ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Эксплуатационная документация на терминал

«MKT-card long»

Руководство по эксплуатации

11443195.4012.070 РЭ

Листов 33

Москва

2017

АННОТАЦИЯ

Настоящий документ является руководством по эксплуатации терминала «МКТ-card long» (далее также – защищенный терминал) и содержит сведения о характеристиках терминала «МКТ-card long» и указания, необходимые для его правильной и безопасной эксплуатации.

Перед эксплуатацией продукта рекомендуется внимательно ознакомиться с настоящим руководством.

Использование защитных мер терминала «МКТ-card long» должно дополняться общими мерами предосторожности и физической безопасности микрокомпьютера.

СОДЕРЖАНИЕ

1 Общие сведения

1.1 Назначение и область применения

«МКТ-card long» является защищенным микрокомпьютером с динамически изменяемой архитектурой.

Операционная система (ОС) «МКТ-card long» размещена в памяти с физически устанавливаемым доступом 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 «МКТ-card long».

Терминал «МКТ-card long» 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 «МКТ-card long» 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 «МКТ-card long» в режиме локальной загрузки ФПО: установленное на терминальном сервере программное решение по доставке приложений на удаленную рабочую станцию;

– для использования терминала «МКТ-card long» в режиме сетевой загрузки ФПО:

- установленное на терминальном сервере ПО Citrix XenApp;
- развернутый СХСЗ;
- развернутый АРМ «Центр»;
- назначенное Пользователю клиентское устройство ШИПКА.

1.3 Организационные меры

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

– физическая охрана терминала «МКТ-card long», в том числе проведение мероприятий по обеспечению целостности его корпуса;

– хранение в тайне PIN-кода клиентского устройства ШИПКА.

1.4 Роли пользователей

Терминал «МКТ-card long» 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 клиентских устройств ШИПКА;
- 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 «MKT-card long» выполнение процедур создания шаблона образа ПО ТС, платформы ТС, сбора образа ПО ТС из шаблона не требуется. Образ ПО ТС для терминала «MKT-card long» (MKTrust01) уже собран и добавлен в ПО АРМ «Центр» при производстве.

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.

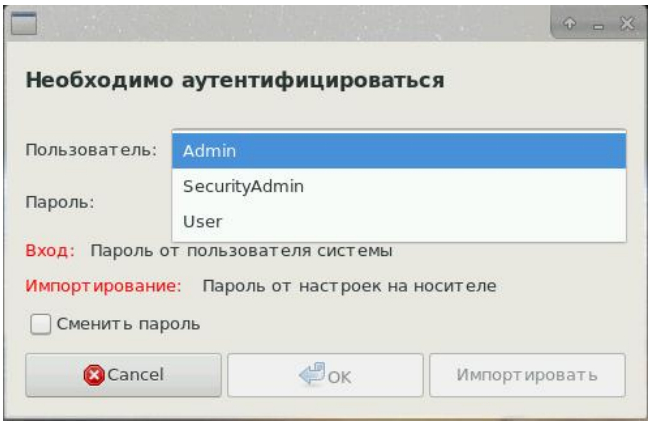

Рисунок 1 – Окно аутентификации

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 «МКТ-card long»

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»:
  - VMware Horizon;
  - СОН: Консоль пользователя;
  - xFreeRDP;
  - Parallels;
  - Thinlinc Client;
  - RDesktop;
  - NoMachine NX;
  - VNC;
  - Citrix Receiver;
  - Virt-Manager;
  - SPICE Client;
  - Firefox browser.

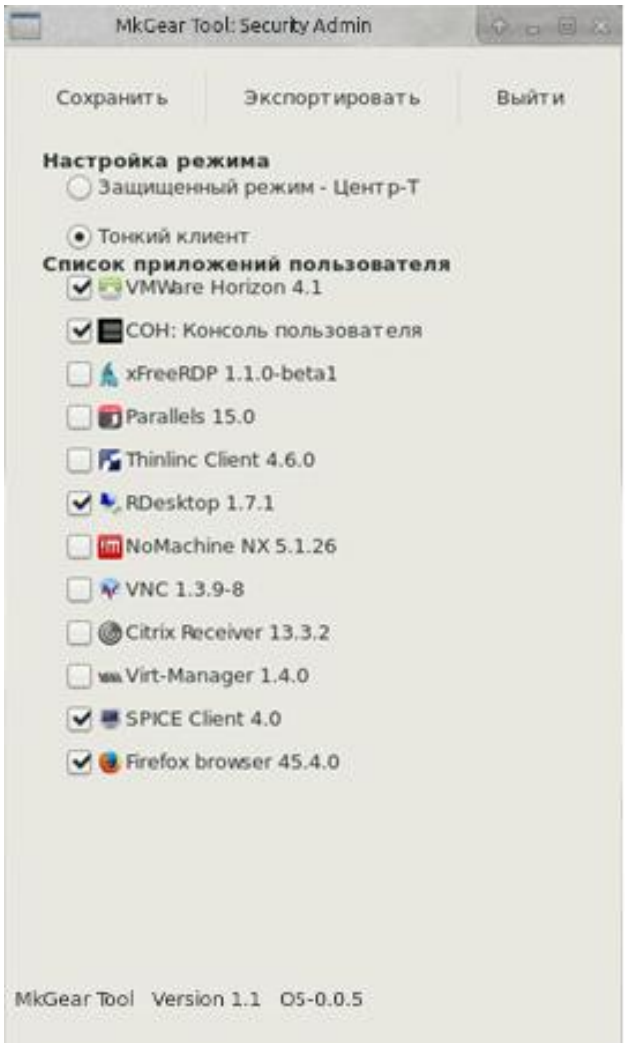

Рисунок 2 – Окно установки режима работы

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 завершению настроек Администратору БИ следует нажать кнопку <Выйти>.

3.3 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 3):

- *группа настроек «Настройки интерфейса»:*

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

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

– *группа настроек «Настройки сети»:*

– имя хоста – позволяет установить имя защищенного терминала;

– 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.

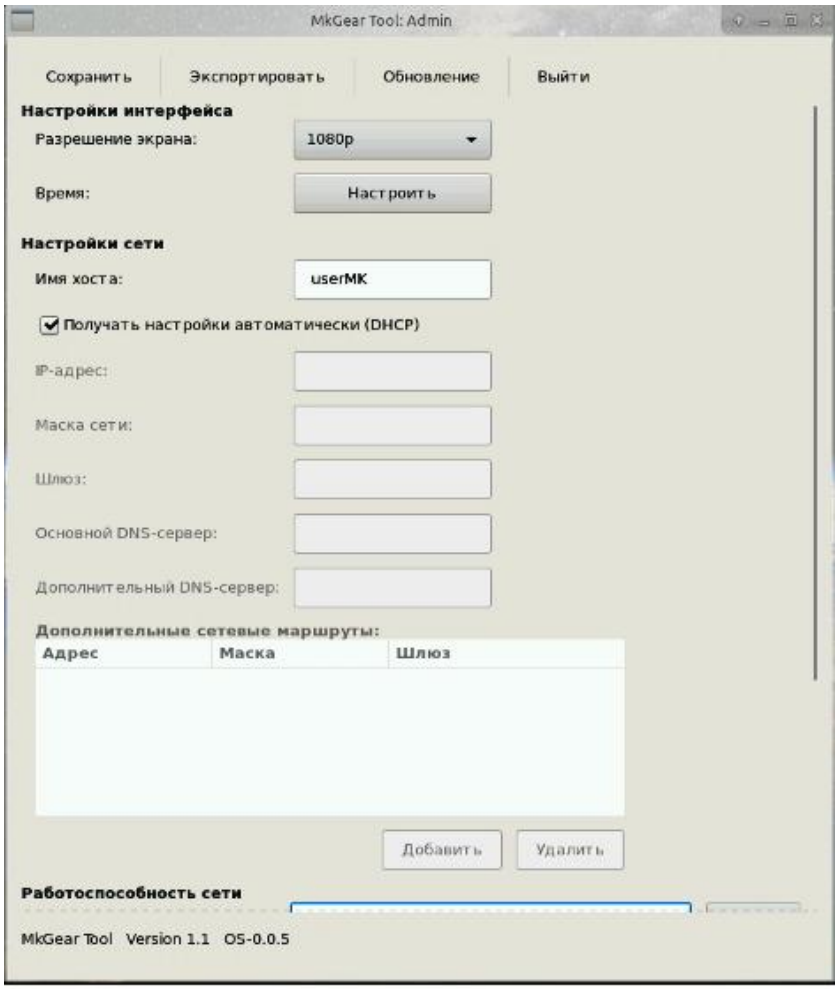

Рисунок 3 – Окно настроек интерфейса и сетевых настроек

Для настройки даты и времени необходимо нажать кнопку <Настроить> в строке «Время». При этом появляется окно, которое показано на рисунке 4.

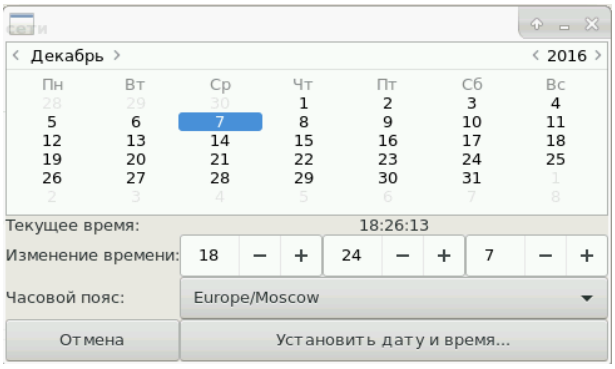

Рисунок 4 – Окно настройки даты и времени

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 завершению настроек Администратору следует нажать кнопку <Выйти>.

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 Использование терминала «МКТ-card long» в режиме сетевой загрузки функционального ПО

5.2.1 Начало работы

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

Если Администратором БИ установлен режим сетевой загрузки ФПО, клиентское устройство ШИПКА Пользователя должно быть подключено до включения терминала «МКТ-card long».

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 5).

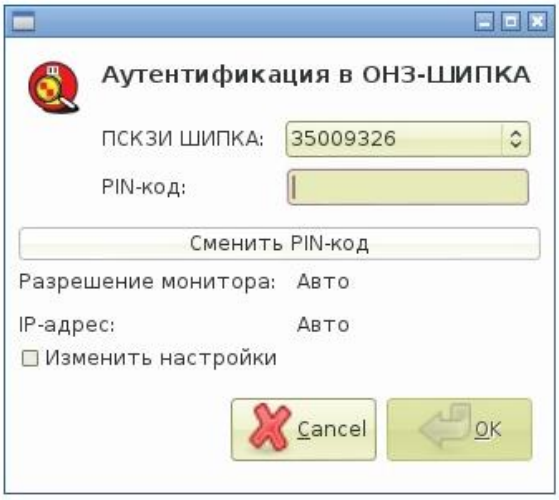

Рисунок 5 – Окно аутентификации Пользователя

Если в поле «Разрешение монитора» указано значение «Авто», то в образе ПО ТС используются параметры, установленные на этапе сборки ПО ТС (рисунок 5).

Если при настройке защищенного терминала Администратор установил автоматическое получение настроек по DHCP, то в поле «IP-адрес» стоит значение «Авто» (рисунок 5).

При первом запуске «МКТ-card long» в режиме сетевой загрузки ФПО пользователю необходимо установить адрес Citrix-брокера[1]. Для этого нужно установить флаг «Изменить настройки» (рисунок 5).

В поле «ПСКЗИ ШИПКА» следует выбрать серийный номер подключенного клиентского устройства ШИПКА, в поле «PIN -код» ввести

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

соответствующий PIN–код и нажать кнопку <OK> для подтверждения операции или кнопку <Cancel> для ее отмены.

По нажатию кнопки <OK> 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 «МКТ-card long» нужный образ ПО ТС.

При возникновении ошибки в процессе получения образа ПО ТС в появившемся на экране окне (рисунок 6) следует нажать кнопку <Назад> и повторить процедуру аутентификации.

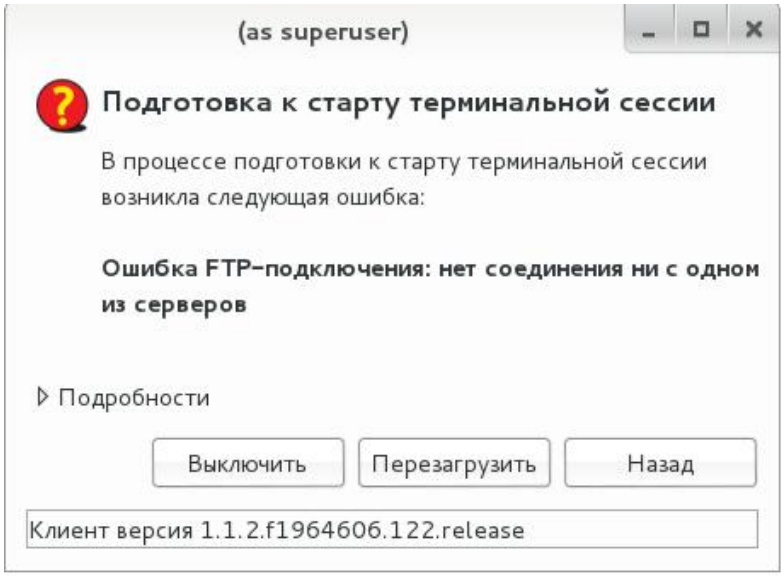

Рисунок 6 – Ошибка при получении образа ПО ТС

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

Если процедура корректно завершена, «МКТ-card long» 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 А.

5.2.2 Работа пользователя в соответствии с функциональными обязанностями

Пользователю «МКТ-card long» предоставляется возможность работы в рамках терминальной сессии, организованной средствами загруженного образа ПО ТС с заданными параметрами. Также в рамках терминальной сессии пользователю может быть предоставлена возможность

использования USB-носителей «Секрет Особого Назначения», подключенных непосредственно к «МКТ-card long».

5.3 Использование терминала «МКТ-card long» в режиме локальной загрузки функционального ПО

5.3.1 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:

- VMware Horizon;
- xFreeRDP;
- Parallels;
- Thinlinc Client;
- RDesktop;
- NoMachine NX;
- VNC;
- Citrix Receiver;
- Virt-Manager;
- SPICE Client;
- Firefox browser.

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.

5.3.2 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.

Также в рамках терминальной сессии пользователю может быть предоставлена возможность использования USB-носителей «Секрет Особого Назначения», подключенных непосредственно к «МКТ-card long». Клиентское ПО ПАК «Секрет Особого Назначения установлено на защищенный терминал.

5.3.3 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 7.

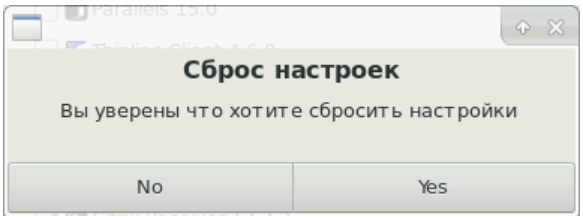

Рисунок 7 – Окно подтверждения сброса настроек

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.

5.4 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 «МКТ-card long» необходимо завершить терминальную сессию и работу приложений, запустить утилиту «Power Dialog» и нажать кнопку «Выключить» либо «Перезагрузить».

7 Обновление терминала «МКТ-card long»

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 «МКТ-card long».

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 «МКТ-card long» 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 «MKT-card long».

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 3, следует нажать кнопку <Обновление> в панели инструментов.

В появившемся окне (рисунок 8) нужно указать подключенный USB-носитель и нажать кнопку <OK>. После завершения поиска обновлений на экране отображаются названия файлов обновлений (рисунок 9).

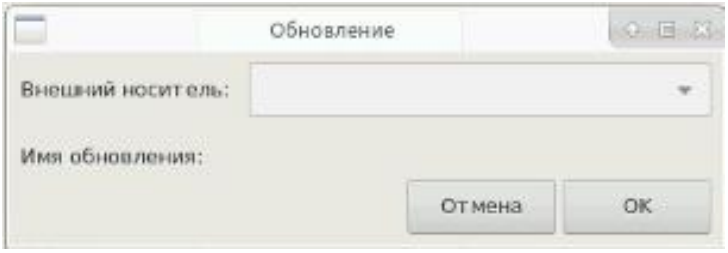

Рисунок 8 – Окно выбора файла обновления

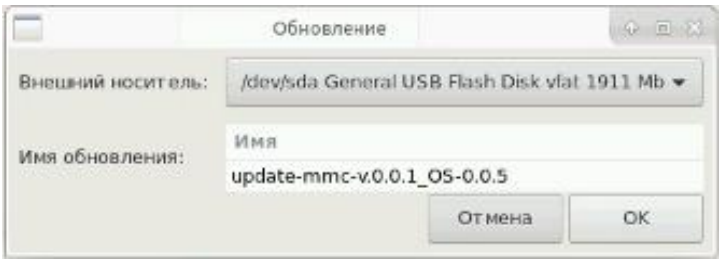

Рисунок 9 – Доступные обновления образа ОС

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.

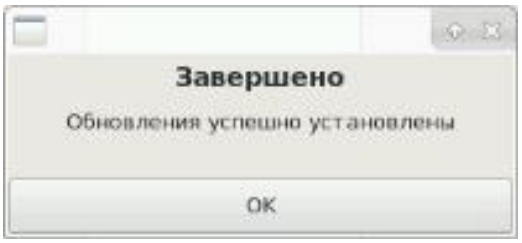

Рисунок 10 – Сообщение об успешном обновлении образа ОС

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. Методы устранения неполадок в работе «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»	«МКТ-card long»	После загрузки ОС клиентское устройство ШИПКА Пользователя не было присоединено или была извлечена из USB-разъема	Перезагрузить терминал «МКТ-card long», не извлекая ШИПКУ из USB-разъема
«Не найден объект с настройками»	«МКТ-card long»	Для Пользователя не выполнена настройка сети	1) обратиться к Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» должен задать настройки сети для Пользователя
«Не удалось получить сетевой адрес по протоколу DHCP»	«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 «МКТ-card long»; 2) Администратор терминала «МКТ-card long» обратится к лицу, обеспечивающему работоспособность DHCP-сервера

«Ошибка при переводе сетевого интерфейса в рабочий режим: (Подробное описание)»	«МКТ-card long»	Проблема доступа к локальной сети. Ошибка ОС	1) обратиться к Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» выполнит необходимые действия, исходя из описания ошибки ОС
«Ошибка при переводе сетевого интерфейса в рабочий режим»	«МКТ-card long»	Проблема доступа к локальной сети	1) проверить шнур подключения к локальной сети. При повторении ошибки обратиться к Администратору терминала «МКТ-card long»; 2) Администратору терминала «МКТ-card long» проверит подключение к локальной сети и правильность заданных настроек сети
«Ошибка при установке сетевого маршрута по умолчанию»	«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 «МКТ-card long»; 2) Администратор терминала «МКТ-card long» проверит подключение к локальной сети, правильность заданных настроек сети
«Аутентификация не выполнена»	«МКТ-card long»	PIN -код не введен или введен некорректно	ввести корректный PIN -код
«Ошибка FTP -сессии»	«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 обратится к Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» 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»	«МКТ-card long», в логе активности операторов на СХСЗ	Файл с подписью образа ПО ТС поврежден либо отсутствует	1) обратиться к администратору Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» 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»	«МКТ-card long», в логе активности операторов на СХСЗ	Образ ПО ТС поврежден	1) обратиться к Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» 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»	«МКТ-card long», в логе активности пользователей на СХСЗ	Проверка подписи образа ПО ТС завершена некорректно	1) обратиться Администратору терминала «МКТ-card long»; 2) Администратор терминала «МКТ-card long» 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»	«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»	«МКТ-card long»	Используется версия СХС3, не передающая данные о времени	1) обратиться к администратору СХС3; 2) администратор СХС3 обновит СХС3