Утвержден

МБРЦ.468313.001-ЛУ

# ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС “ГОРИЗОНТ-ВС”

ВЕРСИЯ 01-02-01.02-02-02

*Руководство пользователя*

МБРЦ.468313.001 Д1

Листов 21

| Инв. № подл | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
|---|---|---|---|---|
| | | | | |

***Содержание***

Настоящее руководство пользователя МБРЦ.468313.001 Д1 является основным документом, описывающим порядок действий пользователя при работе с изделием программно-аппаратный комплекс (ПАК) “Горизонт-ВС” МБРЦ.468313.001 (далее по тексту – изделие).

В руководстве пользователя приведены основные сведения, необходимые пользователю для работы с изделием, установленным на *терминале*, созданном на базе персональной электронной вычислительной машины (ПЭВМ).

## *1 Назначение и основные функции изделия*

ПАК “Горизонт-ВС” является многокомпонентным распределённым комплексом с единой политикой безопасности, в состав которого входит модуль идентификации и контроля доверенной среды (МИиКДС) “Шина” МБРЦ.468264.001 (далее по тексту – МИиКДС “Шина”) и комплекс программ (КП) “Терминал-Сервер” RU.МБРЦ.501130.01-01 (далее по тексту – КП “Терминал-Сервер”).

МИиКДС “Шина” предназначен для защиты автоматизированных рабочих мест, являющихся *терминалами*[1] (далее по тексту – *терминал* или ПЭВМ), от несанкционированного доступа (НСД) и взаимодействия с индивидуальным USB-носителем (далее по тексту - индивидуальный USB-носитель или ИН), на котором установлен КП “Терминал-Сервер”.

КП “Терминал-Сервер” является гипервизором, устанавливаемым непосредственно на аппаратное обеспечение в качестве системного программного обеспечения, и предназначен для организации исполнения виртуальных машин (ВМ), а также для подключения *терминалов* по протоколу SPICE к виртуальным машинам[2], исполняемым на *сервере виртуализации*[3]. На *терминалы* устанавливается компонент “Тонкий клиент” (компонент 1 согласно формуляру МБРЦ.468313.001 ФО) из состава КП “Терминал-Сервер”.

В ПАК “Горизонт-ВС” предусмотрено два режима работы:

- основной – работа изделия в составе ГИС 1 класса защищенности;

- дополнительный – работа изделия в составе ГИС 2 класса защищенности и ниже (в данном режиме предусмотрено отключение МИиКДС “Шина”).

Изделие, установленное на *терминале*, обеспечивает выполнение следующих функций:

- идентификацию и аутентификацию пользователя;
- доверенную загрузку КП с индивидуального USB-носителя пользователя;
- контроль целостности файлов на USB-носителе;
- блокировку работы *терминала* в случае неудачной идентификации и аутентификации пользователя;

---

[1] *Терминал* – аппаратное устройство, предназначенное для удаленного подключения к виртуальной машине, исполняемой на *сервере* виртуализации.

[2] Виртуальная машина – эмуляция аппаратной среды, сформированной программным способом.

[3] *Сервер виртуализации* – аппаратное устройство, предназначенное для создания и исполнения виртуальных машин.

– блокировку входа в систему зарегистрированного пользователя при:

1) нарушении целостности контролируемых объектов, входящих в КП;

2) превышении предельного числа неудачных попыток входа и истечении срока действия пароля;

3) блокировании администратором средства доверенной загрузки (СДЗ) входа пользователя;

– ведение журнала регистрации событий, в котором производится регистрация событий, имеющих отношение к безопасности системы;

– самотестирование (проверку технического состояния);

– подключение к ВМ, исполняемым на *сервере виртуализации*, по протоколу SPICE;

– вывод графической и звуковой информации ВМ через *терминал*;

– ввод информации с клавиатуры *терминала* в ВМ;

– подключение манипулятора типа “мышь” (далее по тексту – “мышь”) *терминала* к ВМ;

– ввод звуковой информации в ВМ через микрофон *терминала*;

– подключение USB-устройств *терминала* к ВМ;

– предоставление средств для настройки сетевых параметров соединения *терминала*, настройки режима работы *терминала*;

– восстановление системы после сбоя;

– непрерывную круглосуточную работу.

## *2 Общие сведения*

Для работы пользователя на *терминале* с установленным изделием, необходима регистрация пользователя в изделии. Процедуру регистрации пользователей производит администратор СДЗ.

После регистрации администратор СДЗ должен сообщить пользователю пароль для входа в систему, а также выдать персональный электронный ключ DS1995 (далее по тексту – электронный ключ, ЭК или ЭК аутентификации), содержащий идентифицирующую информацию данного пользователя и индивидуальный USB-носитель с установленным КП “Терминал-Сервер”.

Электронный ключ и пароль необходимы для подтверждения права работы с изделием, а индивидуальный USB-носитель необходим для загрузки КП “Терминал-Сервер”. ЭК и индивидуальный USB-носитель предъявляются системе защиты при каждом включении *терминала*.

