# Программно-аппаратный комплекс «Горизонт-ВС»

*Руководство пользователя*

МБРЦ.468313.001.ИЗ.01

Листов: 32

Москва 2023

ГОРИЗОНТ-ВС

ЦИФРОВОЕ БУДУЩЕЕ
НАЧИНАЕТСЯ СЕГОДНЯ



| | |
|---|---|
| Почтовый адрес: | 123022, г. Москва,<br>ул. 2-ая Звенигородская, дом<br>13, строение 43, офис 73 |
| Телефон: | +7 (495) 120-15-37 |
| E-mail: | info@gorizont-vs.ru |
| Web: | https://gorizont-vs.ru/about-us.html |

## Аннотация

Настоящее руководство пользователя МБРЦ.468313.001 ИЗ.01 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).

## Содержание

# 1 Введение

## 1.1 Область применения

ПАК «Горизонт-ВС» предназначен для организации взаимодействия пользователей *терминалов*[1] с ресурсами *серверов виртуализации*, объединенных в IP-сеть с использованием технологии «клиент-сервер».

## 1.2 Краткое описание возможностей

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;
- блокировку входа в систему зарегистрированного пользователя при:
  - нарушении целостности контролируемых объектов, входящих в КП;
  - превышении предельного числа неудачных попыток входа и истечении срока действия пароля;
  - 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*;

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

- 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.

В ПАК «Горизонт-ВС» отсутствуют механизмы, направленные на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов. Наличие изолированной среды и полного аудита всех событий в системе исключает возможность создания пользователями каналов, скрытых от систем наблюдения и контроля, обоснование чего приведено в документе «ПАК «Горизонт-ВС». Анализ скрытых каналов МБРЦ.468313.001Д14».

### 1.3 Уровень подготовки персонала

Администраторы СГУ «Горизонт» должны иметь опыт работы с:

- персональным компьютером на уровне квалифицированного пользователя;
- стандартными приложениями на уровне свободного выполнения базовых операций;
- операционными системами:
  - Windows;
  - Unix-подобными ОС.

### 1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Администратору СГУ «Горизонт» необходимо ознакомиться со следующими документами:

- Руководство пользователя. МБРЦ.468313.001.ИЗ.01.

- Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина». МБРЦ.468313.001.ИЗ.02-01;
- Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-сервер». МБРЦ.468313.001.ИЗ.02-02.

# 2 Назначение и условия применения

## 2.1 Назначение системы

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*[2] (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[3], исполняемым на *сервере виртуализации*[4]. На *терминалы* устанавливается компонент «Тонкий клиент» (компонент 1 согласно формуляру МБРЦ.468313.001 ФО) из состава КП «Терминал-Сервер».

---

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

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

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

### 2.2 Условия применения

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 Подготовка к работе

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.*

## 3.1 Аутентификация пользователя

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).

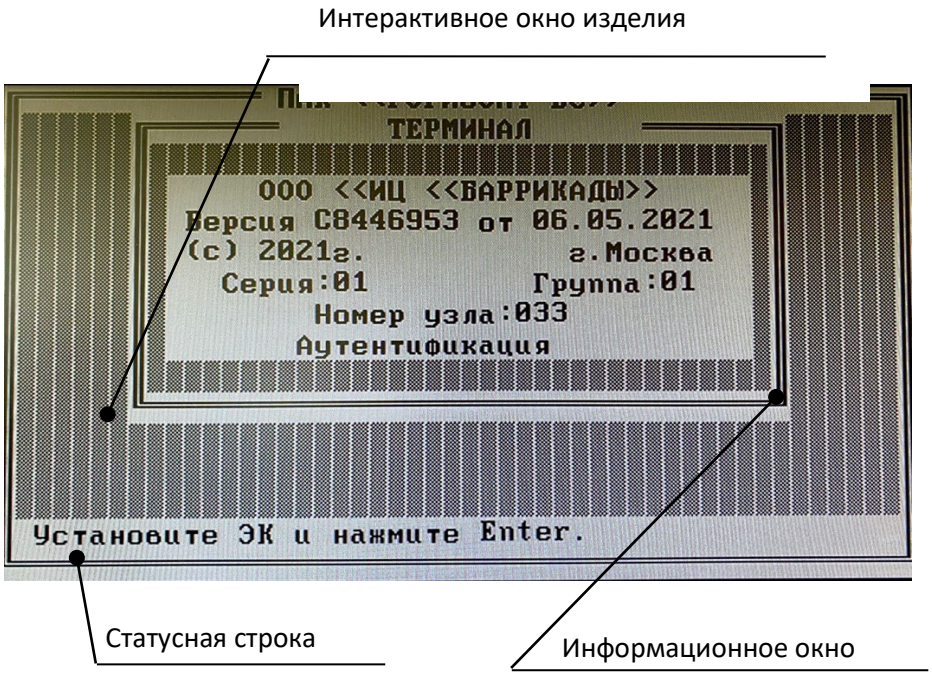


Рисунок 1 – Интерактивное окно

В информационное окно выводится:

- номер узла (номер терминала в АГ);
- номер АГ в глобальной сети;
- серия (учетная информация);
- 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 таблице (Таблица 1).

После включения/перезагрузки терминала в статусной строке сообщение: **Установите ЭК и нажмите Enter**.

**Для аутентификации пользователя**:

1. Установить ЭК аутентификации пользователя в считыватель для электронных ключей (далее по тексту – считыватель). Правила работы с электронным ключом описаны в приложении к данному документу (ПРИЛОЖЕНИЕ А).
2. Нажать клавишу **Enter**.

   В статусной строке появится сообщение: **Введите пароль…** (Рисунок 2).

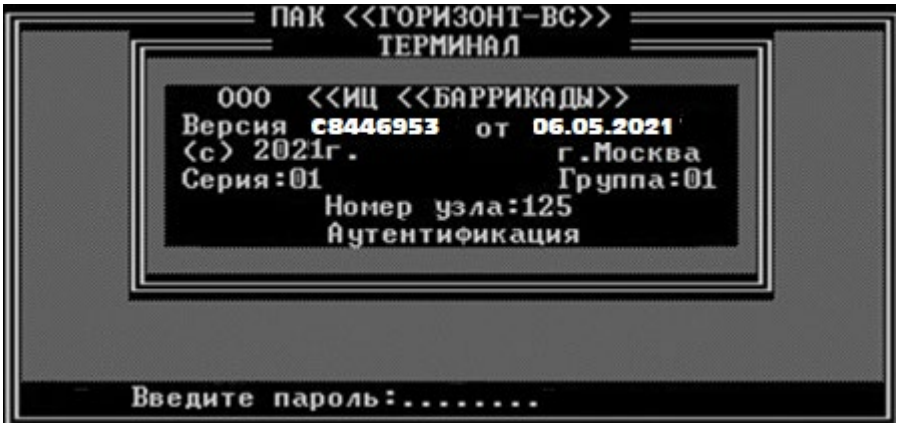


Рисунок 2 – Ввод пароля

3. Введите пароль.

   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 **Back-Space)** и повторить ввод.

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

После корректного ввода пароля в статусной строке появится сообщение: **Ждите. Идет аутентификация**.

4. Дождаться завершения процесса аутентификации.

   После успешной аутентификации появится сообщение **Успешная аутентификация**.

   Список возможных сообщений об ошибках и действий пользователя представлен в таблице (Таблица 1).

   Запустится процесс проверки целостности индивидуального USB-носителя пользователя.

5. Дождаться завершения процесс проверки целостности индивидуального USB-носителя пользователя.

   На экран выводятся окна, подобные представленным на рисунках ниже (Рисунок 3 и Рисунок 4).

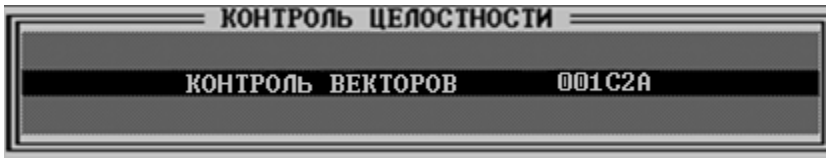


Рисунок 3 – Контроль целостности - режим контроля посекторный

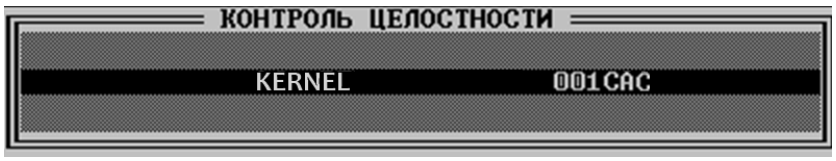


Рисунок 4 – Контроль целостности – режим контроля файловый

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

   При отсутствии ошибок появится сообщение: **Уберите ЭК из считывателя**. Пользователь получит доступ к запуску КП «Терминал-Сервер» и работе в среде ВМ.

   Список возможных ошибок и действий пользователя представлен в таблице (Таблица 1).

6. Перейти к загрузке КП «Терминал-Сервер»:
   а. Нажать клавишу **Enter**.
   б. Извлечь ЭК аутентификации из считывателя.
   в. Нажать клавишу **Enter**.

### 3.2 Контроль времени действия пароля

*Время действия пароля* – это интервал времени, который устанавливается по умолчанию – 90 дней. 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 таблице (Таблица 1).

***Внимание!*** *Пароли пользователей меняются администратором СДЗ один раз в три месяца (90 дней).*

# 4 Описание операций

Тонкий клиент имеет два варианта исполнения:

- исполнение 1 – системный тонкий клиент, поставляемый на USB-накопителе и предназначенный для запуска в качестве общесистемного ПО на терминалах, в том числе и бездисковых рабочих станциях. Работа с ним описывается в п. 4.1;
- исполнение 2 – программный тонкий клиент, предназначенный для запуска в среде операционных систем (ОС) семейства Linux. Работа с ним описывается в п.4.4.

## 4.1 Аутентификация пользователя на терминале

После успешного прохождения процесса аутентификации с помощью МИиКДС «Шина», открывается окно аутентификации на терминале (Рисунок 5).

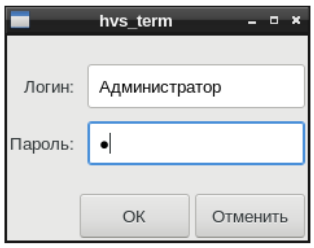


Рисунок 5 – Окно аутентификации

В окне аутентификации необходимо ввести имя пользователя, пароль и нажать кнопку **ОК**.

Если введены неверные данные, то появится сообщение об ошибке (Рисунок 6).

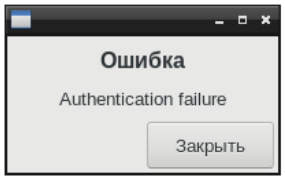


Рисунок 6 – Сообщение об ошибке

После ввода верных имени пользователя и пароля появляется окно работы с программой (Рисунок 7).

### 4.2 Управление брокерами подключения

После аутентификации пользователя на терминале появляется **Панель управления** (Рисунок 7), позволяющая:

- добавлять брокеры (сервисы) ~~подключенийподключения~~;
- удалять брокеры (сервисы);
- назначать брокерам протокол (транспорт).

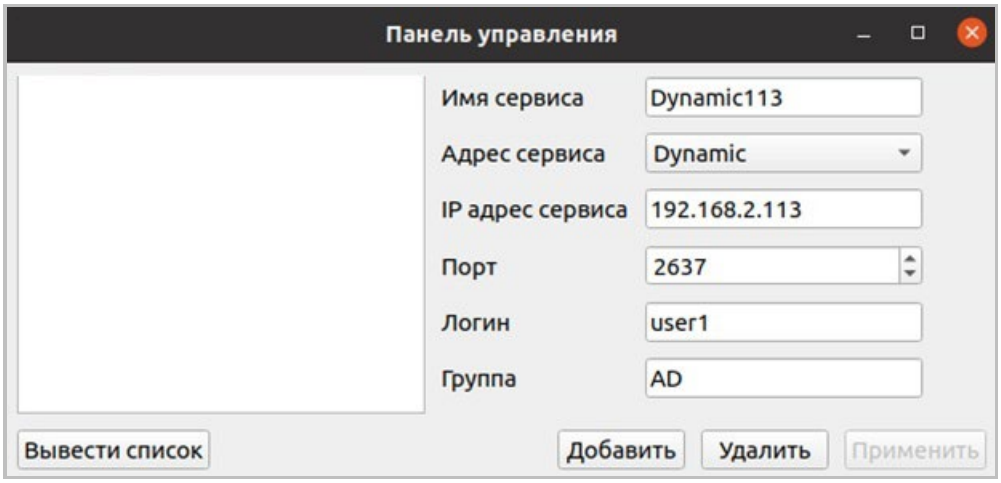


Рисунок 7 – Панель управления пользователями и брокерами подключения

**Для добавления брокера подключений:**

1. Нажать кнопку **Добавить** (Рисунок 7).
2. В поле **Имя сервиса** ввести имя брокера (сервиса).
3. В поле **Адрес сервиса** выбрать значение: **Dynamic** или **Static**.
4. Заполнить поля: **IP адрес сервиса**, **Порт**, **Логин**, **Группа**.

   Станет доступна кнопка **Применить**.
5. Нажать кнопку **Применить**.

   Добавленный брокер отобразится в списке в левой части окна (Рисунок 8).

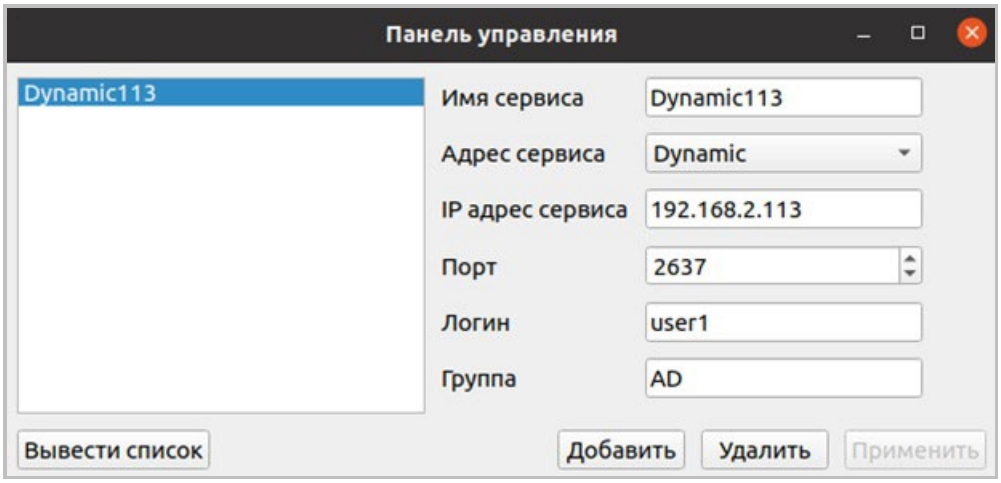


Рисунок 8 – Брокер добавлен в список

6. Выбрать в списке брокеров нужный элемент.
7. Нажать на кнопку **Вывести список.**

   Появится окно ввода пароля пользователя (Рисунок 9).


Рисунок 9 – Окно ввода пароля

8. Ввести пароль и нажать кнопку **ОК**.

   Если все данные указаны верно, в нижней части окна появится список доступных сервисов (Рисунок 10).

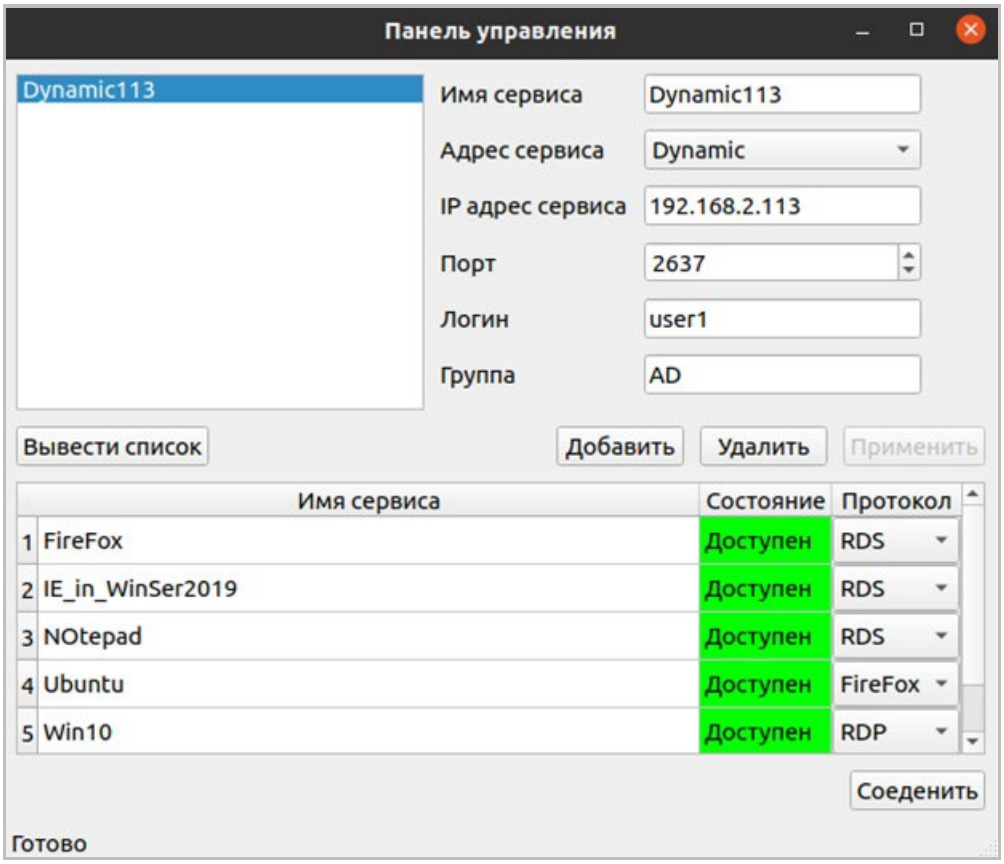


Рисунок 10 – Список доступных брокеров (сервисов)

Таблица брокеров состоит из следующих колонок:

- Имя сервиса;
- Состояние;
- Протокол – позволяет выбрать протокол.

9. При необходимости, выбрать протокол в соответствующей ячейке.
10. Выбрать строку сервиса нажатием.
11. Нажать на кнопку **Соединить** в нижнем правом углу.

Откроется окно рабочего стола.

### 4.3 Загрузка ВМ на терминале

После аутентификации пользователя на терминале появляется окно **выбора ВМ** (Рисунок 11), в котором показаны ВМ, разрешенные администратором СДЗ для данного пользователя.

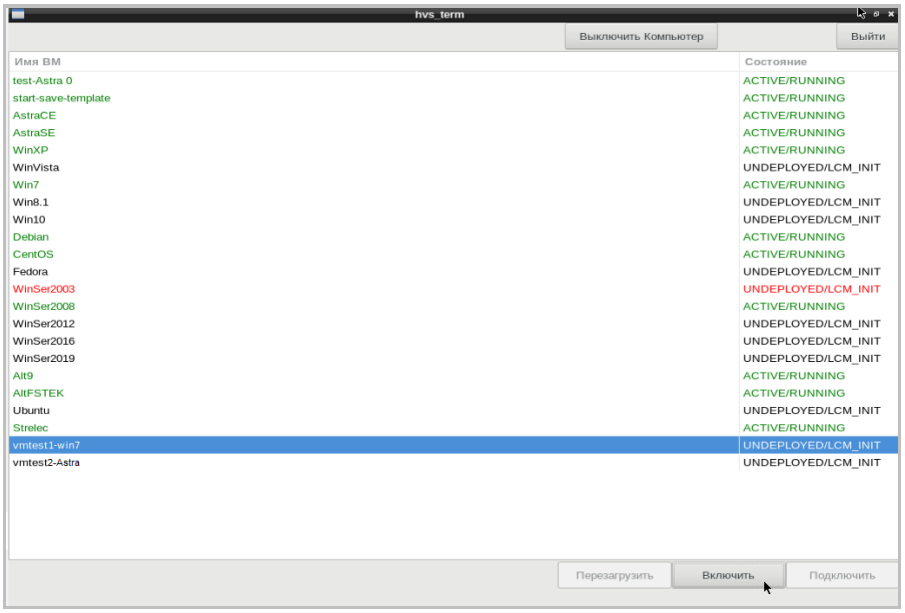


Рисунок 11 – Выбор ВМ

**Для загрузки ВМ:**

1. Выбрать ВМ.
2. Если состояние ВМ **UNDEPLOYED** («Выключен»), нажать кнопку **Включить**.
3. Дождаться, когда состояние ВМ сменится на **ACTIVE/RUNNING** (ВМ запустится на *сервере виртуализации*).
4. Нажать кнопку **Подключить** (Рисунок 12).

   Начнется загрузка операционной системы, установленной на ВМ.

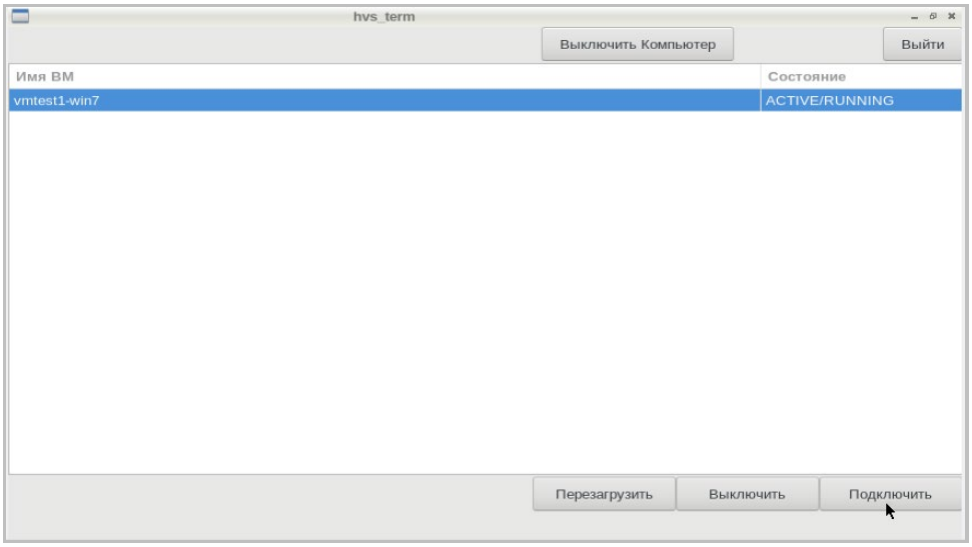


Рисунок 12 – Подключение к ВМ

**Для завершения работы ВМ** нажать кнопку **Выключить** (Рисунок 13).

**Для перезагрузки ВМ** нажать кнопку **Перезагрузить** (Рисунок 13).

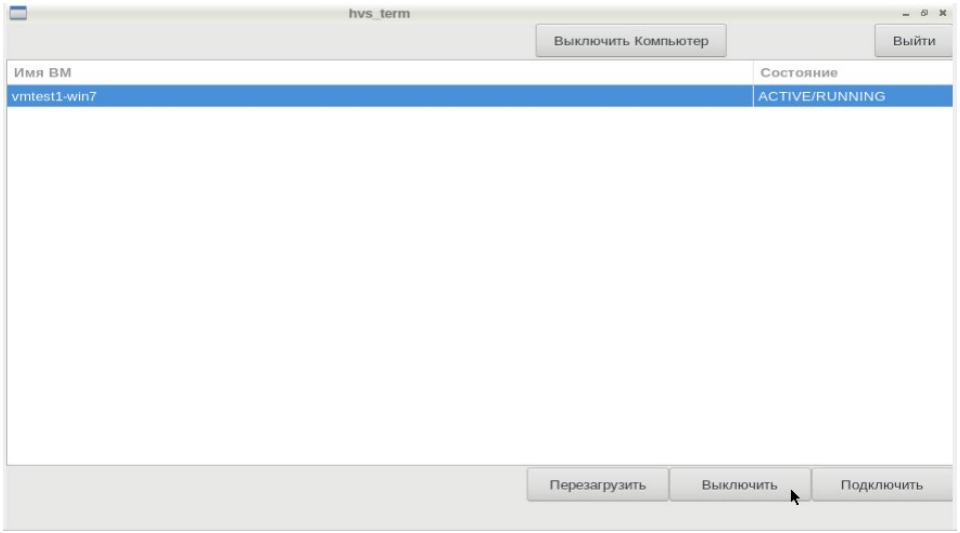


Рисунок 13 – Выключение работающей ВМ

**Для перезагрузки терминала** нажать кнопку **Выключить Компьютер** (13).

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 14).

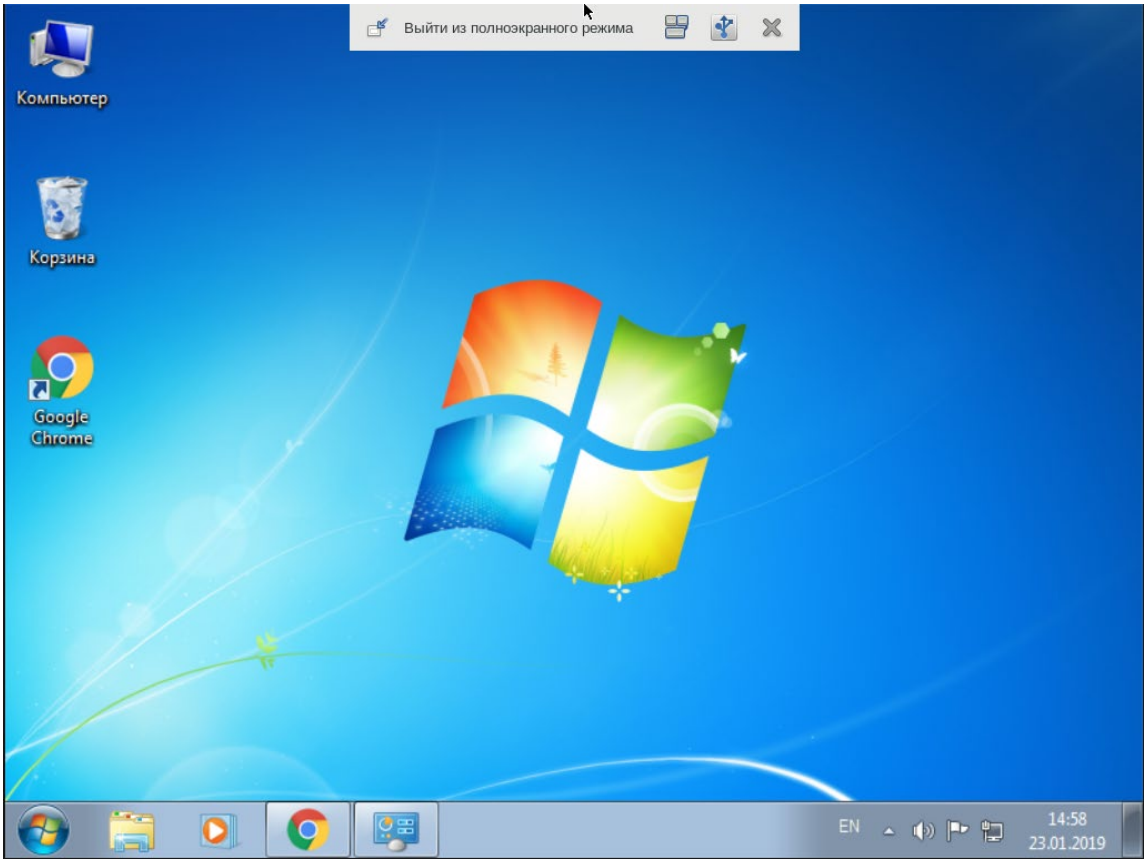


Рисунок 14 – Рабочий стол пользователя ОС Windows 7

Для работы с терминалом предназначено меню, которое появляется при подведении манипулятора типа «мышь» к центру верхнего края экрана (Рисунок 15).

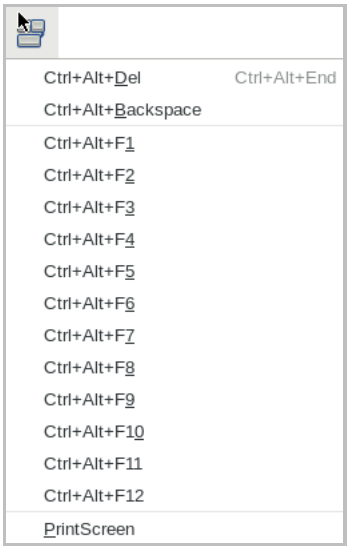


Рисунок 15 – Список комбинаций клавиш

**Для выхода из полноэкранного режима** нажать кнопку **Выход из полноэкранного режима**.

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 отправки в ОС Microsoft Windows 7 некоторую комбинацию клавиш** нажать кнопку меню **Отправить комбинацию клавиш**  и выбрать из раскрывающегося списка нужную комбинацию (Рисунок 15):

- **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.

**Для подключения к терминалу внешних USB-устройств:**

1. Нажать кнопку меню **Выбор устройства USB**  .
2. В появившемся окне (16) отметить флажком нужное USB-устройство для подключения.

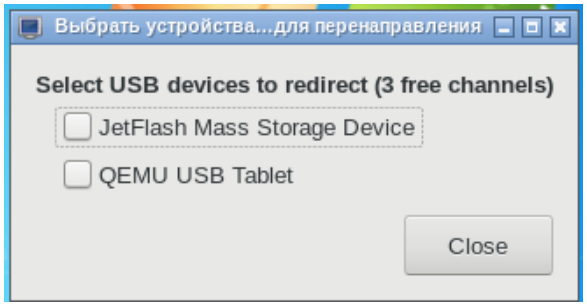


Рисунок 16 – Выбор USB-устройства

3. Нажать кнопку **Close**

***Внимание**! Не зарегистрированные на сервере виртуализации USB-устройства на терминале работать не будут.*

При штатной работе программы никаких сообщений пользователю не выводится.

Если на экране появляются какие-либо сообщения, например, как на рисунке ниже (17), то следует обратиться к администратору СДЗ.

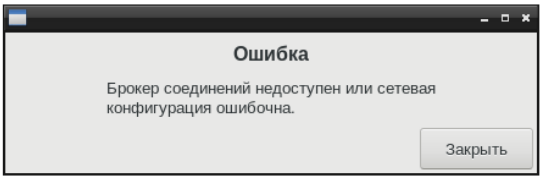


Рисунок 17 – Сообщение о неудачной попытке подключения к *серверу виртуализации*

### 4.4 Загрузка тонкого клиента и подключение ВМ в ОС Linux

**Для запуска КП «Тонкий клиент»** выполнить команду:

```
python3 /usr/bin/hvs-term.py
```

Откроется окно **Тонкий клиент** (Рисунок 18).

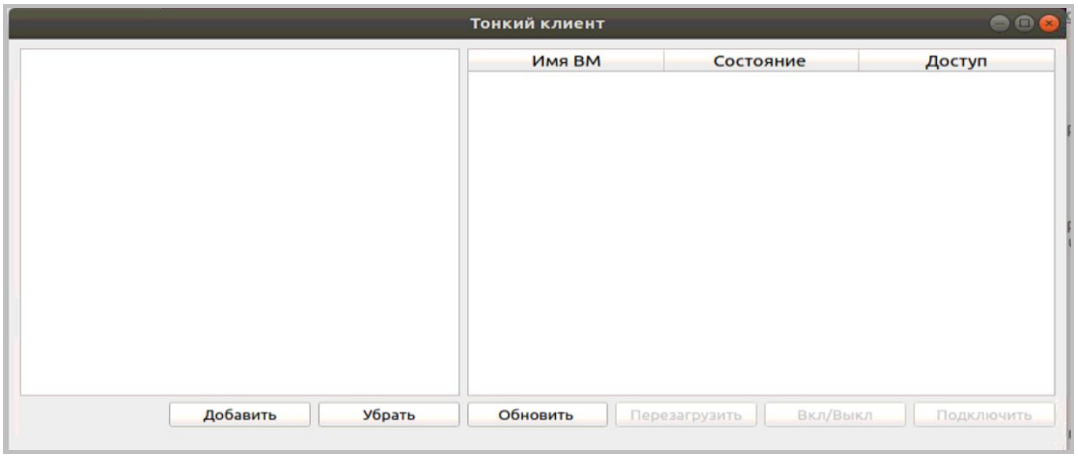


Рисунок 18 – Стартовое окно "Тонкого клиента"

**Для подключения к ВМ:**

1. Нажать кнопку **Добавить**.

   Откроется окно конфигурации соединения (Рисунок 19).

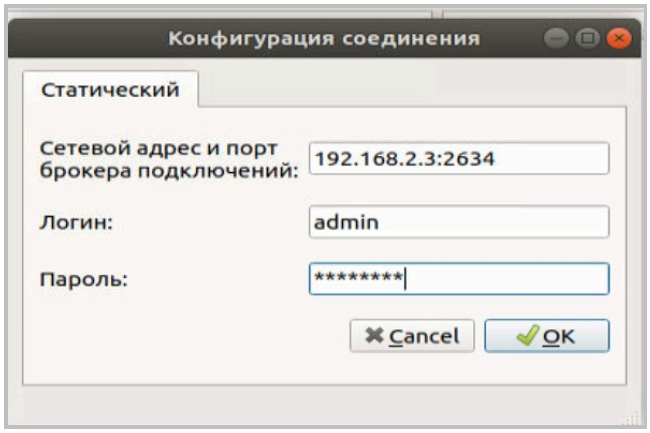


Рисунок 19 – Конфигурация соединения

2. Установить параметры подключений:
   а. В поле **Сетевой адрес и порт брокера подключений** следует ввести: адрес брокера подключений (IP-адрес сервера с установленной СГУ) и порт (по умолчанию порт 2634).
   б. В поля
   в. х **Логин** и **Пароль** ввести аутентификационные данные пользователя.
3. Нажать кнопку **ОК**

   В левую часть окна будет добавлен адрес брокера подключений.

**Для подключения к ВМ:**

1. Выделить из списка адрес брокера.

   В правой части окна **Тонкий клиент** (Рисунок 18) появится список ВМ, разрешенных данному пользователю администратором (Рисунок 20).

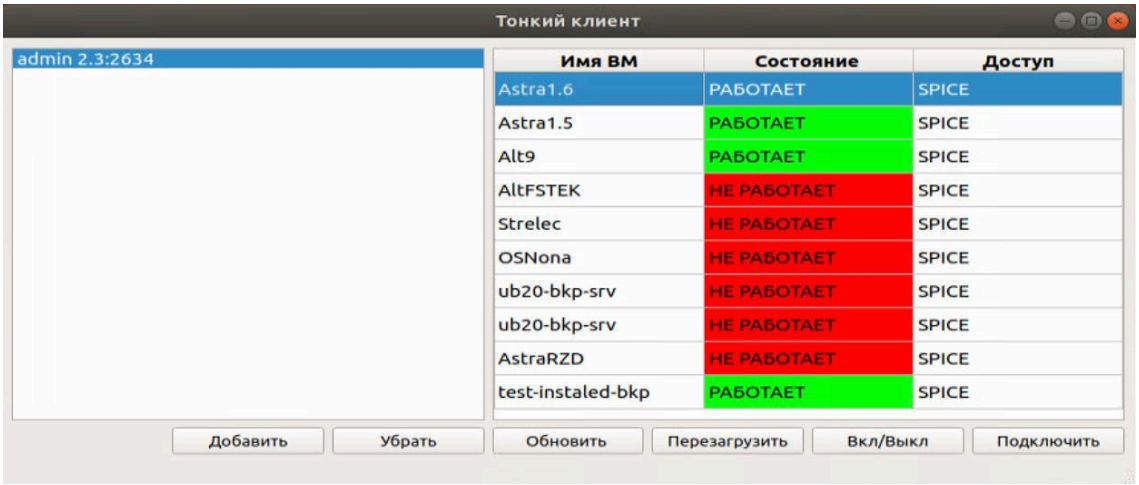


Рисунок 20 – Список ВМ, разрешенных данному пользователю администратором

2. Выбрать ВМ и, если состояние ВМ **НЕ РАБОТАЕТ**, нажать кнопку **Вкл/Выкл**.
3. Дождаться, когда состояние ВМ сменится на **РАБОТАЕТ** (ВМ запустится на *сервере виртуализации*).
4. Нажать кнопку **Подключить** (Рисунок 20).

   Начнется загрузка ОС, установленной на ВМ.

   **Для обновления статусов ВМ** нажать кнопку **Обновить**.

   **Для завершения** работы ВМ нажать кнопку **Вкл/Выкл**.

После успешного запуска ВМ пользователь попадает в среду ОС, установленную на ВМ, исполняемой на *сервере виртуализации*.

### 4.5 Запуск тонкого клиента в среде без графического интерфейса

Для запуска ТК без графического интерфейса:

1. Ввести команды в командной строке:

```
python3
./hvs-term.pyc --no-gui -l <имя_пользователя> -p <пароль> -u <IP-адрес
брокера>:<порт> --view-list
```

2. Нажать клавиши **Enter.**

   В консоли отобразится список доступных ВМ.

   **Для подключения к выбранной ВМ** необходимо ввести:

```
python3
./hvs-term.py -l <имя_пользователя> -p <пароль> -u <IP-адрес
брокера>:<порт> --connect <имя_ВМ>
```

   Можно добавить аргумент:

```
--proxy-port <номер порта прокси>
```

### 4.6 Журнал ошибок

Для просмотра журнала ошибок необходимо перейти в директорию **~/hvs.log или /home/user/hvs.log**.

События в журнале записываются и выводятся в следующем формате:

**ERROR <дата> <время> <код ошибки>**

(например, «ERROR 2019-11-18 13:58:37,974 Ошибка 1: Ошибка запуска ВМ (СГУ)»).

Коды ошибок:

Ошибка 1: Ошибка запуска ВМ (СГУ)

Ошибка 2: Ошибка получения списка ВМ (СГУ)

Ошибка 3: Ошибка запуска ВМ (HDC – Horizon Dynamic Client)

Ошибка 4: Ошибка соединения с брокером (HDC)

Ошибка 5: Ошибка логина СГУ (неверный логин/ пароль)

Ошибка 6: Ошибка соединения с брокером (СГУ)

# 5 Аварийные ситуации

## 5.1 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.*

## 5.2 Сообщения при аутентификации и действия пользователя

Перечень сообщений, выдаваемых в статусной строке во время аутентификации пользователя, и необходимые действия, приведены в таблице ниже (Таблица 1).

Таблица 1 – Перечень сообщений, выдаваемых в статусной строке при аутентификации пользователя

| Сообщение | Тип сообщения | Пояснения | Действия пользователя |
|---|---|---|---|
| Введите пароль: ..... | И | | Ввести пароль из 8 символов |
| Ждите. Идет аутентификация | И | | Ждать завершения процесса аутентификации |
| Истекло время аутентификации | О | Превышено время аутентификации | Перезагрузить терминал |
| Истекает срок действия пароля | И | | Сменить пароль |
| Неправильный пароль или ЭК | О | | Установить правильный ЭК или ввести правильный пароль |
| Ошибка при загрузке изделия | С | Сбой изделия | При многократных сообщениях изделие считать неисправным |
| Ошибка при КОНТРОЛЕ ВЕКТОРОВ | О | В процессе контроля целостности индивидуального USB-носителя была обнаружена ошибка | Нажать клавишу Enter для продолжения работы |

| Сообщение | Тип сообщения | Пояснения | Действия пользователя |
|---|---|---|---|
| Пользователь заблокирован | И | Вход пользователя заблокирован администратором в списке пользователей изделия | Обратиться к администратору |
| Превышено число попыток входа | И | Количество неудачных попыток входа пользователя больше 10 | Обратиться к администратору |
| РАБОТА ИЗДЕЛИЯ ОСТАНОВЛЕНА | И | После трех попыток ввода пароля процесс аутентификации закончился неудачно | Перезагрузить терминал |
| | | Произведено подряд 8 неудачных попыток входа или общее число неудачных попыток входа превысило значение 10.Произошло блокирование его ЭК в изделии, и дальнейшая работа данного пользователя на данном терминале будет невозможна | |
| Сбой при чтении ЭК | О/С | 1 Вставлен неверный тип ЭК.<br>2 Сбой изделия | |
| Срок действия пароля истек | И | Пользователь блокируется системой защиты | Сменить пароль |
| Успешная аутентификация | И | Аутентификация прошла успешно | |
| ЭК не установлен | О | Сбой изделия | Проверить ЭК и/или считыватель |
| Уберите ЭК из считывателя | И | Аутентификация прошла успешно. Получен доступ к терминалу | Приступить к загрузке терминала |

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

## А.1 Назначение электронного ключа

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

## А.2 Технические характеристики электронного ключа

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

Характеристики:

- 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.

## А.3 Особенности работы с электронным ключом DS1995

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

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.

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.

### А.4 Порядок работы с электронным ключом DS1995

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

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 21).

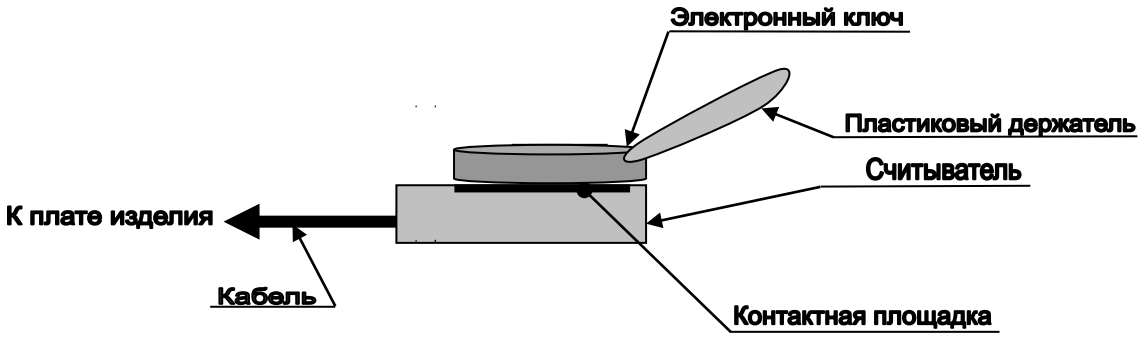


Рисунок 21 – Доступ к данным при касании электронным ключом к контактной площадке считывателя

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 21) 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

| Сокращение | Расшифровка |
|---|---|
| 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 | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |