАК «Центр-Т») – Сервера хранения и сетевой загрузки (СХСЗ).

Во втором режиме пользователь может получить доступ к терминальному серверу, используя различные установленные приложения.

При использовании Терминала в обоих режимах работы обеспечиваются следующие возможности:

- идентификация и аутентификация пользователя на сервере;
- целостность ПО и его защита от несанкционированной модификации;
- поддержка применения в рамках терминальной сессии защищенных USB-носителей «Секрет Особого Назначения».

1.2 Технические условия применения

Для применения Защищенного терминала необходим следующий минимальный набор технических и программных средств:

- терминальный сервер с установленной ОС Microsoft Windows Server 2003 и выше; дополнительно на терминальном сервере рекомендуется использовать ПАК СЗИ НСД «Аккорд-Win32»/ «Аккорд-Win64»;
- для использования Терминала в режиме локальной загрузки ФПО: установленное на терминальном сервере программное решение по доставке приложений на удаленную рабочую станцию;
- для использования Терминала в режиме сетевой загрузки ФПО:
  - установленное на терминальном сервере ПО Citrix XenApp;
  - развернутый СХСЗ;
  - развернутый АРМ «Центр»;
  - клиентские устройства на базе ШИПКА-2.0 со встроенным ПО версии 50.13 и выше.

Следует отметить, что ПО МКТ-card long для Банка России не предусматривает возможности работы с беспроводной связью.

1.3 Организационные меры

Для эффективного применения Защищенного терминала и поддержания необходимого уровня защищенности информационных ресурсов необходимы:

- физическая охрана Терминала, в том числе проведение мероприятий по обеспечению целостности его корпуса;
- хранение в тайне паролей пользователей, выполняющих поддерживаемые роли;
- хранение в тайне PIN-кода идентификатора МКТ-card long;
- принять меры по исключению извлечения MicroSD из МКТ-card long (например, посредством проведения процедуры опечатывания).

1.4 Роли пользователей

Терминал поддерживает следующие роли:

- Администратор безопасности информации (БИ);
- Администратор;
- Пользователь.

2 Предварительная настройка

До использования Защищенного 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 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 образов ПО ТС (пользователям защищенных терминалов соответствует образ MKTrust01);
- управление сетевыми настройками СХСЗ.

ВНИМАНИЕ! В рамках технологии «Центр-Т» для защищенных терминалов выполнение процедур создания шаблона образа ПО ТС, платформы ТС, сборки образа ПО ТС из шаблона не требуется. Готовые образы для них добавляются в ПО АРМ «Центр» при производстве или передаются с обновлением. Для пользователей защищенных терминалов с возможностью использования в качестве аппаратного идентификатора нужно назначать образ MKTrust03, для пользователей всех остальных защищенных терминалов требуется назначать образ MKTrust01).

Вне зависимости от режима работы Терминала, который планируется использовать, до начала работы с ним рекомендуется выполнить настройки Citrix, обеспечивающие корректное отображение окон с опубликованными приложениями и описанные в приложении А.

3 Содержание работы Администратора БИ

3.1 Установка пароля

При первой загрузке Защищенного терминала Администратор БИ должен использовать логин и пароль, установленные для него по умолчанию (таблица 1).

Таблица 1 – Установленные по умолчанию параметры Администратора БИ для входа в систему

Логин	**Пароль**
securityadmin	securityadmin

После загрузки ОС Администратору БИ следует установить собственный пароль. Для этого необходимо запустить утилиту MKGearTool, щелкнув левой кнопкой мыши по ярлыку MKGearTool в панели инструментов, расположенной в нижней части рабочего стола.

В появившемся окне нужно выбрать пользователя Security Admin из выпадающего списка в строке «Пользователь» (рисунок 1), после чего появляется запрос на установку пароля.

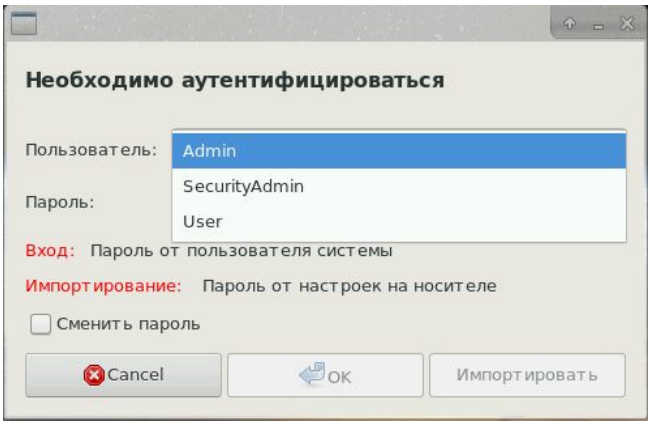

Рисунок 1 – Окно аутентификации пользователя

Администратору БИ необходимо установить пароль, следуя указаниям ПО. В дальнейшем выполнение процедуры установки пароля для Администратора БИ не запрашивается.

Пароль Администратора БИ необходим для входа в ОС, установки режима работы Защищенного терминала и смены пароля.

3.2 Установка режима работы Терминала

Установка режима работы Защищенного терминала выполняется Администратором БИ после успешного прохождения процедуры аутентификации в утилите MKGearTool. Администратору БИ доступны следующие настройки (рисунок 2):

- настройка режима – позволяет установить доступный пользователю режим работы:
  - защищенный режим «Центр-Т»;
  - тонкий клиент;
- список приложений пользователя – позволяет указать разрешенные пользователю приложения для доступа к терминальному серверу при его работе в режиме «тонкий клиент»:
  - NoMachine NX;
  - COH: Консоль пользователя;
  - RDesktop;
  - VMware Horizon;
  - xFreeRDP;
  - VNC;
  - Thinlinc Client;
  - Firefox browser
  - Parallels;
  - Citrix Receiver;
  - Virt-Manager;
  - SPICE Client.

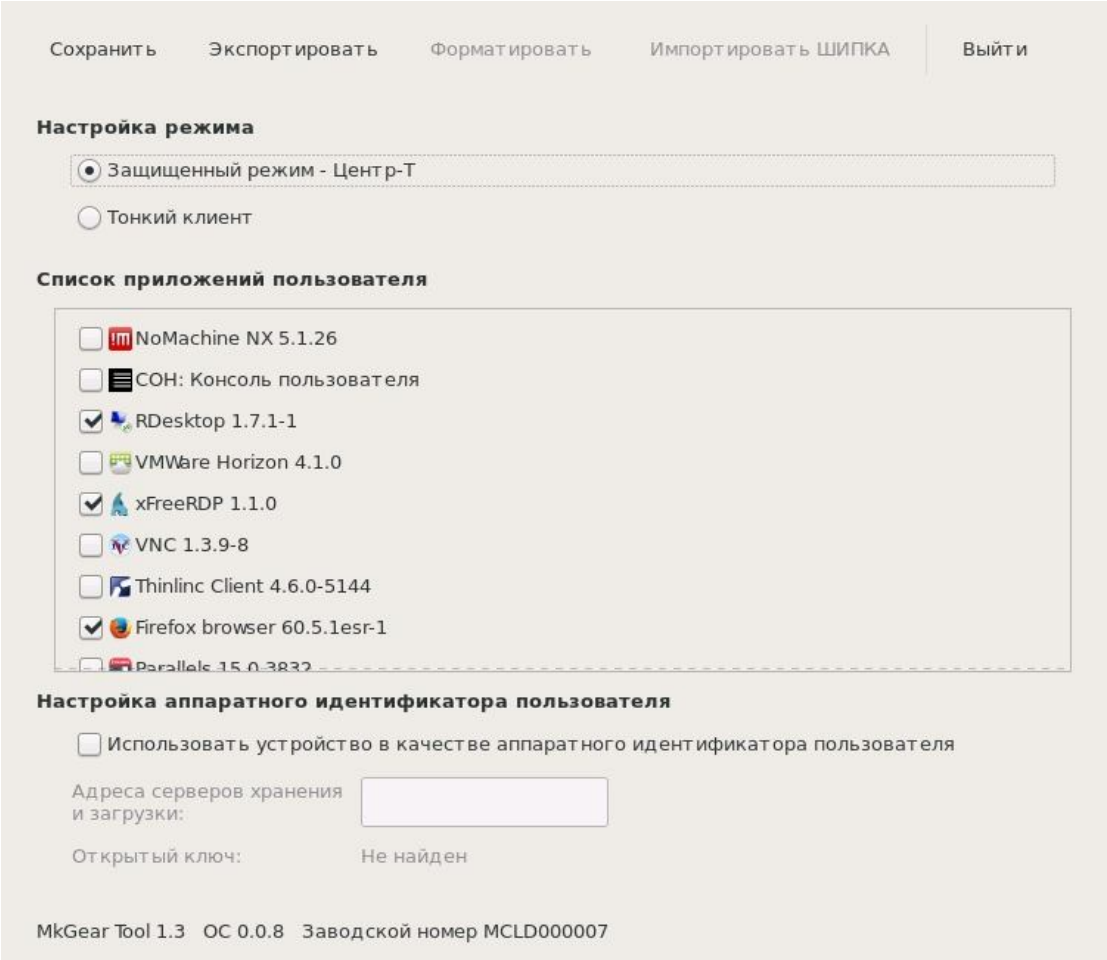

Рисунок 2 – Окно настроек Администратора БИ

После установки режима работы Защищенного терминала и выбора доступных пользователю приложений следует 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.

Настройки, выполненные Администратором БИ, 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 БИ следует нажать кнопку <Выйти>.

3.3 Настройка Терминала в качестве аппаратного идентификатора пользователя

3.3.1 Настройка возможности использования Терминала в качестве аппаратного идентификатора пользователя

ВНИМАНИЕ! Возможность использования Терминала в качестве аппаратного идентификатора пользователя доступна не для всех его конфигураций. Для использования данной возможности необходимо убедиться, что версия системного ПО (указана в Техническом паспорте) содержит в выделенном элементе номер 002 или выше: CR1-**002**-X-R.

Защищенный терминал может использоваться в качестве аппаратного идентификатора пользователя на терминальном сервере в любом режиме работы. Для установки Терминала в качестве аппаратного идентификатора следует в окне, изображенном на рисунке 2, 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 (рисунок 3).

Терминал в качестве аппаратного идентификатора 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.

Примечание.

В случае необходимости использования Терминала в качестве аппаратного идентификатора в ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд-Win64» регистрация идентификатора производится в следующем порядке:

1. Подключить клиентское устройство (для ПАК «Центр-Т») / идентификатор администратора безопасности ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд-Win64» (в зависимости от выбранного режима работы).

2. Подключиться к серверу, на котором необходимо зарегистрировать Терминал в качестве аппаратного идентификатора (по протоколу RDP/ICA).

3. Запустить программу «Aced32» из состава ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд-Win64» и пройти процедуру аутентификации.

4. Отключить от Терминала идентификатор администратора безопасности ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд-Win64».

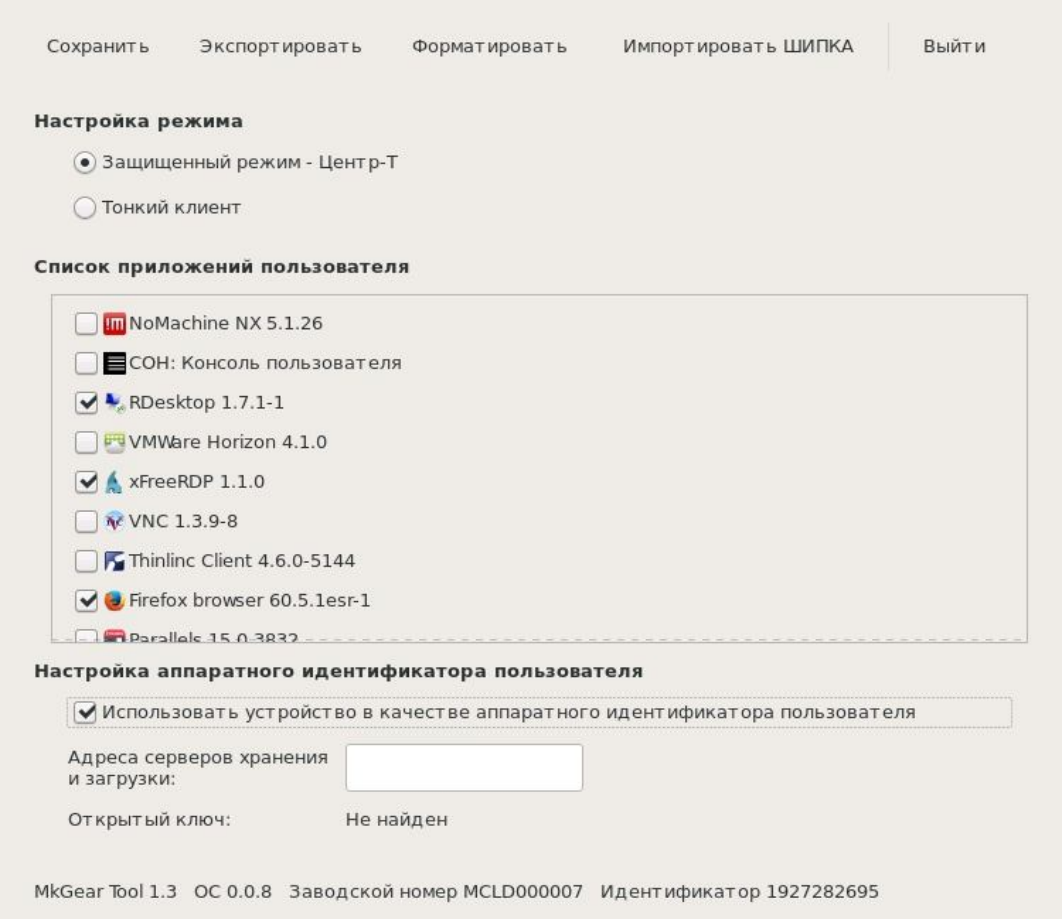

Рисунок 3 – Окно настройки возможности использования устройства в качестве аппаратного идентификатора

5. Выполнить назначение пользователю идентификатора (если выполняется первый раз, то с генерацией ключа).

3.3.2 Импорт настроек клиентского устройства из состава ПАК «Центр-Т»

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 в окне, изображенном на рисунке 3, нажать кнопку <Импортировать ШИПКА>. При этом на экране последовательно появляются сначала окно для ввода PIN-кода идентификатора Терминала, а затем – окно для ввода PIN-кода подключенного клиентского устройства. В результате успешного завершения процедуры появляется соответствующее сообщение (рисунок 4), а в окне настроек Администратора БИ отображаются импортированные настройки (рисунок 5).

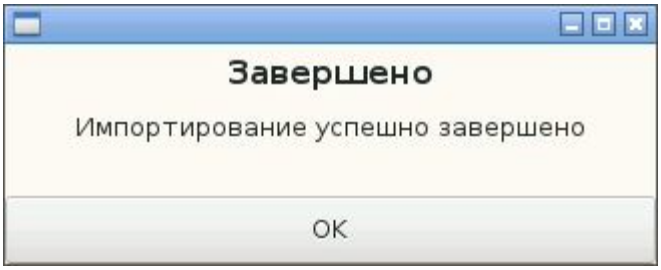

Рисунок 4 – Сообщение об успешном завершении процедуры импорта настроек

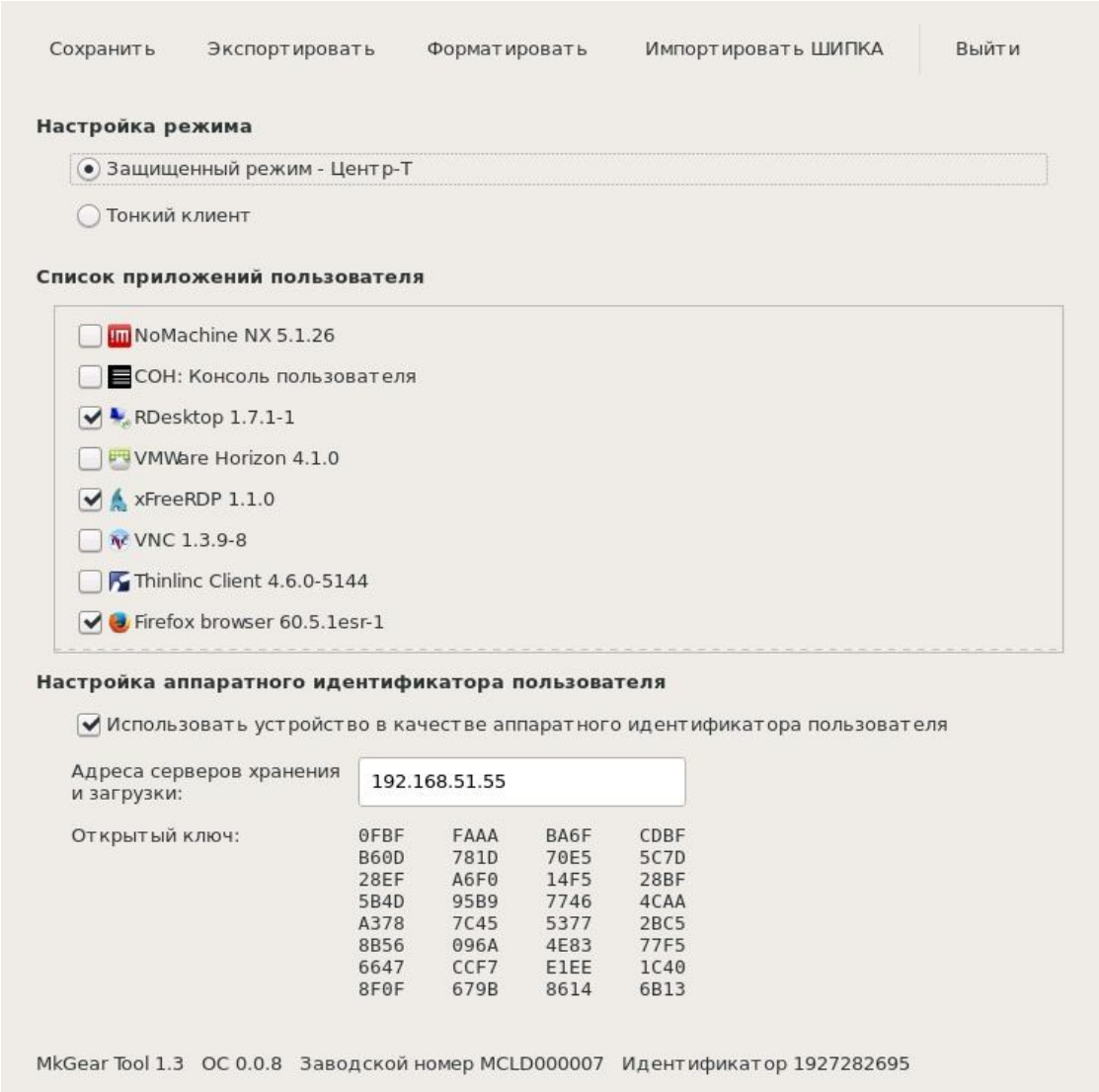

Рисунок 5 – Окно настроек Администратора БИ после выполнения процедуры импорта

3.3.3 Форматирование Терминала в качестве аппаратного идентификатора

Терминал в качестве аппаратного идентификатора имеет свой PIN-код для авторизации пользователя. Менять PIN-код может только Пользователь Защищенного терминала. Если он забыл PIN-код, Администратору БИ следует выполнить форматирование идентификатора. При форматировании PIN-код сбрасывается в значение по умолчанию, и стираются импортированные с ШИПКИ данные.

Для выполнения процедуры Администратору БИ следует нажать кнопку <Форматировать> в окне, изображенном на рисунке 3.

В результате успешного выполнения процедуры появляется сообщение, отображенное на рисунке 6.

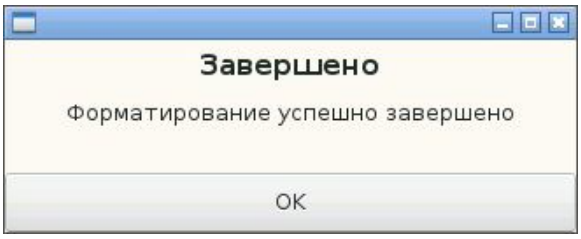

Рисунок 6 – Сообщение об успешном завершении процедуры форматирования идентификатора

3.4 Смена пароля

Для смены пароля Администратору БИ нужно запустить утилиту MKGearTool, в окне аутентификации (рисунок 1) установить флаг «Сменить пароль» и нажать кнопку <ОК>.

При этом на экране появляется окно смены пароля, в котором следует выбрать пользователя утилиты Security Admin, ввести старый пароль и новый пароль с подтверждением.

Для продолжения процедуры следует нажать кнопку <ОК>, для отмены – кнопку <Закрыть>.

Если процедура выполнена успешно, на экране появляется сообщение об успешной смене пароля.

4 Содержание работы Администратора

4.1 Установка пароля

При первой загрузке защищенного терминала Администратор должен использовать логин и пароль, установленные для него по умолчанию (таблица 2).

Таблица 2 – Установленные по умолчанию параметры Администратора для входа в систему

Логин	**Пароль**
admin	admin

После загрузки ОС Администратору следует сменить пароль. Для этого необходимо запустить утилиту MKGearTool, щелкнув левой кнопкой мыши по ярлыку MKGearTool в панели инструментов, расположенной в нижней части рабочего стола.

В появившемся окне нужно выбрать пользователя Admin из выпадающего списка в строке «Пользователь» (рисунок 1), после чего появляется запрос на установку пароля. Администратору необходимо установить пароль, следуя указаниям ПО. В дальнейшем выполнение процедуры установки пароля для Администратора не запрашивается.

Пароль Администратора необходим для входа в ОС, редактирования настроек интерфейса и сетевых настроек и смены пароля.

4.2 Редактирование настроек интерфейса и сетевых настроек

Редактирование настроек интерфейса и сетевых настроек выполняется Администратором после успешного прохождения процедуры аутентификации. Администратору доступны следующие настройки (рисунок 7):

- *группа настроек «Настройки интерфейса»:*

– разрешение экрана – позволяет изменить разрешение экрана на подходящее для используемого монитора;

– время гашения экрана – позволяет задать временной интервал, по истечении которого выполняется переход в режим гашения экрана;

– время – позволяет установить текущие дату, время и часовой пояс;

– *группа настроек «Настройки сети»:*

– имя хоста – позволяет установить имя Защищенного терминала (в рамках ICA-сессии имя Защищенного терминала отображается с приставкой «-c», то есть в виде «имя_хоста-c»);

– получать настройки автоматически (DHCP) – позволяет включить/выключить функцию автоматического получения сетевых настроек от DHCP-сервера;

– IP-адрес – позволяет задать IP-адрес клиента;

– маска сети – позволяет задать маску сети, в которой находится клиент;

– шлюз – позволяет задать шлюз подсети клиента;

– основной DNS-сервер – позволяет задать основной DNS-сервер сети клиента;

– дополнительный DNS-сервер – позволяет задать дополнительный DNS-сервер сети клиента;

– *«Дополнительные сетевые маршруты»* – позволяет задать дополнительные маршруты сети клиента;

– *«Работоспособность сети»* – позволяет проверить доступность сетевого ресурса.

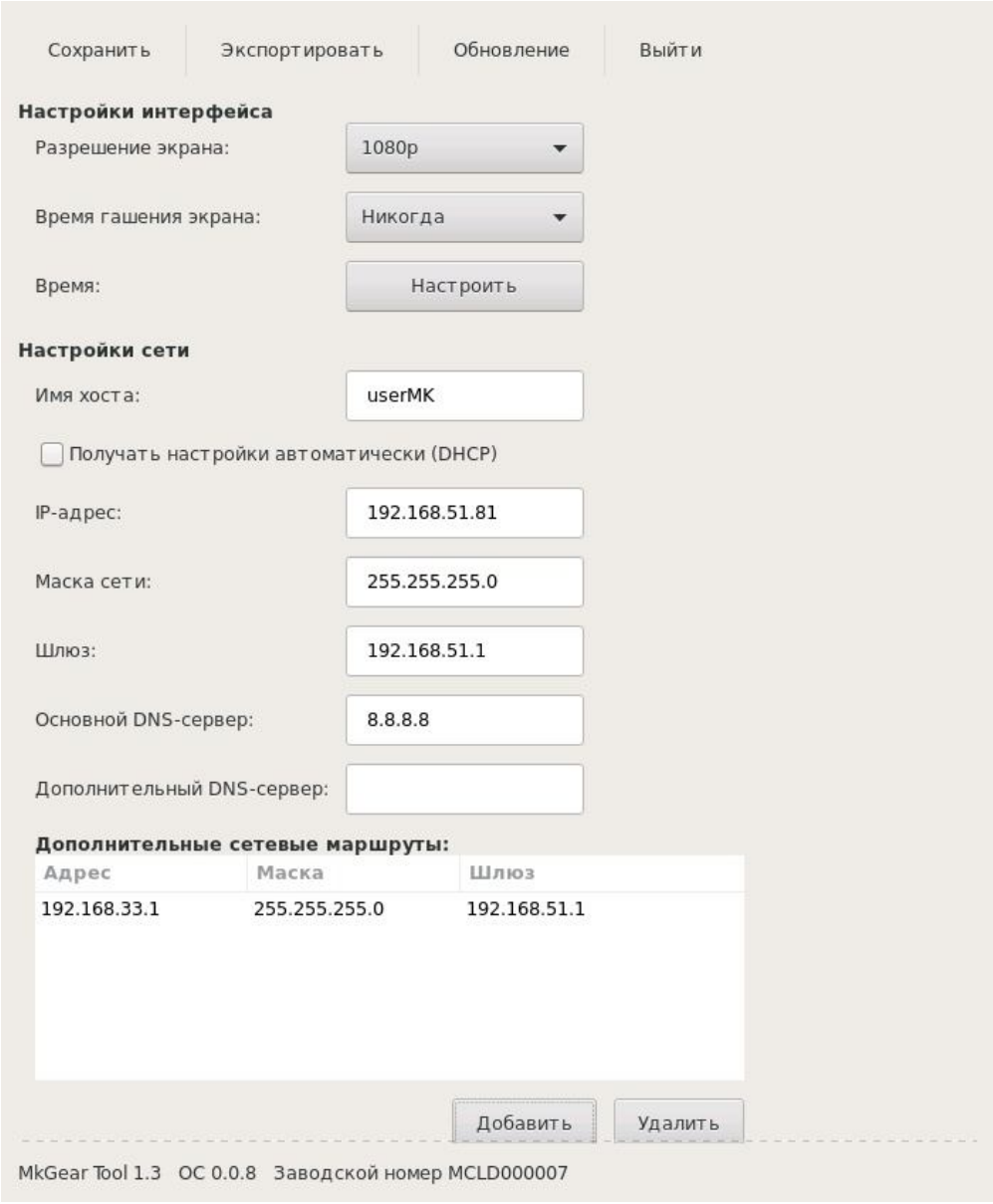

Рисунок 7 – Окно настроек, доступных Администратору

Для настройки даты и времени необходимо нажать кнопку <Настроить> в строке «Время». При этом появляется окно, которое показано на рисунке 8.

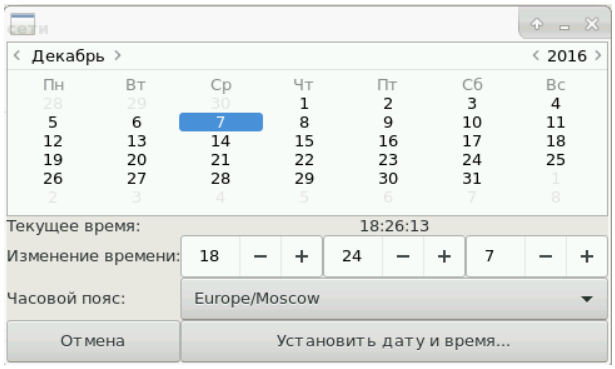

Рисунок 8 – Окно настройки даты и времени

Администратору нужно указать текущую дату, время и часовой пояс, после чего нажать кнопку <Установить дату и время…> для сохранения настроек или кнопку <Отмена> для отмены операции.

Для добавления нового сетевого маршрута необходимо нажать кнопку <Добавить>. При этом на экран выводится окно, в котором необходимо ввести параметры сетевого маршрута: адрес, маску и шлюз.

После указания необходимых параметров сетевого маршрута следует нажать кнопку <Добавить> в этом окне. В случае ввода корректных параметров операция завершается успешно, а добавленный маршрут появляется в списке.

Для проверки работоспособности сети необходимо указать сетевой ресурс в предназначенной для этого строке и выбрать способ определения доступности сети (ping или traceroute).

После указания необходимых данных следует нажать кнопку <Старт>. Процесс проверки отображается ниже в этом же окне.

Для сохранения настроек Администратору необходимо 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>.

ВНИМАНИЕ! Выполненные Администратором настройки распространяются на оба режима работы.

4.3 Смена пароля

Для смены пароля Администратору нужно запустить утилиту MKGearTool, в окне аутентификации (рисунок 1) установить флаг «Сменить пароль» и нажать кнопку <ОК>.

При этом на экране появляется окно смены пароля, в котором следует выбрать пользователя утилиты Admin, ввести старый пароль и новый пароль с подтверждением. Для продолжения процедуры следует нажать кнопку <ОК>, для отмены – кнопку <Закрыть>.

Если процедура выполнена успешно, на экране появляется сообщение об успешной смене пароля.

5 Содержание работы Пользователя

5.1 Установка пароля

При первой загрузке Защищенного терминала Пользователь должен использовать логин и пароль, установленные для него по умолчанию (таблица 3).

Таблица 3 – Установленные по умолчанию параметры Пользователя для входа в систему

Логин	**Пароль**
user	user

После загрузки ОС Пользователю следует сменить пароль. Для этого необходимо запустить утилиту MKGearTool, щелкнув левой кнопкой мыши по ярлыку MKGearTool в панели инструментов, расположенной в нижней части рабочего стола.

В появившемся окне нужно выбрать пользователя User из выпадающего списка в строке «Пользователь» (рисунок 1), после чего появляется запрос на установку пароля. Пользователю необходимо установить пароль, следуя указаниям ПО. В дальнейшем выполнение процедуры установки пароля для Пользователя не запрашивается.

Пароль Пользователя необходим для входа в ОС, сброса параметров ФПО в режиме локальной загрузки ОС и смены пароля.

5.2 Смена PIN-кода Терминала в качестве аппаратного идентификатора

Если Администратор БИ 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_).

Для смены PIN-кода следует авторизоваться в утилите MKGearTool от имени Пользователя и в окне, показанном на рисунке 9, нажать кнопку <Сменить PIN-код>.

Рисунок 9 – Окно настроек, доступных Пользователю

5.3 Использование Терминала в режиме сетевой загрузки функционального ПО

5.3.1 Начало работы

ВНИМАНИЕ! В рамках технологии «Центр-Т» доступ к терминальному серверу с Защищенного терминала возможен только по протоколу ICA (WEB интерфейс).

Если в качестве аппаратного идентификатора Пользователя на терминальном сервере используется Защищенный терминал, в процессе получения доступа к серверу на Терминале не должны быть подключены

устройства, которые могут выполнять функции аппаратных идентификаторов (например, ШИПКИ).

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 10).

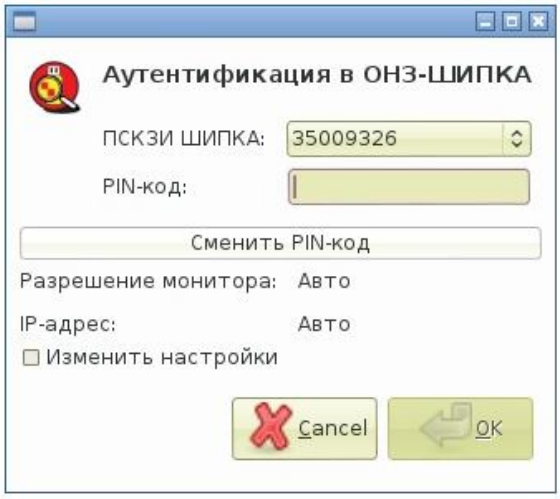

Рисунок 10 – Окно аутентификации Пользователя

Если в поле «Разрешение монитора» указано значение «Авто», то в образе ПО ТС используются параметры, установленные на этапе сборки ПО ТС (рисунок 10).

Если при настройке Защищенного терминала Администратор установил автоматическое получение настроек по DHCP, то в поле «IP-адрес» стоит значение «Авто» (рисунок 10).

При первом запуске Терминала в режиме сетевой загрузки ФПО Пользователю необходимо установить адрес Citrix-брокера[1]. Для этого нужно установить флаг «Изменить настройки» (рисунок 10).

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

[1] Сервер, на котором функционирует Citrix Broker Service и который стоит перед фермой терминальных серверов.

По нажатию кнопки <ОК> на экране появляется окно дополнительных настроек со следующими параметрами:

Группа «Сетевые настройки»:

– «Адрес терминального сервера» – задает адрес Citrix-брокера. Адрес указывается в виде http://server, где server – ip-адрес или доменное имя Citrix-брокера (поле доступно для изменения Пользователем);

– «Получать настройки автоматически (DHCP)» – отображает способ получения сетевых настроек от DHCP-сервера;

– «IP-адрес» – отображает ip-адрес клиента;

– «Маска сети» – отображает маску сети, в которой находится клиент;

– «Шлюз» – отображает шлюз подсети клиента;

– «Основной DNS-сервер» – отображает основной DNS-сервер сети клиента;

– «Дополнительный DNS-сервер» – отображает дополнительный DNS-сервер сети клиента.

Параметры группы «Настройки монитора» отображают разрешение экрана монитора.

После указания адреса терминального сервера нужно нажать кнопку <Применить>, для отмены операции – кнопку <Отмена>.

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

В дальнейшем при необходимости адрес Citrix-брокера может быть изменен аналогичным способом.

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

При возникновении ошибки в процессе получения образа ПО ТС в появившемся на экране окне (рисунок 11) следует нажать кнопку <Назад> и повторить процедуру аутентификации.

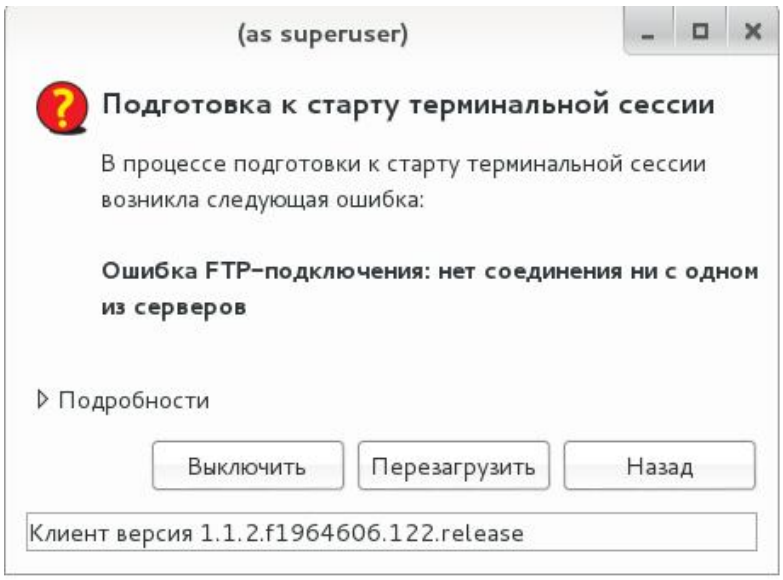

Рисунок 11 – Ошибка при получении образа ПО ТС

В этом случае повторно посылается запрос СХСЗ на получение образа с ПО ТС.

Если процедура корректно завершена, Терминал получает образ по сети.

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.

Выводимые на экран монитора сообщения о неполадках, причины их возникновения и рекомендуемый порядок действий пользователей по их устранению указаны в приложении Б.

5.3.2 Работа Пользователя в соответствии с функциональными обязанностями

Пользователю Терминала предоставляется возможность работы в рамках терминальной сессии, организованной средствами загруженного образа ПО ТС с заданными параметрами.

ВНИМАНИЕ! Для переключения между окнами в терминальной сессии необходимо сначала произвести захват окна терминального подключения,

нажав «Ctrl+Shift», и только затем осуществить переключение между окнами, используя сочетание клавиш «Alt+Tab».

Также в рамках терминальной сессии Пользователю может быть предоставлена возможность использования USB-носителей «Секрет Особого Назначения», подключенных непосредственно к Терминалу.

Если Администратор БИ установил в качестве аппаратного идентификатора Пользователя Защищенный терминал, то при доступе к терминальному серверу запрашивается его PIN-код.

ВНИМАНИЕ! Если в качестве аппаратного идентификатора Пользователя используется Защищенный терминал, к нему в процессе получения доступа к серверу не должны быть подключены устройства, которые могут выполнять функции аппаратных идентификаторов (например, ШИПКИ).

5.4 Использование Терминала в режиме локальной загрузки функционального ПО

5.4.1 Начало работы

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

В рамках режима локальной загрузки ФПО Пользователь может получить удаленный доступ к терминальному серверу с помощью встроенных средств:

- SPICE Client;
- RDesktop;
- VMware Horizon;
- xFreeRDP;
- VNC;
- Thinlinc Client;
- Firefox browser;

- Parallels;
- NoMachine NX;
- Citrix Receiver;
- Virt-Manager.

Настройка клиентского ПО для доступа к терминальному серверу выполняется Пользователем Защищенного терминала в соответствии с документацией на программное решение по доставке приложений на удаленную рабочую станцию.

5.4.2 Работа Пользователя в соответствии с функциональными обязанностями

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.

После прохождения процедуры идентификации/аутентификации на сервере Пользователь может приступить к работе в рамках терминальной сессии.

ВНИМАНИЕ! Если планируется подключение к терминальному серверу по протоколу RDP, то рекомендуется изменить комбинацию для переключения языка ввода с «Shift+Alt» на «Shift+Ctrl» в ОС терминального сервера.

Также в рамках терминальной сессии Пользователю может быть предоставлена возможность использования USB-носителей «Секрет Особого Назначения», подключенных непосредственно к Терминалу. Клиентское ПО ПАК «Секрет Особого Назначения установлено на Защищенный терминал.

5.4.3 Сброс настроек функционального ПО

Пользователь после успешного прохождения процедуры аутентификации в утилите MKGearTool может удалить параметры,

установленные в процессе выполнения им настройки приложений для доступа к терминальному серверу. Для этого в окне утилиты MKGearTool Пользователю необходимо отметить приложения, параметры для которых необходимо удалить, и нажать кнопку <Сбросить>. После этого появляется окно, показанное на рисунок 12.

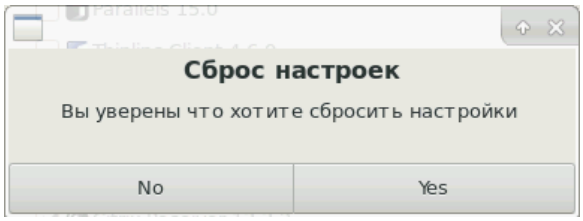

Рисунок 12 – Окно подтверждения сброса настроек

После нажатия кнопки <Yes> все параметры удаляются, и Пользователь может выполнить настройку заново с другими параметрами.

По завершению настройки Защищенного терминала необходимо завершить работу с ним, как указано в разделе 6.

5.5 Смена пароля

Для смены пароля Пользователю нужно запустить утилиту MKGearTool, в окне аутентификации (рисунок 1) установить флаг «Сменить пароль» и нажать кнопку <ОК>.

При этом на экране появляется окно смены пароля, в котором следует выбрать пользователя утилиты, ввести старый пароль и новый пароль с подтверждением. Для продолжения процедуры следует нажать кнопку <ОК>, для отмены – кнопку <Закрыть>.

Если процедура выполнена успешно, на экране появляется сообщение об успешной смене пароля Пользователя.

6 Завершение работы и выход из системы

Для завершения работы с Терминалом необходимо завершить терминальную сессию и работу приложений, запустить утилиту «Power Dialog» и нажать кнопку «Выключить» либо «Перезагрузить».

7 Обновление Терминала

Обновление Защищенного терминала выполняется уполномоченным лицом с помощью файлов обновлений, получаемых от производителя, и может включать:

- запись эталонного образа sd-карты;
- обновление образа ОС Защищенного терминала.

Запись эталонного образа sd-карты осуществляется с помощью специальной утилиты, входящей в комплект поставки Терминала.

Файлы обновлений образа ОС защищены технологически.

Способ установки файлов обновлений образа ОС зависит от версии утилиты MKGearTool.

Если версия утилиты меньше 1.1, в случае необходимости обновления образа ОС файлы обновлений образа ОС следует записать на sd-карту. Для записи файлов обновлений на sd-карту необходимо:

- отсоединить отчуждаемый ПК от док-станции;
- извлечь sd-карту из разъема отчуждаемого ПК;
- с помощью устройства чтения карт памяти подключить sd-карту к компьютеру;
- записать файлы обновлений на корневой каталог sd-карты;
- установить sd-карту в разъем отчуждаемого ПК;
- подключить отчуждаемый ПК к док-станции и включить микрокомпьютер.

При обновлении образа ОС в процессе загрузки Терминала проверяется корректность файлов обновлений, а на экране появляется сообщение: «Loading, please wait…».

Если проверка завершается успешно, появляется сообщение: «Apply update success».

В случае если проверка завершается ошибкой, возникает сообщение об ошибке: «Error loading. Update file verification failure! Please contact your

system administrator or technical support. Press OK/Enter to power off». По нажатии кнопки <OK> или <Enter> микрокомпьютер завершает работу и выключается. В этом случае необходимо проверить правильность выполнения процедуры обновления и повторить процедуру или обратиться в техническую поддержку производителя.

Если версия MKGearTool 1.1 и выше, обновление образа ОС Защищенного терминала выполняется Администратором с помощью утилиты MKGearTool.

Для выполнения операции следует записать файл обновления в корневую директорию внешнего USB-носителя и подключить USB-носитель к Терминалу.

ВНИМАНИЕ! Обязательным условием является запись файла обновления в корневую директорию – это необходимо для обнаружения файла программным обеспечением Защищенного терминала.

Далее в окне, изображенном на рисунке 7, следует нажать кнопку <Обновление> в панели инструментов.

В появившемся окне (рисунок 13) нужно указать подключенный USB-носитель и нажать кнопку <OK>. После завершения поиска обновлений на экране отображаются названия файлов обновлений (рисунок 14).

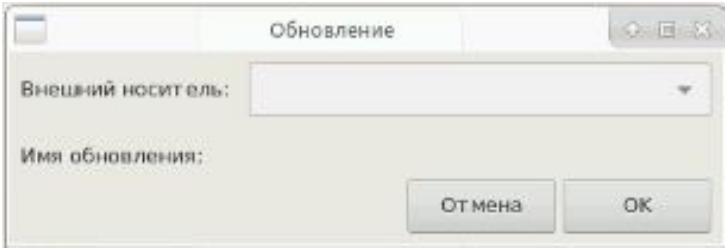

Рисунок 13 – Окно выбора файла обновления

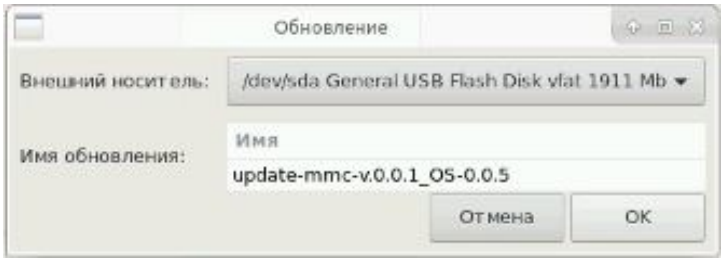

Рисунок 14 – Доступные обновления образа ОС

Администратору следует выбрать требуемый файл и нажать кнопку <ОК>.

При этом появляется окно с запросом аутентификации. В результате успешного завершения процедуры аутентификации Администратора начинается процесс обновления.

В случае возникновения ошибки в процессе обновления следует повторить процедуру или обратиться в техническую поддержку производителя.

Если обновление успешно завершено, появляется соответствующее сообщение.

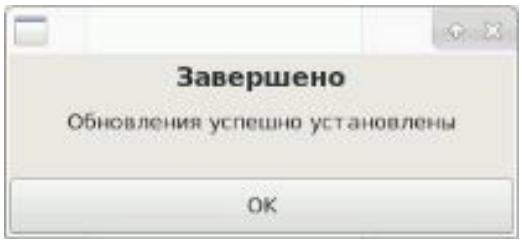

Рисунок 15 – Сообщение об успешном обновлении образа ОС

8 Перечень принятых сокращений и обозначений

БИ	–	безопасность информации;
ОНЗ	–	образ начальной загрузки;
ОС	–	операционная система;
ПАК СЗИ НСД	–	программно-аппаратный комплекс средств защиты информации от несанкционированного доступа;
ПО	–	программное обеспечение;
СХСЗ	–	сервер хранения и сетевой загрузки;
ТС	–	терминальная станция;
ФПО	–	функциональное программное обеспечение;
USB	–	universal serial bus.

Приложение А. Инструкция по настройке Citrix для работы с Терминалом (образ версии 0.0.6)

Для обеспечения корректного отображения окон с опубликованными приложениями при работе с терминалом на базе МКТ-card long (образ версии 0.0.6) необходимо учитывать два основных правила при добавлении опубликованных приложений:

1. при создании публикации для приложения в поле «Application name (for administrator)» (рисунок 16) необходимо указывать название приложения, используя латинский алфавит (например, «Notepad»).

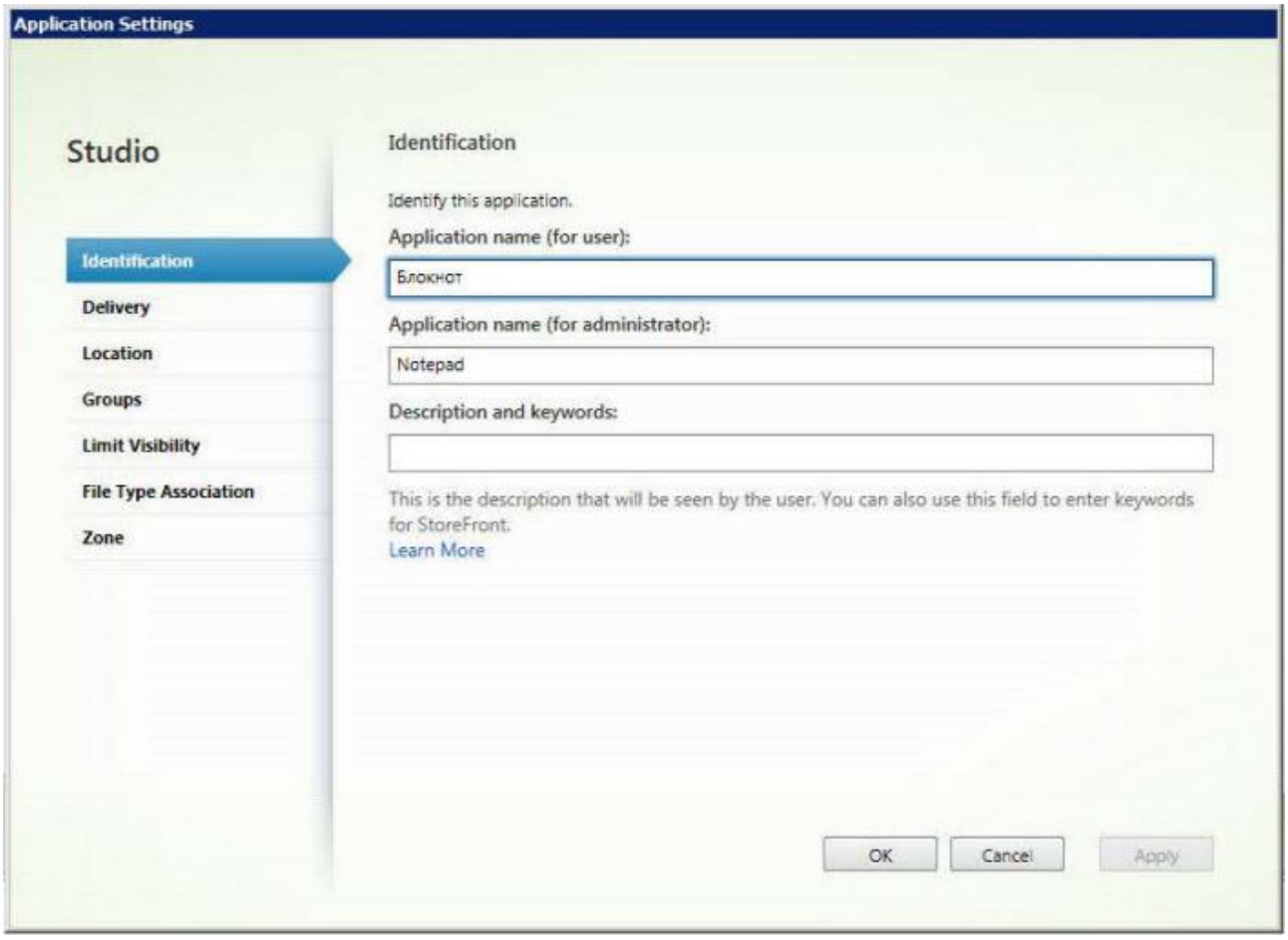

Рисунок 16 – Окно создания публикации приложения

В поле «Application name (for user)» можно вводить название в любом удобном виде (например, «Блокнот»), указанное в этом поле название будет видно пользователю.

ВНИМАНИЕ! Если все необходимые приложения уже были опубликованы ранее без учета этого правила, следует удалить их и опубликовать заново в указанном порядке.

2. после создания публикации необходимо открыть файл default.ica, расположенный в каталоге с ПО Citrix (например, в каталоге C:\inetpub\wwwroot\Citrix\Store\App_Data для Citrix версии 7.15; для другой версии Citrix расположение файла может отличаться), и добавить после Applications= новую пустую строку, а затем с новой строки – запись типа:

[имя_приложения]

TWIMode=Off

Например, для приложения «Блокнот» запись будет выглядеть так:

[Notepad]

TWIMode=Off

Для изменения размера окна приложения необходимо в том же файле задать параметры DesiredHRES (размер окна по горизонтали) и DesiredVRES (размер окна по вертикали) для интересующего приложения после записи, указанной выше. Например,

[имя_приложения]

TWIMode=Off

DesiredHRES=640

DesiredVRES=480

После редактирования и сохранения изменений следует перезапустить IIS-сервер для продолжения работы.

Приложение Б. Методы устранения неполадок в работе терминала на базе МКТ-card long в режиме сетевой загрузки

Выводимые на экран монитора сообщения о неполадках, возникающих в процессе работы Пользователя, причины их возникновения и рекомендуемый порядок действий Пользователя по их устранению приведены в таблице 4.

Таблица 4 – Методы устранения неполадок в работе

Сообщение на экране	**АРМ, на котором появляется сообщение**	**Возможные причины возникновения неполадки**	**Порядок действий**
«ПСКЗИ ШИПКА не присоединена»	Терминал на базе МКТ-card long	После загрузки ОС клиентское устройство ШИПКА Пользователя не было присоединено или была извлечена из USB-разъема	Перезагрузить Терминал не извлекая ШИПКУ из USB-разъема
«Не найден объект с настройками»	Терминал на базе МКТ-card long	Для Пользователя не выполнена настройка сети	1) обратиться к Администратору Терминала; 2) Администратор Терминала должен задать настройки сети для Пользователя
«Не удалось получить сетевой адрес по протоколу DHCP»	Терминал на базе МКТ-card long	Проблема доступа к локальной сети. Нет доступа к DHCP-серверу или он настроен неверно	1) проверить шнур подключения к локальной сети. При повторении ошибки обратиться к Администратору Терминала; 2) Администратор Терминала обратится к лицу, обеспечивающему работоспособность DHCP-сервера
«Ошибка при переводе сетевого интерфейса в рабочий режим: (Подробное описание)»	Терминал на базе МКТ-card long	Проблема доступа к локальной сети. Ошибка ОС	1) обратиться к Администратору Терминала; 2) Администратор Терминала выполнит необходимые действия, исходя из описания ошибки ОС

«Ошибка при переводе сетевого интерфейса в рабочий режим»	Терминал на базе МКТ-card long	Проблема доступа к локальной сети	1) проверить шнур подключения к локальной сети. При повторении ошибки обратиться к Администратору Терминала; 2) Администратору Терминала проверит подключение к локальной сети и правильность заданных настроек сети
«Ошибка при установке сетевого маршрута по умолчанию»	Терминал на базе МКТ-card long	Проблема доступа к локальной сети. Шлюз по умолчанию задан неверно и не может быть задан	1) проверить шнур подключения к локальной сети. При повторении ошибки обратиться к Администратору Терминала; 2) Администратор Терминала проверит подключение к локальной сети, правильность заданных настроек сети
«Аутентификация не выполнена»	Терминал на базе МКТ-card long	PIN -код не введен или введен некорректно	ввести корректный PIN -код
«Ошибка FTP -сессии»	Терминал на базе МКТ-card long, в логе активности операторов на СХСЗ (если система журналирования СХСЗ доступна)	Проблема доступа к СХСЗ. Проблема при установлении FTP -сессии	1) проверить шнур подключения к локальной сети. Перезагрузиться, при повторении ошибки обратиться к Администратору Терминала; 2) Администратор Терминала проверит подключение к локальной сети Терминала и СХСЗ, выполнит необходимые действия, исходя из описания ошибки FTP -сессии

«Ошибка при распаковке образа ПО ТС: «Ошибка чтения подписи образа ПО ТС»	Терминал на базе МКТ-card long, в логе активности операторов на СХСЗ	Файл с подписью образа ПО ТС поврежден либо отсутствует	1) обратиться к администратору Администратору Терминала; 2) Администратор Терминала обратится к администратору АРМ «Центр», затем к администратору БИ СХСЗ; 3) администратор АРМ «Центр» подпишет образ ПО ТС на АРМ «Центр»; 4) администратор БИ СХСЗ назначит подписанный образ пользователю
«Ошибка при распаковке образа ПО ТС»	Терминал на базе МКТ-card long, в логе активности операторов на СХСЗ	Образ ПО ТС поврежден	1) обратиться к Администратору Терминала; 2) Администратор Терминала обратится к администратору АРМ «Центр» и администратору БИ СХСЗ; 3) администратор АРМ «Центр» заново создаст образ ПО ТС на АРМ «Центр»; 4) администратор БИ СХСЗ назначит новый образ
«Ошибка при проверке целостности»	Терминал на базе МКТ-card long, в логе активности пользователей на СХСЗ	Проверка подписи образа ПО ТС завершена некорректно	1) обратиться Администратору Терминала; 2) Администратор Терминала обратится к администратору АРМ «Центр»; 3) администратор АРМ «Центр» проверит актуальность информации для проверки кода аутентификации и актуальность кода аутентификации образа ПО ТС

«Ошибка при сохранении параметров терминального подключения. Некорректный IP-адрес или доменное имя. Проверьте адрес вашего Citrix Broker»	Терминал на базе МКТ-card long	IP-адрес Citrix-брокера или доменное имя введены некорректно	проверить правильность указанного IP-адреса Citrix-брокера/доменного имени. При повторении ошибки обратиться к администратору Citrix-брокера
«Время не синхронизировано. Терминальная сессия может работать неправильно»	Терминал на базе МКТ-card long	Используется версия СХС3, не передающая данные о времени	1) обратиться к администратору СХС3; 2) администратор СХС3 обновит СХС3