Пользователь может работать с одним и тем же ЭК аутентификации и ИН только на том *терминале*, на котором он зарегистрирован.

Изделие контролирует время действия пароля (это интервал времени - 90 дней). По истечении срока действия пароля пользователь будет заблокирован изделием.

Пользователь работает в среде операционной системы, установленной на ВМ, исполняемой на *сервере виртуализации*.

# 3 Аутентификация пользователя на терминале

## 3.1 Начало работы

**Примечание**: в режиме “дополнительный” работа начинается с загрузки КП “Терминал-Сервер”, поэтому следует читать, начиная с п. 1.

В начале работы пользователь должен установить индивидуальный USB-носитель в разъем USB-порта и включить *терминал* кнопкой включения питания (**Power**).

***ВНИМАНИЕ:*** *ИНДИВИДУАЛЬНЫЙ USB-НОСИТЕЛЬ ДОЛЖЕН БЫТЬ УСТАНОВЛЕН В ОДНОМ ИЗ РАЗЪЕМОВ USB-ПОРТА НА ПРОТЯЖЕНИИ ВСЕГО СЕАНСА РАБОТЫ.*

Процедура аутентификации выполняется при каждом включении/перезагрузке *терминала*. После включения/перезагрузки *терминала* и выполнения аппаратных тестов на экране открывается главное интерактивное окно изделия (рисунок 1).

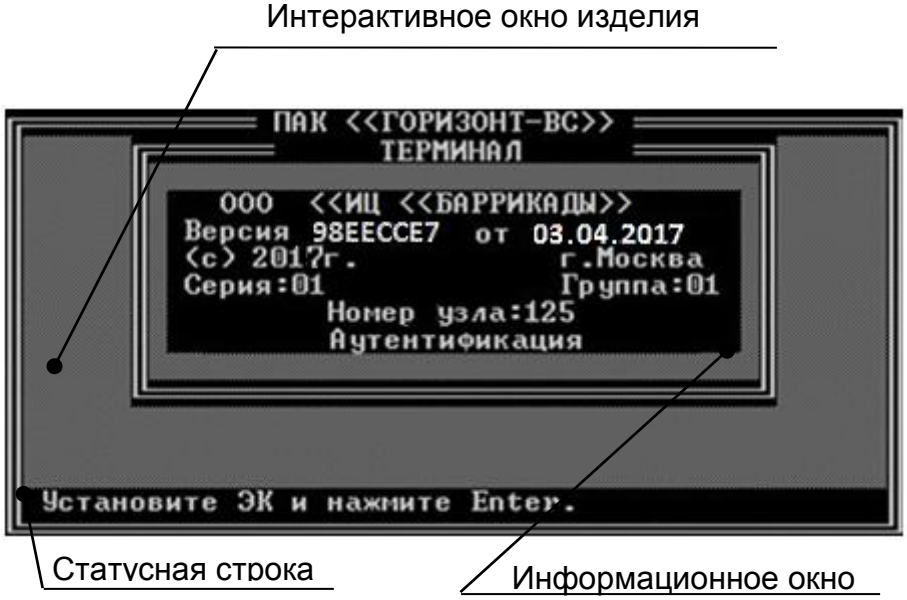


Рисунок 1 – Интерактивное окно

В информационное окно выводится: номер узла (номер *терминала* в АГ), номер АГ в глобальной сети, серия (учетная информация) и текущий процесс – **Аутентификация**.

В нижней части окна находится статусная строка, в которую выдаются сообщения об ошибках и различные указания для работы с ЭК (полный список сообщений статусной строки приведен в приложении А).

На сообщение:

**Установите ЭК и нажмите Enter.**

необходимо установить ЭК аутентификации пользователя в считыватель для электронных ключей (далее по тексту – считыватель) (правила работы с электронным ключом описаны в приложении Б) и нажать клавишу **Enter**. Далее в статусную строку выводится приглашение для ввода пароля аутентификации (рисунок 2).

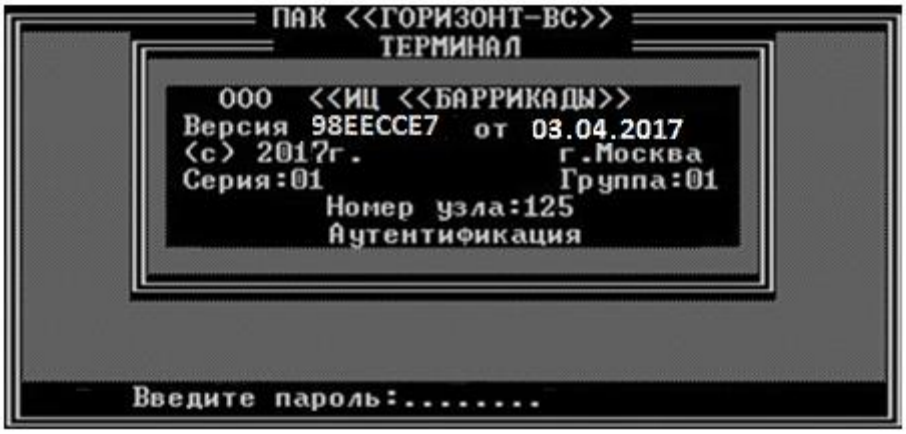


Рисунок 2 – Ввод пароля

***Примечание*** *– В том случае, если более двух минут (120 секунд) не вводить пароль, то терминал блокируется.*

Длина пароля – 8 символов. Пароль может содержать латинские, служебные символы и цифры; заглавные и прописные буквы различаются. Все введенные символы отображаются знаком ‘*’. Если какой-либо символ введен неверно, то его можно стереть (клавиша **BackSpace)** и повторить ввод.

После ввода восьмого символа начинается процесс аутентификации и в статусную строку выводится следующее сообщение:

**Ждите. Идет аутентификация.**

При успешном выполнении аутентификации в статусную строку выдается сообщение:

**Успешная аутентификация.**

В том случае, если был установлен незарегистрированный ЭК аутентификации или при вводе пароля допущена ошибка (неудачная попытка входа), то в статусную строку выдается сообщение:

**Неправильный пароль или ЭК.**

В ответ на это сообщение необходимо нажать клавишу **Enter** и повторить процедуру аутентификации с помощью другого - правильного ЭК или повторить попытку ввода пароля. Если после трех попыток ввода пароля процесс аутенти-

фикации закончился неудачно, то на экран и в статусную строку выдается сообщение:

**Работа изделия остановлена.**

Для дальнейшей работы необходимо перезагрузить *терминал* и повторить попытку входа.

В том случае, если ЭК аутентификации пользователя зарегистрирован в изделии, но произведено подряд 8 неудачных попыток входа или общее число неудачных попыток входа превысило значение 10, то произойдет блокирование его ЭК в изделии, и дальнейшая работа данного пользователя на данном *терминале* будет невозможна.

При попытке входа пользователя в статусную строку выдается сообщение:

**Пользователь заблокирован.**

Данное сообщение также выдается в том случае, если зарегистрированный пользователь заблокирован администратором СДЗ.

За разъяснениями и помощью в данных случаях необходимо обратиться к администратору СДЗ.

При успешном выполнении аутентификации для перехода к загрузке КП “Терминал-Сервер” необходимо нажать клавишу **Enter**. В статусную строку выдается сообщение:

**Уберите ЭК из считывателя.**

Необходимо извлечь ЭК аутентификации из считывателя и нажать клавишу **Enter**.

На экран выдаются окна, подобные представленным на рисунках 3 и 4, в которые выводится информация о выполнении процесса проверки целостности индивидуального USB-носителя пользователя.

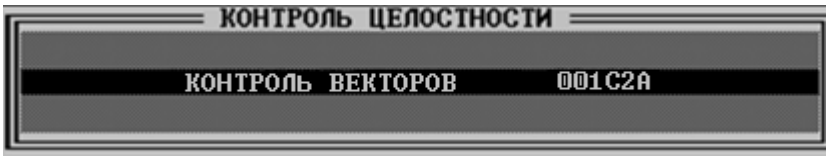


Рисунок 3 - Контроль целостности - режим контроля **посекторный**

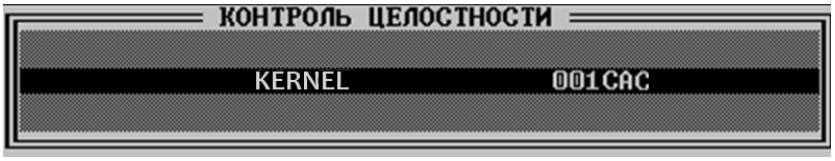


Рисунок 4 **–** Контроль целостности - режим контроля **файловый**

***Примечание*** *– При* ***посекторном*** *режиме контроля выполняется проверка целостности секторов USB-носителя, а при* ***файловом*** *- отдельных файлов.*

Если при проверке целостности не обнаружены ошибки, то пользователь получит доступ к запуску КП “Терминал-Сервер” и работе в среде ВМ (раздел 3).

В противном случае выдается сообщение:

**Ошибка при КОНТРОЛЕ ВЕКТОРОВ.**

или

**<имя файла>  ERR**,

необходимо нажать клавишу **Enter** – выдается сообщение:

**Ошибка при КОНТРОЛЕ ВЕКТОРОВ.**

Для продолжения надо нажать клавишу **Enter**. В статусную строку выдается сообщение:

**Работа изделия остановлена.**

В данном случае необходимо проверить соответствие индивидуального USB-носителя текущему пользователю, установить правильный ИН и выполнить перезагрузку.

Если ошибка при контроле векторов повторится, следует обратиться к администратору СДЗ за разъяснениями и помощью.

### *3.2 Контроль времени действия пароля*

Время действия пароля - это интервал времени, который устанавливается по умолчанию - 90 дней.

В том случае, если после установки ЭК в считыватель и нажатия клавиши **Enter,** на экран выдается сообщение:

**Истекает срок действия пароля.**

следует сообщить об этом администратору СДЗ. Данное сообщение будет выводиться в течение пяти дней. Пользователь может продолжить работу и перейти к процедуре ввода пароля, нажав клавишу **Enter**. Если же за этот период времени (пять дней) смена пароля не будет выполнена, на экран будет выдано сообщение:

**Срок действия пароля истек.**

Для продолжения нажать клавишу **Enter**. В статусную строку выдается сообщение:

**Работа изделия остановлена.**

При появлении данного сообщения работа *терминала* блокируется. За разъяснениями и помощью следует обратиться к администратору СДЗ.

***ВНИМАНИЕ:*** *ПАРОЛИ ПОЛЬЗОВАТЕЛЕЙ МЕНЯЮТСЯ АДМИНИСТРАТОРОМ СДЗ ОДИН РАЗ В ТРИ МЕСЯЦА (90 ДНЕЙ).*

# 4 Работа пользователя в среде ВМ

## 4.1 Загрузка ВМ

После успешного прохождения процесса аутентификации с помощью МИиКДС “Шина” выдается окно **Требуется аутентификация** (рисунок 5), в котором нужно ввести имя пользователя, пароль и нажать кнопку **Yes**.

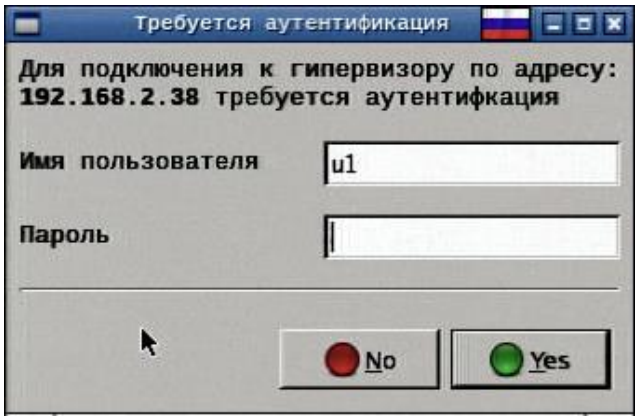


Рисунок 5 - Окно аутентификации

Если введены неверные данные, то будет выдано сообщение об ошибке (рисунок 6).

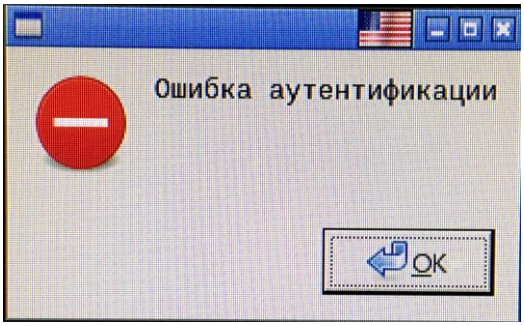


Рисунок 6 - Сообщение об ошибке

После ввода верных имени пользователя и пароля появляется окно **Выбор ВМ** (рисунок 7), в котором показана ВМ, разрешенная администратором СДЗ для данного пользователя.

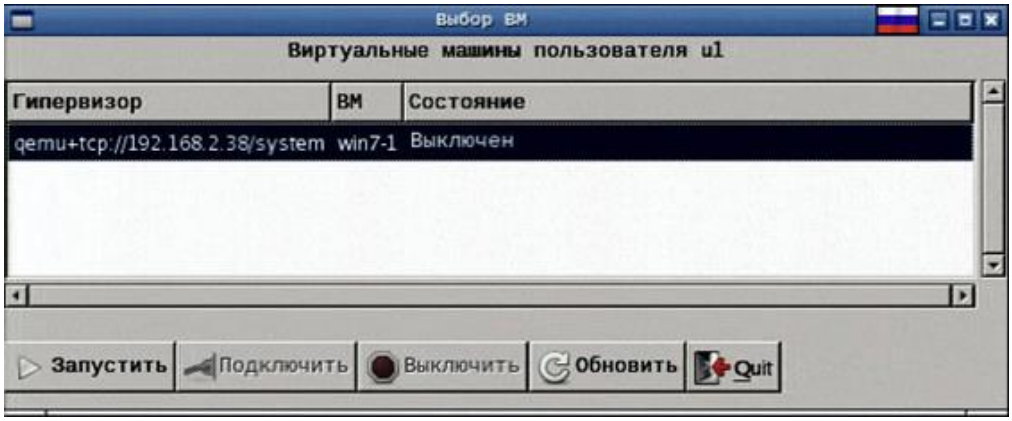


Рисунок 7 - Выбор ВМ

Следует выбрать ВМ и, если состояние ВМ “Выключен”, нажать кнопку **Запустить**. Далее необходимо дождаться, когда состояние ВМ сменится на “Работает” (ВМ запустится на *сервере виртуализации*). После этого нажать кнопку **Подключить** (рисунок 8), и начнется загрузка операционной системы (ОС), установленной на ВМ.

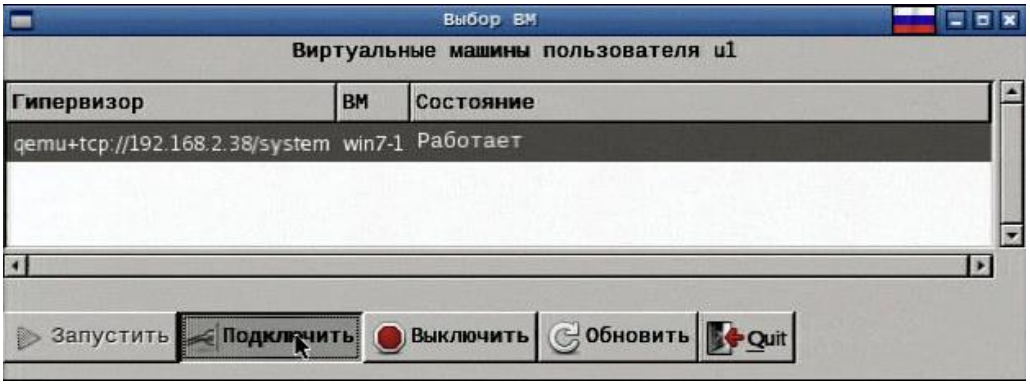


Рисунок 8 - Подключение к ВМ

Для того чтобы обновить список ВМ, доступных пользователю, или их состояние, следует нажать кнопку **Обновить**.

Для того чтобы завершить работу ВМ, необходимо нажать кнопку **Выключить**.

После нажатия кнопки **Выход** произойдет выключение *терминала*.

После успешного прохождения процесса аутентификации на *терминале* пользователь попадает в среду операционной системы (ОС), установленную на ВМ, исполняемой на *сервере виртуализации*, например, Microsoft Windows 7 (рисунок 9).

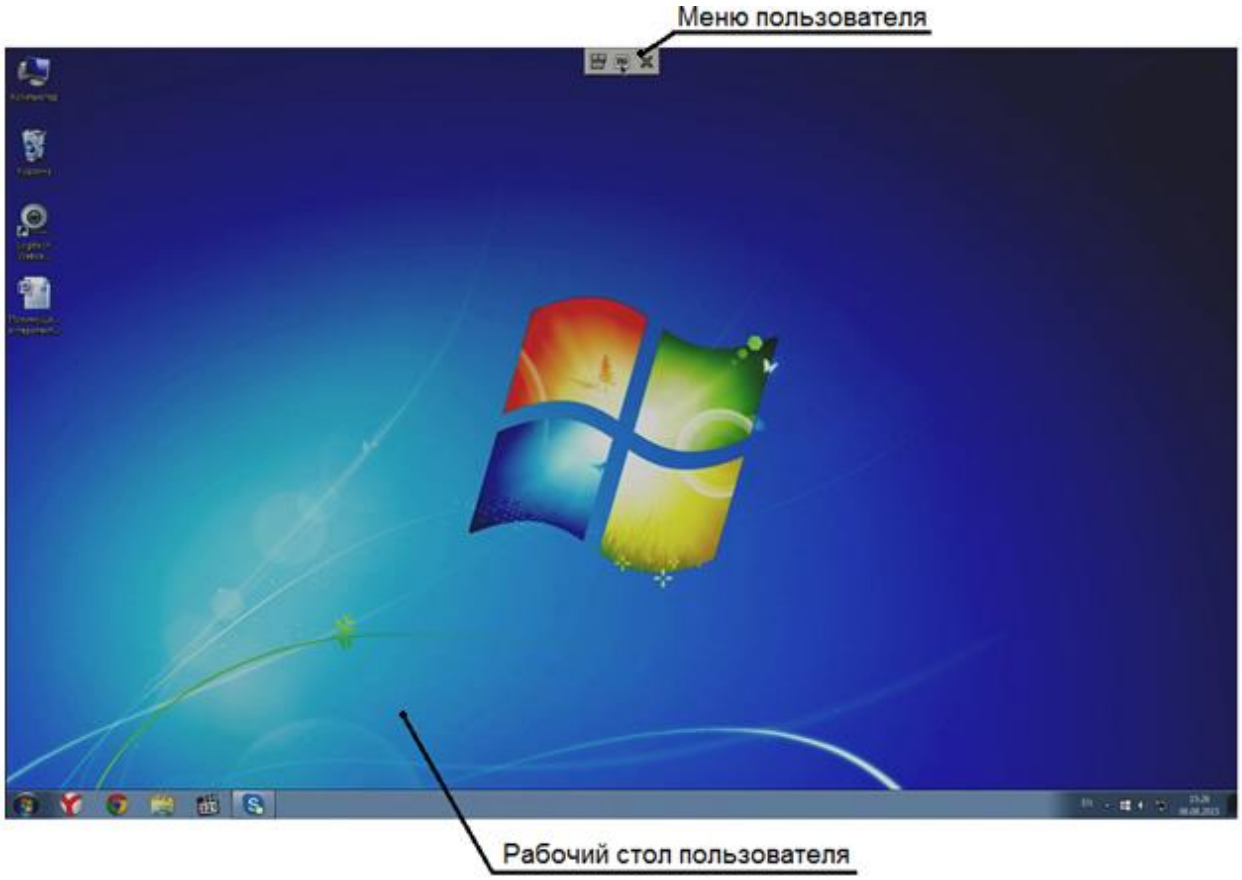


Рисунок 9 – Рабочий стол пользователя ОС Windows 7

### *4.2 Меню пользователя*

Для работы с *терминалом* предназначено меню, которое появляется при подведении манипулятора типа “мышь” к центру верхнего края экрана (рисунок 9).

ОС при нажатии определенных сочетаний клавиш может выполнять различные операции. ОС *сервера виртуализации* резервирует для себя определенные комбинации клавиш на клавиатуре (например, **Ctrl+Alt+Del**). Для выполнения действий, связанных с использованием системных комбинаций клавиш, в ВМ используется меню с готовыми комбинациями клавиш.

Для того чтобы отправить в ОС Microsoft Windows 7 некоторую комбинацию клавиш, следует нажать кнопку меню **Отправить комбинацию клавиш**  и выбрать из раскрывающегося списка нужную комбинацию (рисунок 10):

– **Ctrl+Alt+Del** позволяет перезагрузить ОС в ВМ;

– **Ctrl+Alt+Backspace** перезагружает графическую среду;

– **Ctrl+Alt+Fx** (где **Fx** одна из функциональных клавиш от **F1** до **F12**) позволяет переключаться между консолями;

– **PrintScreen** делает снимок экрана.

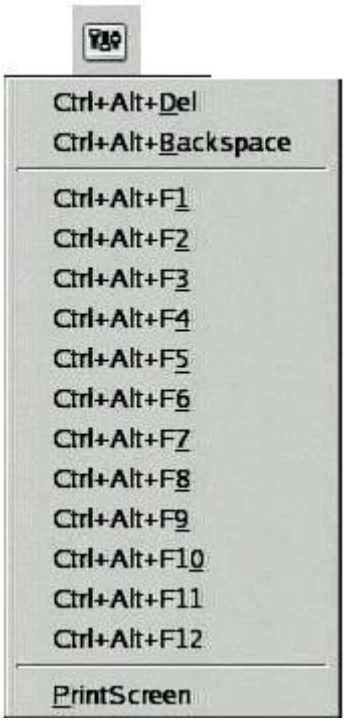


Рисунок 10 – Список комбинаций клавиш

Для подключения к *терминалу* внешних USB-устройств, необходимо нажать кнопку меню **Выбор устройства USB**  , в появившемся окне (рисунок 7) отметить флажком нужное USB-устройство для подключения и нажать кнопку **Закрыть**.

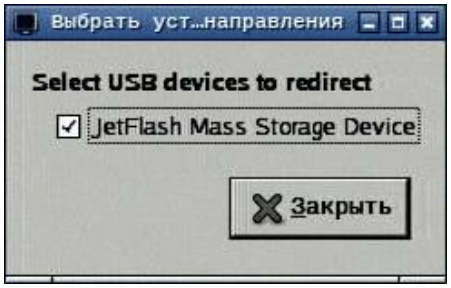


Рисунок 11 – Выбор USB-устройства

***ВНИМАНИЕ**: НЕЗАРЕГИСТРИРОВАННЫЕ НА СЕРВЕРЕ ВИРТУАЛИЗАЦИИ USB-УСТРОЙСТВА НА ТЕРМИНАЛЕ РАБОТАТЬ НЕ БУДУТ*.

Для завершения работы с ВМ и выключения *терминала* следует нажать правую кнопку меню **Отключиться**. На экране появится сообщение об отключении (рисунок 8). После нажатия кнопки **ОК**, *терминал* будет отключен.

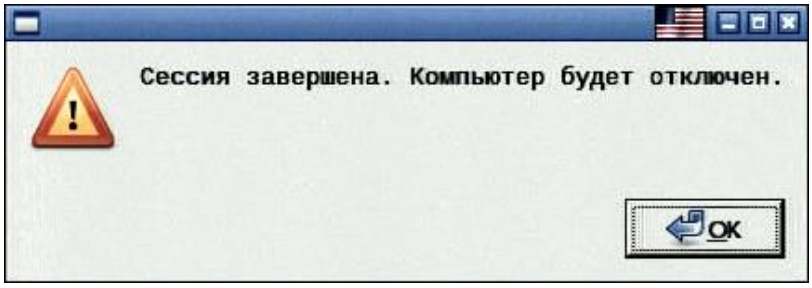


Рисунок 12 – Сообщение об отключении

Кроме того, сообщение об отключении компьютера может появиться, если администратор СДЗ *сервера виртуализации* остановит работу ВМ, к которой подключен пользователь.

### *4.3 Сообщения пользователю*

При штатной работе программы никаких сообщений пользователю не выводится.

Если на экране появляются какие-либо сообщения, например, как на рисунке 9, то следует обратиться к администратору СДЗ.

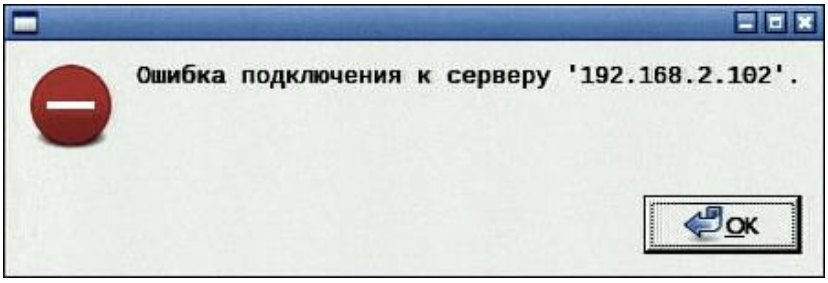


Рисунок 13 – Сообщение о неудачной попытке подключения к *серверу виртуализации*

## *5 Действия пользователя при компрометации*

Под компрометацией ЭК аутентификации понимается их утрата, хищение, захват ключей или другие происшествия, в результате которых судьба ключей аутентификации стала неизвестной.

При компрометации ЭК аутентификации пользователя необходимо обратиться к администратору СДЗ для получения нового ЭК взамен скомпрометированного.

***ВНИМАНИЕ:*** *1 ЭК АУТЕНТИФИКАЦИИ ДОЛЖНЫ ХРАНИТЬСЯ ТАКИМ ОБРАЗОМ, ЧТОБЫ ИСКЛЮЧИТЬ ВОЗМОЖНОСТЬ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ НА НИХ.*

*2 ПОЛЬЗОВАТЕЛЮ ПРИ ЭКСПЛУАТАЦИИ НЕОБХОДИМО СОХРАНЯТЬ В ТАЙНЕ ЭК АУТЕНТИФИКАЦИИ, А ТАКЖЕ СВОЙ ПАРОЛЬ.*

# *Приложение А*

(справочное)

Список сообщений, выдаваемых в статусной строке при аутентификации

А.1 В таблице А.1 приведен перечень сообщений, выдаваемых в статусной строке.

Таблица А.1

| Сообщение | Тип сообщения | Пояснения и рекомендации |
|---|---|---|
| 1 Введите пароль:..... | И | Ввести пароль из 8 символов |
| 2 Ждите. Идет аутентификация | И | Идет процесс аутентификации |
| 3 Истекло время аутентификации | О | Превышено время аутентификации. Необходимо перезагрузить *терминал* |
| 4 Истекает срок действия пароля | И | Необходимо выполнить операцию смены пароля аутентификации |
| 5 Неправильный пароль или ЭК | О | Установить правильный ЭК или ввести правильный пароль |
| 6 Ошибка при загрузке изделия | С | Сбой изделия. При многократных сообщениях - изделие считать неисправным |
| 7 Ошибка при КОНТРОЛЕ ВЕКТОРОВ | О | В процессе контроля целостности индивидуального USB-носителя была обнаружена ошибка |
| 8 Пользователь заблокирован | И | Вход пользователя заблокирован в списке пользователей изделия |
| 9 Превышено число попыток входа | И | Количество неудачных попыток входа пользователя больше 10 |
| 10 РАБОТА ИЗДЕЛИЯ ОСТАНОВЛЕНА | И | Необходимо перезагрузить *терминал* |
| 11 Сбой при чтении ЭК | О/С | 1 Вставлен неверный тип ЭК.<br>2 Сбой изделия |
| 12 Срок действия пароля истек | И | Пользователь блокируется системой защиты. Необходимо выполнить операцию смены пароля аутентификации |
| 13 Успешная аутентификация | И | Аутентификация прошла успешно |
| 14 ЭК не установлен | О | 1 Проверить ЭК и/или считыватель.<br>2 Сбой изделия |

Примечание - Сообщения в статусной строке могут быть четырех типов:

1) сообщения связанные с ошибками администратора/пользователя (О);

2) сообщения о сбоях изделия (С);

3) сообщения о событиях, которые могут быть вызваны или ошибками администратора/пользователя или сбоями изделия (О/С);

4) информационные сообщения (И).

# *Приложение Б*

(справочное)

Правила работы с электронным ключом DS1995 и
контактным устройством RDS-13

Б.1 Назначение электронного ключа

Б.1.1 Электронный ключ DS1995 предназначен для хранения ключевой информации пользователей. Ключевая информация необходима для идентификации и аутентификации пользователя при попытке входа в операционную систему ПЭВМ.

Б.2 Технические характеристики

Б.2.1 Электронный ключ DS1995 из семейства iButton

Электронный ключ работает в составе изделия, информация считывается и записывается в электронный ключ с помощью считывателя (контактное устройство RDS-13).

Хранение данных в памяти электронного ключа в течение 10 лет.

Контактная стойкость – не менее $10^6$ циклов запись/стирание.

Работоспособность электронного ключа обеспечивается при температуре окружающей среды от минус 40 до плюс 70 °С.

Электронный ключ DS1995 обладает высокой стойкостью к таким воздействиям окружающей среды, как грязь, влажность и удары.

Б.3 Общие положения

Б.3.1 Пользователь может работать с одним и тем же электронным ключом на нескольких ПЭВМ.

Б.3.2 Для работы пользователя в составе АГ необходимо, чтобы электронный ключ был создан и зарегистрирован в изделиях, установленных на ПЭВМ, к которым разрешен доступ данного пользователя. Процедура создания и регистрации электронного ключа выполняет администратор АГ.

Б.3.3 После создания электронного ключа пользователя администратор СДЗ должен выдать ему электронный ключ и сообщить пароль аутентификации.

Электронный ключ и пароль необходимы для подтверждения права работать в ОС. Электронный ключ требуется при каждой загрузке ПЭВМ.

Б.4 Порядок работы с электронным ключом DS1995

Б.4.1 Электронный ключ - это устройство в форме таблетки, вмонтированной в пластиковый держатель. В памяти электронного ключа хранится ключевая информация.

Б.4.2 Электронный ключ работает совместно со считывателем, который, в свою очередь подсоединен к плате изделия. Компактный профиль в форме таблетки позволяет электронному ключу автоматически центрироваться в считывателе, что дает возможность пользователям легко им оперировать. Доступ к данным может происходить при касании электронным ключом к контактной площадке считывателя (рисунок Б.1).

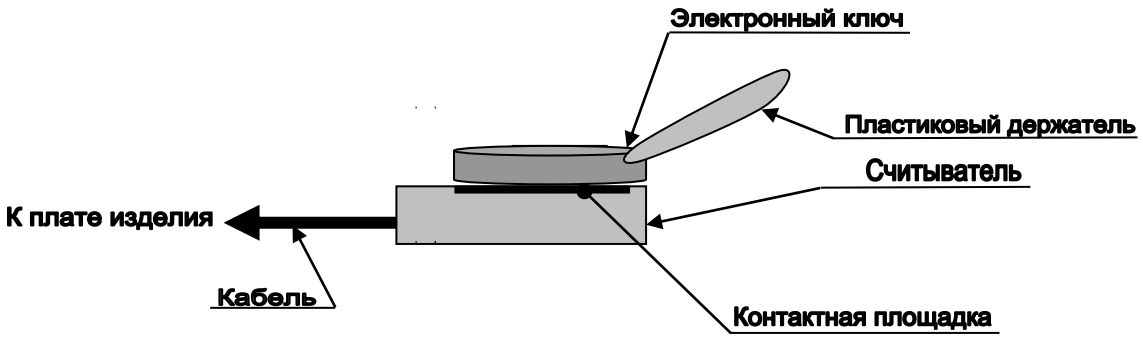


Рисунок Б.1

Б.4.3 Электронный ключ пользователь устанавливает в считыватель, когда на экран монитора выдается сообщение:

**Установите ЭК и нажмите Enter.**

Пользователь должен плотно приложить к считывателю электронный ключ (рисунок Б.1) и нажать клавишу **Enter**, затем на предложение ввести пароль - ввести свой пароль с помощью клавиатуры.

После этих действий доступ к ПЭВМ (запуск ОС) будет разрешен владельцам только тех электронных ключей, которые зарегистрированы на данной ПЭВМ, и при условии неизменности контролируемых объектов (контролируемые объекты определяет администратор СДЗ).

Если электронный ключ неправильно установлен, если в процессе чтения возникли ошибки или система обнаружила нарушения в структуре информации электронного ключа, в статусную строку выдаются соответствующие сообщения об ошибках.

В этом случае следует убедиться, что электронный ключ правильно установлен и затем, после нажатия клавиши **Enter**, повторить попытку ввода информации с электронного ключа. Если ошибка повторится, то необходимо обратиться к администратору СДЗ (администратор СДЗ должен заменить электронный ключ).

В том случае, если длительность процесса аутентификации превышает значение, установленное в плате изделия (120 секунд), то работа изделия будет остановлена и ПЭВМ заблокируется.

## *Перечень принятых сокращений*

| | | |
|---|---|---|
| ВМ | – | виртуальная машина |
| ИН | – | индивидуальный носитель |
| ЛВС | – | локальная вычислительная сеть |
| МИиКДС | – | модуль идентификации и контроля доверенной среды |
| НСД | – | несанкционированный доступ |
| ПАК | – | программно-аппаратный комплекс |
| ПЭВМ | – | персональная электронная вычислительная машина |
| ОС | – | операционная система |
| КП | – | комплекс программ |
| СДЗ | – | средства доверенной загрузки |
| ЭК | – | электронный ключ |

## *Лист регистрации изменений*

| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в документе | Номер документа | Входящий номер сопроводительного документа и дата | Подпись | Дата |
|---|---|---|---|---|---|---|---|---|---|
| | измененных | замененных | новых | аннулированных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |