Руководство пользователя

Программный комплекс электронный замок Витязь

ВЕРСИЯ 2.2

АННОТАЦИЯ

Настоящий документ предназначен для ознакомления пользователя с программным комплексом электронный замок «Витязь» версии 2.2 (далее по тексту ПК ЭЗ «Витязь» В2.2). Содержит описание применения ПК ЭЗ «Витязь» В2.2, который поставляется в предустановленном виде системного программного обеспечения материнских плат.

В документе содержится информация о назначении, функциональных особенностях, работе с ПК ЭЗ «Витязь» В2.2, приводятся информационные сообщения, сообщения об ошибках ЭЗ и способы их устранения.

Данное руководство ориентировано для подготовленных пользователей.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Термин
BIOS	Basic Input/Output System – базовая система ввода-вывода
EXT	Extended File System – расширенная файловая система
FAT	File Allocation Table – тип файловой системы
KSS	Оболочка Kraftway Secure Shell
NTFS	New Technology File System – файловая система новой технологии
Smart Card CCID	Smart Card Integrated Circuit(s) Cards Interface Devices – стандартизированный тип интерфейса для считывателя смарткард
SPI Flash	Микросхема памяти для хранения внутреннего ПО материнской платы
TokenID	Уникальный серийный номер АН
UEFI	Unified Extensible Firmware Interface – интерфейс между операционной системой и программным обеспечением, управляющим низкоуровневыми функциями оборудования
USB	Universal Serial Bus – универсальная последовательная шина
АН	Аутентифицирующий носитель
КД	Конструкторская документация
КСЗ	Комплекс средств защиты
КЦ	Контроль целостности
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
Пароль	PIN-код
ПК ЭЗ «Витязь» В2.2	Программный комплекс электронный замок Витязь В2.2
ПМДЗ	Программный модуль доверенной загрузки
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
РД	Руководящий документ
СДЗ	Средство доверенной загрузки
СЗИ	Средства защиты информации

Сокращение	Термин
ТУ	Технические условия
УЦ	Удостоверяющий центр
ФС	Файловая система
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЭД	Эксплуатационная документация
ЭЗ	Электронный замок

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение ПО

ПК ЭЗ «Витязь» В2.2 является программным средством доверенной загрузки, соответствующим 2 классу защиты, уровня базовой системы ввода-вывода со встроенным средством антивирусной защиты и предназначен для использования в автоматизированных системах обработки информации, содержащей сведения, составляющие государственную тайну, а также в государственных информационных системах и в информационных системах персональных данных всех классов и уровней защищенности.

Программный комплекс электронный замок «Витязь» версии 2.2 (далее по тексту ПК ЭЗ «Витязь» В2.2) предназначен для обеспечения нейтрализации следующих основных угроз безопасности информации:

1) Для самого средства доверенной загрузки:

– нарушение целостности программного обеспечения средства доверенной загрузки;

– отключение и (или) обход нарушителями компонентов средства доверенной загрузки;

– несанкционированное изменение конфигурации (параметров) средства доверенной загрузки;

– преодоление или обход функций безопасности средства доверенной загрузки;

– несанкционированное внесение изменений в логику функционирования средства доверенной загрузки, в том числе за счет получения остаточной информации средства доверенной загрузки из памяти средства вычислительной техники и (или) получение доступа к ресурсам средства доверенной загрузки из программной среды средства вычислительной техники после завершения работы средства доверенной загрузки;

– сбои и ошибки в процессе функционирования средства доверенной загрузки.

2) Для средства вычислительной техники:

– несанкционированный доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;

– несанкционированную загрузку штатной операционной системы и получение несанкционированного доступа к информации;

– нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе.

ПК ЭЗ «Витязь» В2.2 является средством доверенной загрузки уровня базовой системы ввода-вывода и осуществляет:

– блокирование попыток несанкционированной загрузки нештатной операционной системы;

– контроль доступа пользователей к процессу загрузки операционной системы;

– контроль целостности программного обеспечения и среды функционирования.

ПК ЭЗ «Витязь» В2.2 встраивается в базовую систему ввода-вывода, что обеспечивает невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и ПК ЭЗ «Витязь» В2.2 путем реализации следующих процессов:

– получение управления в процессе выполнения базовой системы ввода-вывода до передачи управления для загрузки операционной системы с машинного носителя информации;

– самотестирование средства доверенной загрузки;

– аутентификация пользователя с использованием портов ввода-вывода средства вычислительной техники;

– контроль целостности среды функционирования (программной среды и элементов аппаратного обеспечения средства вычислительной техники);

– продолжение выполнения базовой системы ввода-вывода с последующей загрузкой операционной системы в случае положительной аутентификации пользователя;

– блокировка загрузки в случае превышения неудачных попыток аутентификации пользователя или попытки загрузки нештатной операционной системы;

– регистрация событий безопасности и запись информации аудита в выделенную область памяти.

1.2 Функции ПО

ПК ЭЗ «Витязь» В2.2 обеспечивает:

1) Разграничение доступа:

– к управлению СДЗ;

– к управлению работой СДЗ;

– к управлению параметрами СДЗ;

2) Аутентификацию с выбором способа аутентификации:

– аутентифицирующий носитель;

– цифровой сертификат;

3) Контроль целостности:

– электронного замка;

– базы данных ЭЗ при каждом старте ПК;

– компонентов компьютера;

– программной среды;

4) Блокирование загрузки операционной системы ЭЗ;

5) Управление доступом к ресурсам компьютера;

6) Аудит безопасности и регистрацию событий в общем журнале событий;

7) Управление журналом аудита;

8) Запрет загрузки ОС с внешних USB;

9) Антивирусную проверку критически важных областей и папок, до загрузки ОС:

– обнаружение зараженных вредоносными компьютерными программами (вирусами) объектов;

– отображение сигнала тревоги при обнаружении вредоносных компьютерных программ (вирусов);

– получение и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

10) Обеспечение безопасности после завершения работы СДЗ.

1.3 Основные характеристики

1.3.1 Состав ЭЗ

ПК ЭЗ «Витязь» В2.2 включает в себя следующие программные модули:

– модуль обеспечивающий основные функции комплекса и взаимодействие с АН для обеспечения двухфакторной аутентификации до загрузки ОС;

– модуль выполняющий выгрузку журнала регистрации событий и отчёта о состоянии ЭЗ;

– модуль для работы с сертификатами УЦ, которые используются для проверки на подлинность сертификатов пользователей при прохождении ими процедуры аутентификации в ЭЗ;

– модуль для формирования списков файлов и контрольных сумм (КС) файлов, выбранных для контроля целостности, а также для вывода результатов проверки КЦ;

– модуль для формирования списков оборудования и контрольных сумм (КС) оборудования для контроля целостности, а также для вывода результатов проверки КЦ;

– модуль для формирования общего журнала событий (ЖС) о программных и аппаратных событиях. Модуль сохраняет события от различных источников в едином журнале событий. Программа просмотра событий позволяет уполномоченному администратору просматривать журнал событий. Программный интерфейс (API) позволяет приложениям записывать в журнал информацию и просматривать существующие записи.

1.4 Ограничения, накладываемые на область применения программы

Ограничений со стороны модуля ЭЗ на аппаратную часть нет. Единственное ограничение – поддерживаемые файловые системы.

ПК ЭЗ «Витязь» версии 2.2 поддерживает следующие файловые системы: FAT16, FAT32, NTFS, ext, ext2, ext3, ext4.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к программному обеспечению

Для функционирования ЭЗ требуется специализированная версия UEFI, которая должна удовлетворять следующим условиям:

– наличие программного кода, обеспечивающего вызов ЭЗ до этапа поиска загрузчика операционной системы компьютера;

– наличие программного кода, пользовательского интерфейса и интерфейсов взаимодействия с ЭЗ (оболочка Kraftway Secure Shell – KSS), которые обеспечивают его интерфейс включения/выключения, очистку содержимого хранилища профилей пользователей и журнала ЭЗ, получение после аутентификации пользователя информации о роли пользователя из ЭЗ с целью обеспечения доступа администратора к настройкам ЭЗ и блокирования такого доступа для пользователя.

Программный модуль формирования списка объектов, целостность которых будет контролироваться ЭЗ, может применяться со следующими файловыми системами:

- FAT16;
- FAT32;
- NTFS (New Technology File System);
- ext, ext2, ext3, ext4 (Extended File System).

2.2 Требования к аппаратному обеспечению

Для работы ЭЗ необходима материнская плата с поддержкой UEFI 2.3.1 или с поддержкой UEFI более поздней версии. Обязательным параметром материнской платы является наличие микросхемы SPI Flash с объемом свободной памяти не менее 1 Мб, которая требуется для работы ЭЗ.

Для хранения настроечной информации и баз данных ЭЗ может использоваться внешнее сертифицированное энергонезависимое защищенное хранилище.

В зависимости от количества объектов, целостность которых будет контролироваться ЭЗ, для хранения списка объектов требуется хранилище размером не менее 256 Кбайт.

ПК ЭЗ «Витязь» взаимодействует с аутентифицирующим носителем () для обеспечения двухфакторной аутентификации, в качестве которых выступают сертифицированные USB-ключи или смарт-карты.

Допускается применять только электронные ключи, прошедшие контроль соответствия требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (Гостехкомиссия России, 1999)», сертифицированные для применения в UEFI.

Для работы с АН, в качестве которого выступает USB-ключ, требуется один свободный USB-порт. Для работы с АН, в качестве которого выступает смарт-карта, необходим один свободный USB-порт, наличие считывателя смарт-карт, соответствующего Smart Card CCID спецификации.

2.3 Организационные меры

2.3.1 Правила работы пользователя с АН

Пользователь обязан соблюдать следующие правила работы с АН:

1) после получения АН заменить установленный в нем PIN-код к АН для защиты доступа к компьютеру;
2) своевременно заменять PIN-код к АН в соответствии с политикой безопасности организации;
3) при вводе PIN-кода к АН исключать возможность визуального просмотра его набора другими лицами;
4) не передавать АН, находящийся в распоряжении пользователя, другим лицам, а также не оставлять его без присмотра. Попадание АН в чужие руки несет опасность его компрометации;
5) не сообщать PIN-код к АН другим лицам, хранить записанные PIN-коды в недоступном для других лиц месте. Разглашение PIN-кода означает его компрометацию;
6) при утере АН немедленно сообщить об этом администратору;
7) беречь АН от механических повреждений;

8) не отсоединять АН от рабочей станции во время работы с использующими его приложениями. Перед отсоединением АН от рабочей станции следует завершить работу всех приложений, использующих АН.

2.3.2 Организационно-технические меры

Должны быть приняты организационные (организационно-технические) меры, исключающие неконтролируемый доступ посторонних лиц к компьютерам пользователей в нерабочее время, а также в рабочее время при отсутствии пользователей. Более подробные сведения об организационно-технических мерах приведены в документе «Программный комплекс электронный замок «Витязь» версия 2.2. Описание применения» (643.18184162.00006-2.2 31).

3 РАБОТА С ЭЗ

Для большей наглядности, при описании последовательностей действий, названия кнопок приводятся в квадратных скобках [ ], а активация или нажатие на них обозначается стрелкой →, название страниц оболочки KSS и различных параметров приводится курсивом, например, на странице *Электронный замок “Витязь”*, значения параметров – в кавычках («»).

3.1 Список операций пользователя

Операции, выполняемые пользователем при работе с ПК ЭЗ «Витязь» В2.2:

1) прохождение аутентификации в ЭЗ;
2) изменение пароля пользователя;
3) вывод детальной информации о пользователе;
4) выполнение загрузки операционной системы.

3.2 Ограничения действий пользователя в ЭЗ

Ограничения, накладываемые на пользователя настройками ЭЗ:

1) максимальное допустимое количество последовательных подключений (путем перебора) АН пользователя к USB-порту;
2) минимальное количество знаков пароля (минимальное 4);
3) количество попыток ввода пароля от 1 – до 4;
4) временное ограничение на ввод пароля;
5) запрет загрузки с внешних USB устройств.

Случаи блокировки ЭЗ дальнейшей загрузки компьютера при нарушении целостности (требуют вмешательства администратора):

1) ЭЗ;
2) файловой системы;
3) оборудования;
4) системного блока.

3.3 Аутентификация в ЭЗ

Для загрузки компьютера необходимо пройти аутентификацию в ЭЗ.

В ПК ЭЗ «Витязь» В2.2 реализовано три способа аутентификации: по электронному ключу, по цифровому сертификату, по цифровому сертификату и электронному ключу.

Аутентификация пользователей проводится посредством предъявления АН на этапе загрузки компьютера.

Одному пользователю соответствует одно АН.

При выборе одного из следующих способов аутентификации: по электронному ключу, по цифровому сертификату и электронному ключу, выполняется проверка наличия серийного номера АН в БД ЭЗ, в которой хранятся серийные номера АН, зарегистрированные ранее в БД.

Занесение серийного номера АН в БД ЭЗ выполняется администратором на этапе создания профиля нового пользователя. При выборе способа аутентификации только по цифровому сертификату данная проверка не выполняется.

В ПК ЭЗ «Витязь» В2.2 реализовано три варианта аутентификации: по PIN-коду к АН, по ключевому полю цифрового сертификата пользователя, по PIN-коду к АН и ключевому полю цифрового сертификата пользователя.

1) При первом варианте аутентификация пользователя осуществляется посредством предъявления PIN-кода к АН, который является паролем пользователя. Количество попыток ввода пароля пользователя ограничивается политикой безопасности организации.

2) При втором варианте аутентификация пользователя осуществляется посредством предъявления PIN-кода к АН, выбора значения ключевого поля цифрового сертификата пользователя и проверки наличия данного значения ключевого поля в БД ЭЗ, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы администратором профили пользователей в ЭЗ. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

3) При третьем варианте аутентификация пользователя осуществляется посредством предъявления PIN-кода к АН, выбора значения ключевого поля цифрового сертификата пользователя и проверки наличия данного значения ключевого поля в БД ЭЗ, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы администратором профили пользователей в ЭЗ. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

Если условия успешной аутентификации не выполнены, дальнейшая загрузка компьютера невозможна.

Далее по тексту приводятся описания прохождения процедуры аутентификации, которые отражают действия пользователя при различных способах аутентификации в ЭЗ.

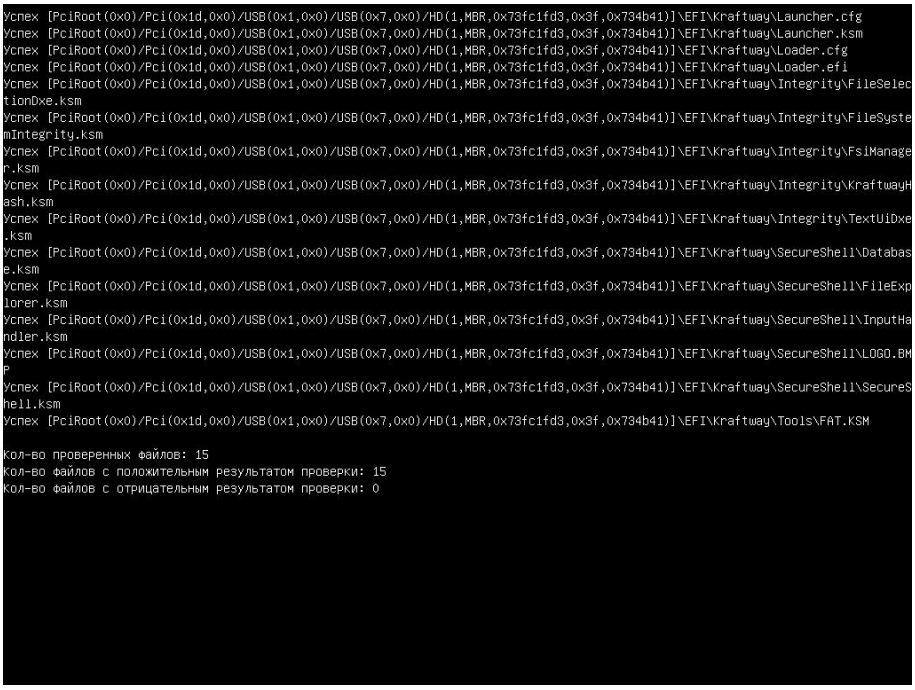
3.3.1 Прохождение аутентификации (вариант 1)

В данном пункте описывается прохождение аутентификации пользователем при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Электронный ключ», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ).

Для прохождения аутентификации следует:

1) включите персональный компьютер, после выполнения данного действия на экране монитора отображается Logo-изображение материнской платы компьютера (см. рисунок 3.1), после отображения Logo-изображения на экран выводится процесс КЦ объектов модулями ЭЗ (см. рисунок 3.2);

Рисунок 3.1 – Logo-изображение материнской платы компьютера



```
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Launcher.cfg
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Launcher.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Loader.cfg
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Loader.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FileSelec
tionDxe.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FileSyste
mIntegrity.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FsiManage
r.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\KraftwayH
ash.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\TextUiDxe
.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\Databas
e.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\FileExp
lorer.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\InputHa
ndler.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\LOGO.BM
P
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\SecureS
hell.ksm
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Tools\FAT.KSM

Кол-во проверенных файлов: 15
Кол-во файлов с положительным результатом проверки: 15
Кол-во файлов с отрицательным результатом проверки: 0
```

Рисунок 3.2 – Процесс проверки КЦ Модулями ЭЗ

Примечания.

1. Процесс КЦ выполняется если администратором предварительно включены соответствующие модули КЦ:

– Модуль КЦ файловой системы;

– Модуль КЦ оборудования;

– Модуль КЦ системного блока.

2. Во время выполнения процедуры КЦ на экран выводится информация о ходе проверки и итоговая информация о результатах проверки.

3. Результат может быть, как с положительным результатом, так и с отрицательным результатом, в этом случае дальнейшие действия пользователя будут заблокированы. При появлении информации о нарушении КЦ обратитесь к Администратору.

2) после окончания процесса КЦ объектов пользователю предлагается подключить АН к свободному USB-порту персонального компьютера (см. рисунок 3.3);

Рисунок 3.3 – Страница *Локальная аутентификация* (вид 1), приглашение на подключение АН

3) подключите АН к свободному USB-порту персонального компьютера;

4) после аутентификации пользователя по АН появится окно для ввода пароля (см. рисунок 3.4);

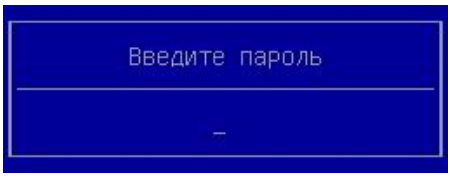


Рисунок 3.4 – Приглашение для ввода пароля пользователя

5) введите пароль пользователя (время на ввод пароля ограничено настройками ЭЗ),

6) → [Enter] на клавиатуре;

7) в случае успешной аутентификации откроется окно выбора дальнейших действий пользователя. Пользователю предлагается (см. рисунок 3.5):

1. дождаться загрузки ОС;
2. → [F1] войти в оболочку Kraftway Secure Shell (KSS).

Рисунок 3.5 – Окно выбора загрузки ОС / KSS

Примечания.

1. Процесс аутентификации пользователя выполняется после включения администратором модуля безопасности *Электронный замок “Витязь”*.

2. Время задержки для действия по входу в KSS задано в настройках ЭЗ.

3.3.2 Прохождение аутентификации (вариант 2)

В данном пункте описывается прохождение аутентификации пользователем при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Общее имя (CN)», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ).

Для прохождения аутентификации следует:

1) включить персональный компьютер, после выполнения данного действия на экране монитора отображается Logo-изображение материнской платы компьютера (см. рисунок 3.1), после отображения Logo-изображения на экран выводится процесс контроля целостности объектов (КЦ) (см. рисунок 3.2);

Примечания.

1. Процесс КЦ выполняется если администратором предварительно включены соответствующие модули КЦ:

– Модуль КЦ файловой системы;

– Модуль КЦ оборудования;

– Модуль КЦ системного блока.

2. Во время выполнения процедуры КЦ на экран выводится информация о ходе проверки и итоговая информация о результатах проверки.

3. Результат проверки может быть, как с положительным результатом, так и с отрицательным результатом, в этом случае дальнейшие действия пользователя будут заблокированы. При появлении информации о нарушении КЦ обратитесь к Администратору.

2) после окончания процесса КЦ объектов пользователю предлагается подключить АН к свободному USB-порту персонального компьютера (см. рисунок 3.3);

3) подключить АН к свободному USB-порту персонального компьютера;

4) после аутентификации пользователя по АН ему предлагается ввести пароль (см. рисунок 3.4);

Примечание. Несмотря на то, что в настройках ЭЗ администратором был выбран способ аутентификации по цифровому сертификату, пользователю предлагается ввести пароль, т.е. PIN-код к АН. Связано это с тем, что сертификат пользователя, по которому выполняется аутентификация пользователя в ЭЗ, размещён в защищённой области АН, доступ к которой, и соответственно к сертификату, осуществляется только после ввода пароля пользователя.

5) ввести пароль пользователя;

6) → [Enter] на клавиатуре, после выполнения данного действия осуществляется поиск сертификатов пользователей, расположенных на АН, во время поиска сертификатов на экран выводится окно следующего вида (см. рисунок 3.6);

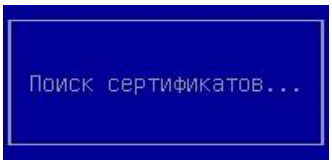


Рисунок 3.6 – Окно, информирующее о поиске сертификатов пользователей

7) после завершения поиска сертификатов пользователю предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов на странице *Локальная аутентификация* (см. рисунок 3.7);

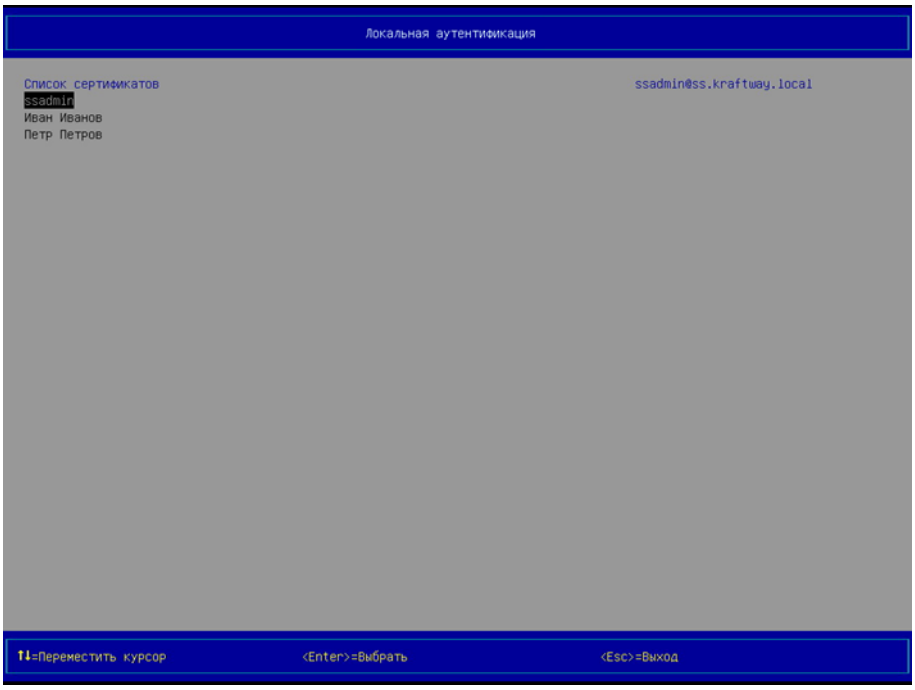


Рисунок 3.7 – Страница *Локальная аутентификация* (вид 2), выбор значения ключевого поля *Общее имя (CN)* сертификатов пользователя

8) выбрать значение ключевого поля *Общее имя (CN)* из списка на странице *Локальная аутентификация*;

9) → [Enter] на клавиатуре, после выполнения данного действия и успешной аутентификации пользователю предлагается дождаться загрузки ОС или войти в оболочку Kraftway Secure Shell (см. рисунок 3.5).

Примечания:

1. Процесс аутентификации пользователя выполняется после включения администратором модуля безопасности *Электронный замок “Витязь”*.

2. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ) – после завершения поиска сертификатов пользователю предлагается выбрать универсальное имя из списка (см. рисунок 3.8).

Рисунок 3.8 – Страница *Локальная аутентификация* (вид 3), выбор универсального имени сертификата

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ) – после завершения поиска сертификатов пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. рисунок 3.9).

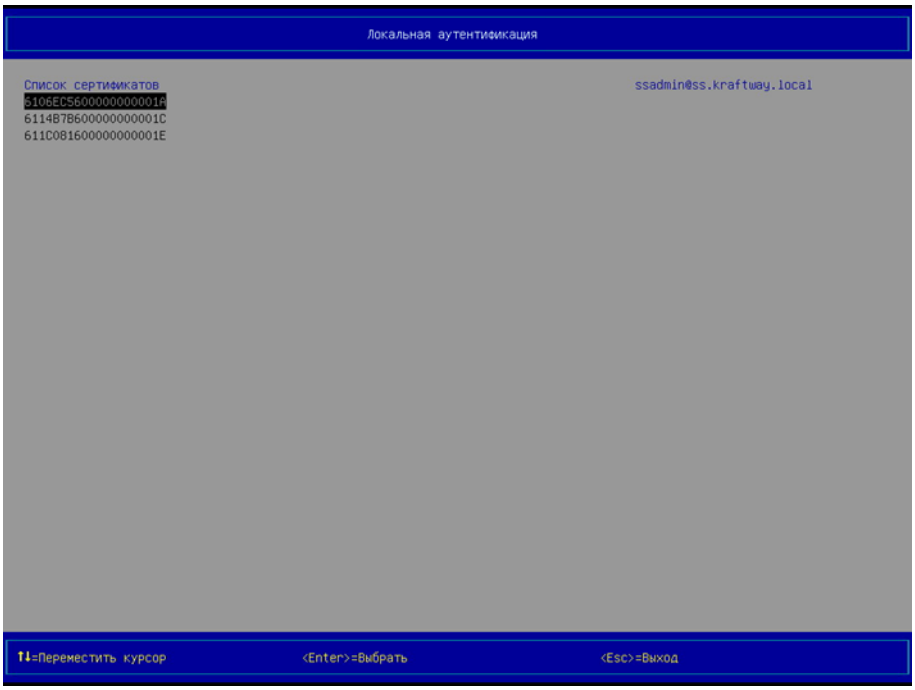


Рисунок 3.9 – Страница *Локальная аутентификация* (вид 4), выбор серийного номера сертификата

3.3.3 Прохождение аутентификации (вариант 3)

В данном пункте описывается прохождение аутентификации пользователем при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ).

Для прохождения аутентификации следует выполнить действия, описанные в пункте 3.3.2.

Примечания:

1. Процесс аутентификации пользователя выполняется после включения администратором модуля безопасности *Электронный замок “Витязь”*.

2. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Универсальное имя (UPN)», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ) – после заверше-

ния поиска сертификатов пользователю предлагается выбрать универсальное имя из списка (см. рисунок 3.8).

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Серийный номер сертификата», *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов, подлежащих контролю целостности (КЦ) – после завершения поиска сертификатов пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. рисунок 3.9).

3.3.4 Дополнительные сведения о процедуре аутентификации в ЭЗ

Если ранее в ЭЗ администратором был добавлен сертификат удостоверяющего центра (УЦ), если аутентификация пользователя выполняется либо по цифровому сертификату, либо по цифровому сертификату и электронному ключу, то во время аутентификации пользователя осуществляется проверка сертификата пользователя на подлинность. Если результат проверки на подлинность отрицательный, то пользователь не сможет пройти процедуру аутентификации с положительным результатом. Если результат проверки на подлинность положительный, то пользователю предлагается дождаться загрузки ОС или войти в оболочку Kraftway Secure Shell (см. рисунок 3.5).

3.4 Вход в оболочку Kraftway Secure Shell

Оболочка Kraftway Secure Shell (далее по тексту оболочка KSS, KSS) предоставляет пользователю выполнить следующие действия: изменение пароля пользователя, вывод детальной информации о пользователе (о своём профиле пользователя).

Для входа в оболочку KSS следует:

1) пройти процедуры аутентификации в ЭЗ (см. п. 3.3);

2) → [F1] на клавиатуре для входа в KSS, после выполнения данного действия на экран выводится страница Kraftway Secure Shell (см. рисунок 3.10);

Рисунок 3.10 – Страница *Kraftway Secure Shell*,
Главное меню оболочки

Примечание. Если ранее администратором не было выполнено никаких настроек в ЭЗ, то сразу же после отображения Logo-изображения материнской платы (см. рисунок 3.1) пользователю предлагается дождаться загрузки ОС или войти в оболочку Kraftway Secure Shell (см. рисунок 3.5).

3.5 Описание интерфейса оболочки Kraftway Secure Shell

Интерфейс оболочки KSS, представленный на рисунке 3.11, состоит из следующих элементов: область № 1 для отображения названия пункта/подпункта меню, область № 2 для отображения пунктов/подпунктов меню, дополнительной или справочной информации, область № 3 подсказок для отображения подсказок.

Рисунок 3.11 – Элементы оболочки KSS

Область № 1 предназначена для вывода названий пунктов или подпунктов меню оболочки KSS, которые, в свою очередь, являются ещё и названиями страниц оболочки KSS. Страница оболочки KSS – это область, которая состоит из всех областей, представленных на рисунке 3.11.

В области № 2 выводятся:

- в левой её части пункты и подпункты меню KSS;
- в правой её части дополнительная информация о выбранном пункте/подпункте меню или справочная информация о выбранном пункте/подпункте (параметре) из левой части данной области.

Для того чтобы просмотреть данные, которые не уместились в области № 2, следует воспользоваться: клавишами [↑], [↓] – для пролистывания данных, клавишами [Page Up], [Page Down] – для вывода данных постранично.

В области № 3 отображается информация о клавишах клавиатуры, предназначенных для выполнения определённых действий в KSS (навигация в оболочке, выбор пунктов меню, присвоение значений параметрам).

3.6 Изменение пароля пользователя

Для изменения пароля пользователя следует:

1) выбрать пункт *Электронный замок “Витязь”* в разделе *Модули безопасности*, в главном меню KSS (см. рисунок 3.10);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. рисунок 3.12);

Рисунок 3.12 – Страница *Электронный замок “Витязь”* (вид 1)

3) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”: список пользователей* (см. рисунки 3.13 - 3.16), на которой представлен единственный профиль пользователя, который только что прошёл процедуру аутентификации в ЭЗ и выполнил вход в оболочку KSS;

Рисунок 3.13 – Страница *Электронный замок “Витязь”: список пользователей* (вид 1), профиль пользователя, *Способ аутентификации* — «Электронный ключ»

Рисунок 3.14 – Страница *Электронный замок “Витязь”: список пользователей* (вид 2), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — «Общее имя (CN)»

Рисунок 3.15 – Страница *Электронный замок “Витязь”: список пользователей* (вид 3), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — «Универсальное имя (UPN)»

Рисунок 3.16 – Страница *Электронный замок “Витязь”: список пользователей* (вид 4), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата»

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. рисунки 3.17), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

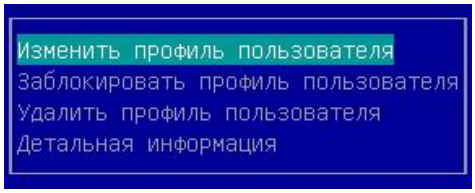


Рисунок 3.17 – Окно для выбора действия
над профилем пользователя

5) выбрать пункт *Изменить профиль пользователя* в окне (см. рисунок 3.17);

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: изменение профиля пользователя* (см. рисунки 3.18 – 3.20);

Рисунок 3.18 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 1), профиль пользователя, *Способ аутентификации* — «Электронный ключ»

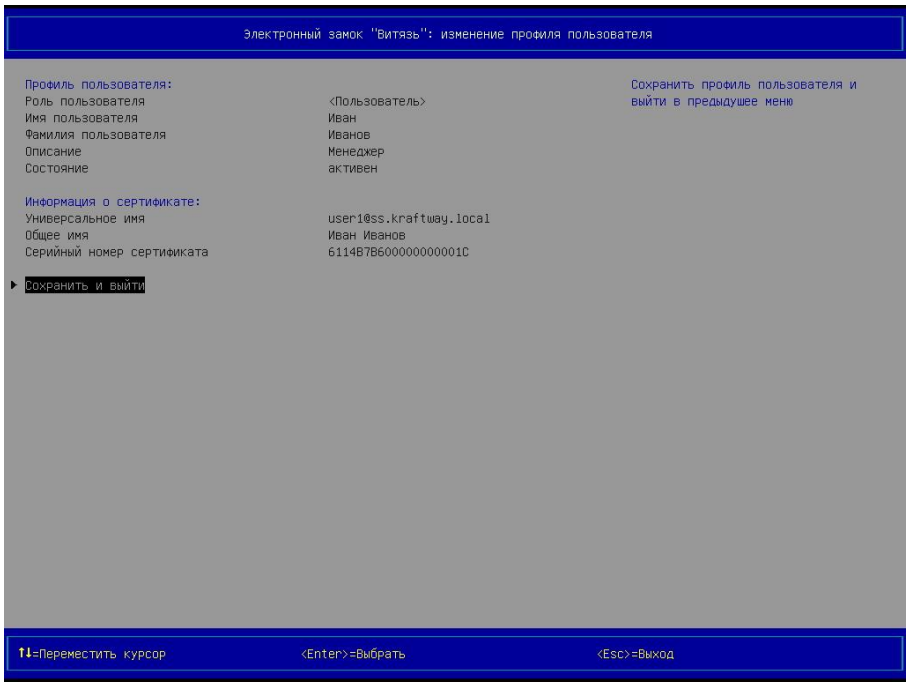


Рисунок 3.19 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 2), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

Рисунок 3.20 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 5), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат и электронный ключ»,

Ключевое поле – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

7) выбрать параметр *Сменить пароль*;

8) подключить АН пользователя к свободному USB-порту персонального компьютера, PIN-код которого подлежит изменению;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно для ввода старого пароля пользователя (см. рисунок 3.21);

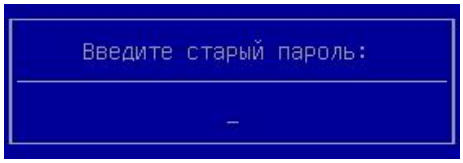


Рисунок 3.21 – Окно для ввода старого пароля пользователя

10) ввести старый пароль в окно;

11) → [Enter] на клавиатуре, на экран выводится окно для ввода нового пароля пользователя (см. рисунок 3.22);

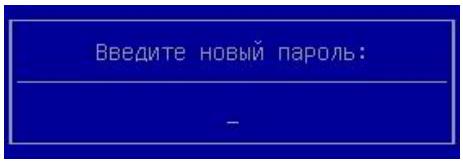


Рисунок 3.22 – Окно для ввода нового пароля пользователя

12) ввести новый пароль пользователя;

13) → [Enter] на клавиатуре, на экран выводится окно для подтверждения нового пароля пользователя (см. рисунок 3.23);

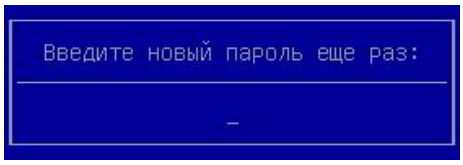


Рисунок 3.23 – Окно для подтверждения нового пароля пользователя

14) ввести новый пароль пользователя;

15) → [Enter] на клавиатуре, на экран выводится окно (см. рисунок 3.24), информирующее об успешном изменении пароля;

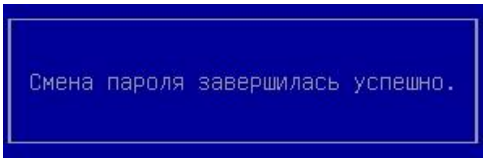


Рисунок 3.24 – Окно, информирующее об успешном изменении пароля пользователя

16) нажать любую клавишу на клавиатуре.

Примечания:

1. При выбранном профиле пользователя в разделе *Профили пользователей* (см. рисунки 3.13 - 3.16) в правой части области № 2 выводится дополнительная информация о профиле (имя пользователя, фамилия пользователя, описание пользователя, роль пользователя, состояние пользователя, идентификатор электронного ключа, название электронного ключа, дата создания профиля пользователя, дата последнего входа пользователя, обладающего данным профилем, количество входов, выполненных пользователем, обладающим данным профилем, максимальное количество попыток ввода пароля, определённое для пользователя администратором). Объём выводимой дополнительной информации о профиле пользователя зависит от способа аутентификации в ЭЗ и роли пользователя.

2. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата» – страница *Электронный замок “Витязь”: список пользователей*, практически анало-

гична тем, страницам, что представлены на рисунках 3.14 - 3.16, когда параметру ЭЗ *Способ аутентификации* присвоено значение «Цифровой сертификат». Разница заключается только в выводе дополнительных сведений о профиле пользователя (идентификатор электронного ключа, название электронного ключа) в правой части области № 2 данной страницы. Т.е. представление дополнительной информации о профиле пользователя в правой части области № 2 страницы *Электронный замок "Витязь": список пользователей* идентичен представлению дополнительной информации при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Электронный ключ» (см. рисунок 3.13).

3. Пользователю предоставляется возможность изменения пароля при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – или «Электронный ключ», «Цифровой сертификат и электронный ключ».

4. При следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок "Витязь": изменения профиля пользователя* (см. рисунок 3.19). При данном способе аутентификации в ЭЗ изменить пароль пользователя нельзя.

3.7 Вывод детальной информации о пользователе

Для вывода детальной информации о пользователе следует:

1) выполнить действия 1-4 п. 3.6;

2) выбрать пункт *Детальная информация* в диалоговом окне (см. рисунок 3.17);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок "Витязь": детальная информация о пользователе* (см.
рисунки 3.25 - 3.27).

Рисунок 3.25 – Страница *Электронный замок “Витязь”: детальная информация о пользователе* (вид 1), профиль пользователя, *Способ аутентификации* — «Электронный ключ»

Рисунок 3.26 – Страница *Электронный замок “Витязь”: детальная информация о пользователе* (вид 2), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

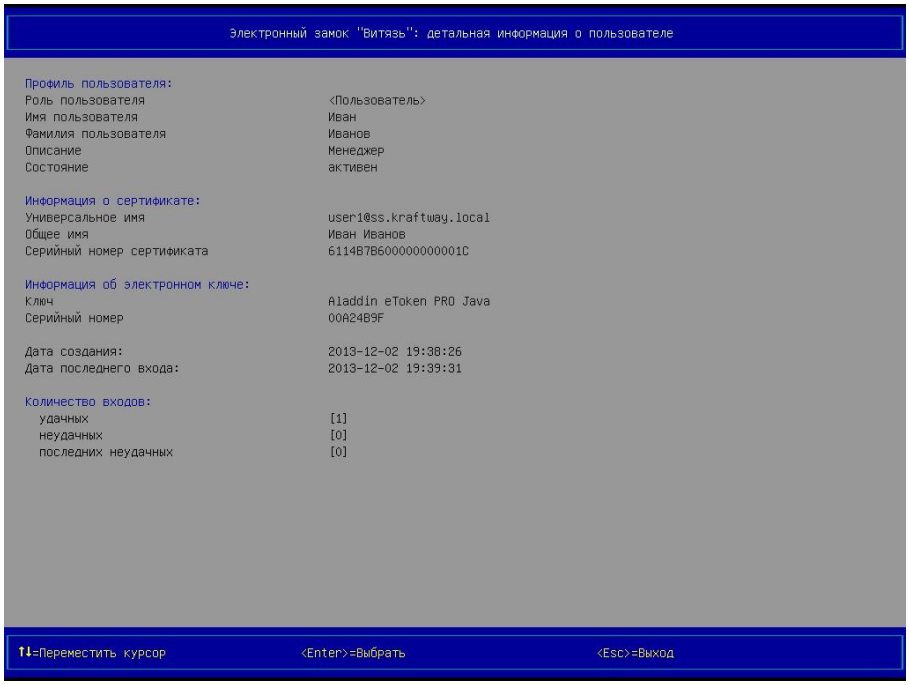


Рисунок 3.27 – Страница *Электронный замок “Витязь”: детальная информация о пользователе* (вид 3), профиль пользователя, *Способ аутентификации* — «Цифровой сертификат и электронный ключ», *Ключевое поле* — или «Общее имя (CN)», или «Универсаль-

ное имя (UPN)»,
или «Серийный номер сертификата»

Примечание. Количество параметров и их значений, выводимых на странице *Электронный замок “Витязь”: детальная информация о пользователе* (см. рисунки 3.25 - 3.27), зависит от роли пользователя, которая была установлена администратором в настройках ЭЗ, и от профиля пользователя, детальную информацию о котором требуется вывести и просмотреть.

Может быть выведена следующая информация о пользователе:

1) роль пользователя (пользователь);
2) имя пользователя;
3) фамилия пользователя;
4) описание пользователя (например, инженер);
5) состояние профиля пользователя (активен или заблокирован);
6) информация о сертификате:
   - универсальное имя;
   - общее имя;
   - серийный номер сертификата;
7) информация об АН;
   - ключ;
   - серийный номер;
8) дата создания пользователя;
9) дата последнего входа пользователя;
10) количество входов:
    - количество удачных входов;
    - количество неудачных входов;
    - количество последних неудачных входов;
11) максимальное количество попыток ввода пароля.

Примечание. Количество последних неудачных входов – это количество попыток аутентификации в ЭЗ, результаты которых были отрицательными. Если хотя бы один раз, после нескольких неудачных попыток аутентификации, пользователь прошёл процедуру

аутентификации с положительным результатом, то количество последних неудачных входов обнуляется.

3.8 Загрузка операционной системы

Для выполнения загрузки операционной системы при включённом ЭЗ пользователю следует пройти процедуру аутентификации в ЭЗ, а после успешного их прохождения – дождаться загрузки ОС (см. п. 3.3).

4 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

Сообщения пользователю – это текстовые сообщения (записи), выводимые на страницах или в окнах ЭЗ в процессе работы с ПК ЭЗ «Витязь» В2.2.

Основная часть сообщений, выводимых на экран монитора, представлена в соответствующих разделах данного руководства. В данном разделе приводятся дополнительные сообщения ЭЗ, которые не были описаны в вышеперечисленных разделах, и требуют отдельного рассмотрения. Также в этом разделе приводятся действия пользователя, которые ему следует выполнить, при выводе сообщений. Дополнительные сообщения ЭЗ приводятся ниже по тексту при описании различного рода ситуаций, с которыми пользователь может столкнуться при работе с ЭЗ.

Ситуация № 1

Во время выполнения процедуры КЦ для каждого файла, прошедшего проверку, на экран выводится результат данной проверки в виде записи: <Результат проверки>: <путь к файлу, прошедшего проверку> (см. рисунок 4.1). Результат проверки может принимать значения: «Успех», «Не найден», «Ошибка». После завершения процедуры КЦ, ниже всех записей с результатами проверки, выводится итоговая информация о результатах данной процедуры, которая содержит: количество проверенных файлов, количество файлов, которые прошли процедуру КЦ с положительным результатом, количество файлов, которые прошли процедуру КЦ с отрицательным результатом. При отрицательном результате процедуры КЦ, на экран выводятся записи следующего вида (см. рисунок 4.1):

Целостность файловой системы нарушена

Нажмите любую клавишу для продолжения…

```
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Launcher.cfg
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Launcher.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Loader.cfg
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Loader.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FileSelec
tionDxe.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FileSyste
mIntegrity.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\FsiManage
r.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\KraftwayH
ash.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Integrity\TextUiDxe
.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\Databas
e.efi
Не найден [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\Fil
eExplorer.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\InputHa
ndler.efi
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\SecureS
hell.efi
Ошибка [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\SecureShell\LOGO.B
MP
Успех [PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x7,0x0)/HD(1,MBR,0x73fc1fd3,0x3f,0x734b41)]\EFI\Kraftway\Tools\Ext.efi

Кол-во проверенных файлов: 15
Кол-во файлов с положительным результатом проверки: 13
Кол-во файлов с отрицательным результатом проверки: 2
Целостность файловой системы нарушена
Нажмите любую клавишу для продолжения...
```

Рисунок 4.1 – Целостность файловой системы нарушена

Решение: при появлении сообщений такого вида пользователю следует обратиться к системному администратору или администратору безопасности организации.

Ситуация № 2

При отрицательном результате процедуры КЦ, и когда ЭЗ включён, после вывода записей, описанных в ситуации № 1 (см. рисунок 4.1), и нажатия на любую клавишу клавиатуры, на экран монитора выводятся записи следующего вида (см. рисунок 4.2):

Ограничение доступа:

Нарушена целостность файловой системы.

Доступ разрешён только администратору

Поиск электронного ключа

Подключите электронный ключ

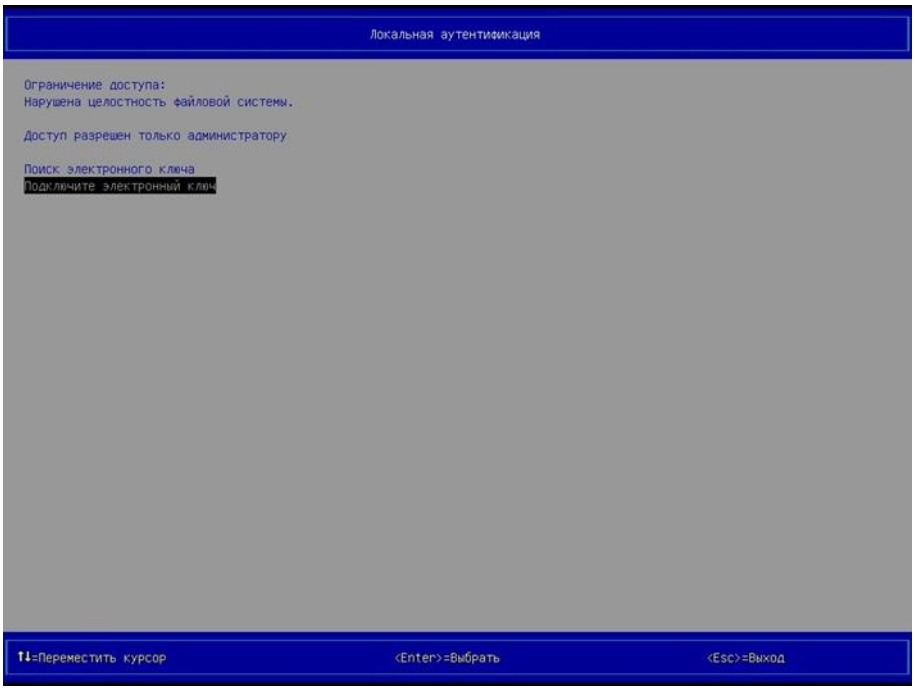


Рисунок 4.2 – Страница *Локальная аутентификация* (вид 5), ЭЗ заблокировал компьютер

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации.

Ситуация № 3

Если после вывода страницы *Локальная аутентификация* (см. рисунок 4.2) пользователь подключит своё АН к USB-порту персонального компьютера, введёт пароль пользователя в соответствующем окне (см. рисунок 3.4) и нажмёт на клавишу [Enter] клавиатуры, то после выполнения данных действий на экран будет выведено окно (см. рисунок 4.3).

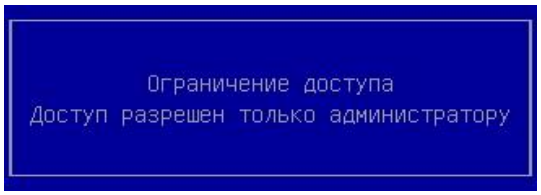


Рисунок 4.3 – Пользователю отказано в доступе

Ситуация № 4

Если текущий пароль пользователя был введён неправильно во время его аутентификации, то на экран выводится окно (см. рисунок 4.4), информирующее о том, что был введён неверный пароль.

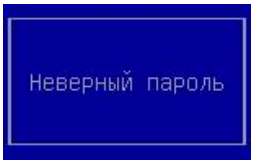


Рисунок 4.4 – Пароль введен неправильно

Решение: пользователю требуется нажать любую клавишу на клавиатуре, после выполнения данного действия ввести правильный пароль в соответствующем поле.

Примечание. Пользователь может последовательно ввести неправильный пароль максимально допустимое число раз. Максимально допустимое число ввода пароля определяется администратором при выполнении настройки ЭЗ.

Ситуация № 5

Если количество неправильно введённого пароля пользователя во время его аутентификации равно максимальному количеству попыток ввода пароля, которое устанавливается администратором для пользователя, то после нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 4.5), информирующее о превышении количества попыток ввода пароля, после повторного нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 4.4), информирующее о том, что был введён неверный пароль, а после третьего нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 4.6), информирующее о попытке входа заблокированного пользователя.

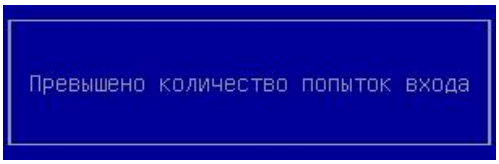


Рисунок 4.5 – Превышено количество попыток ввода пароля

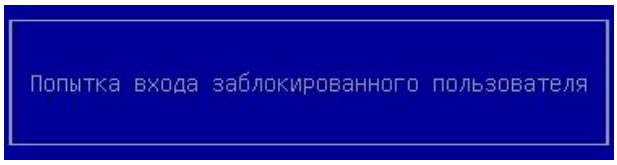


Рисунок 4.6 – Попытка входа заблокированного пользователя

Решение: при появлении сообщений такого вида пользователю следует обратиться к администратору или администратору безопасности организации для разблокировки своего профиля пользователя.

Ситуация № 6

Если после включения персонального компьютера, во время процедуры аутентификации, подключить АН пользователя, профиль которого ранее был заблокирован ЭЗ, то на экран будет выведено окно (см. рисунок 4.6), информирующее о попытке входа заблокированного пользователя).

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации для разблокировки своего профиля пользователя.

Ситуация № 7

На экран выводится запись вида «ОШИБКА! Превышено количество попыток аутентификации. Нажмите любую клавишу для перезагрузки…» при следующих условиях:

- если во время прохождения пользователем процедуры аутентификации было превышено максимальное количество попыток аутентификации, т.е. количество подключений АН пользователя к USB-порту персонального компьютера, которое было задано администратором ранее в настройках ЭЗ;
- если во время прохождения пользователем процедуры аутентификации количество попыток ввода пароля пользователя превысило максимальное количество попыток аутентификации, которое было задано администратором ранее в настройках ЭЗ, т.е. если после вывода окна (см. рисунок 4.6) пользователем было выполнено последовательное нажатие на клавишу [Enter] такое количество раз, которое привело к превышению максимального количества попыток аутентификации.

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации для разблокировки своего профиля пользователя.

Ситуация № 8

Если при прохождении процедуры аутентификации подключить АН пользователя, незарегистрированное в БД ЭЗ, к свободному USB-порту компьютера, то на экран будет выведено окно (см. рисунок 4.7), информирующее о попытке использования незарегистрированного ключа.

Рисунок 4.7 – Попытка использования незарегистрированного ключа

Примечание. Окно (см. рисунок 4.7) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Решения:

1. Пользователю следует: отключить АН пользователя от USB-порта персонального компьютера, которое не было ранее зарегистрировано в ЭЗ; обратиться к администратору или администратору безопасности организации для получения АН, которое применялось при создании в ЭЗ его профиля пользователя и было зарегистрировано в БД ЭЗ; далее повторить процедуру аутентификации в ЭЗ с применением нового АН.
2. Пользователю следует: отключить АН пользователя от USB-порта персонального компьютера, которое не было ранее зарегистрировано в ЭЗ; обратиться к администратору или администратору безопасности организации для создания профиля пользователя с применением имеющегося АН; далее повторить процедуру аутентификации в ЭЗ с применением этого же АН.

Ситуация № 9

Если во время прохождения процедуры аутентификации пользователем было выбрано значение ключевого поля на странице *Локальная аутентификация* (см. рисунки

3.7 - 3.9), которое отсутствует в БД ЭЗ, то после нажатия на клавишу [Enter] клавиатуры на экран будет выведено окно (см. рисунок 4.8), информирующее о том, что пользователь, проходящий в данный момент процедуру аутентификации, не зарегистрирован в ЭЗ.

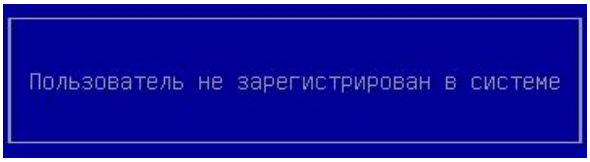


Рисунок 4.8 – Пользователь не зарегистрирован в ЭЗ

Примечание. Окно (см. рисунок 4.8) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок "Витязь"* — «Вкл», *Способ аутентификации* — «Цифровой сертификат».

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации.

Ситуация № 10

Если во время прохождения процедуры аутентификации не были найдены сертификаты пользователей на АН, то на странице *Локальная аутентификация* (см. рисунок 4.9) выводится запись следующего вида:

Сертификатов не обнаружено

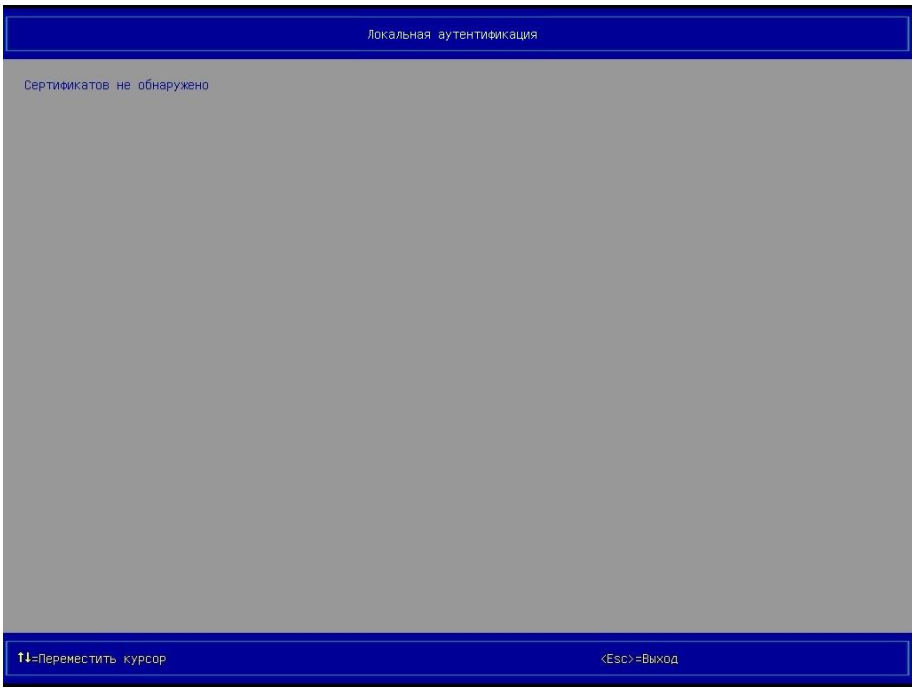


Рисунок 4.9 – Страница *Локальная аутентификация* (вид 6), сертификаты не были найдены на АН

Примечание. Запись, представленная на странице *Локальная аутентификация* (см. рисунок 4.9), может быть выведена тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации для сохранения его сертификата пользователя на АН.

Ситуация № 11

Если во время прохождения пользователем процедуры аутентификации результат проверки сертификата пользователя на подлинность отрицательный (см. п. 3.3.4), то на экран выводится окно (см. рисунок 4.10), информирующее об ошибке аутентификации.

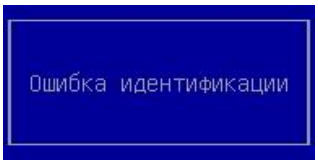


Рисунок 4.10 – Ошибка аутентификации

Примечание. Окно (см. рисунок 4.10) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: при появлении сообщения такого вида пользователю следует обратиться к администратору или администратору безопасности организации.

Ситуация № 12

Если не подключить АН пользователя перед сменой его пароля или подключить АН другого пользователя, для которого смена пароля в данный момент не выполняется, то на экран буден выведено окно (см. рисунок 4.11), информирующее о том, что АН не был подключён, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 4.12), информирующее о том, что произошла ошибка при смене пароля.

Рисунок 4.11 – АН не был подключен

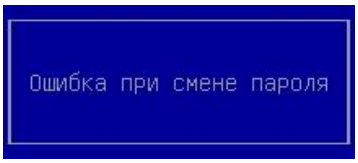


Рисунок 4.12 – Произошла ошибка при смене пароля

Решение: при появлении сообщений такого вида пользователю следует обратиться к администратору или администратору безопасности организации.

Ситуация № 13

Если текущий пароль пользователя был введён неправильно во время изменения пароля пользователя, то на экран выводится окно (см. рисунок 4.13), информирующее о том, что пароль был введён неправильно, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 4.12), информирующее о том, что произошла ошибка при смене пароля.

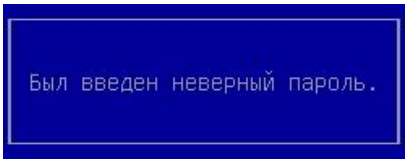


Рисунок 4.13 – Неправильно введён пароль

Решение: пользователю следует нажать на любую клавишу клавиатуры, повторить изменение пароля пользователя.

Ситуация № 14

Если новый пароль пользователя был введен неправильно во время изменения пароля, то на экран выводится окно (см. рисунок 4.14), информирующее о несовпадении паролей, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 4.12), информирующее о том, что произошла ошибка при смене пароля.

Рисунок 4.14 – Пароли не совпадают

Решение: пользователю следует нажать любую клавишу на клавиатуре, после чего повторно выполнить смену пароля пользователя.

Ситуация № 15

Если в течение заданного интервала времени не удалось ввести пароль пользователя (см. п. 3.3), то на экран выводится окно (см. Рисунок 4.15), информирующее о превышении отведенного времени на ввод пароля.

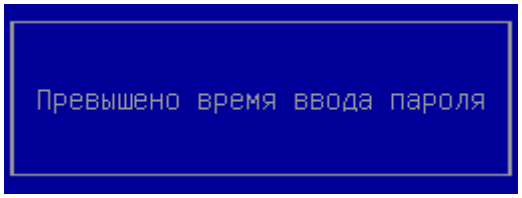


Рисунок 4.15 – Превышено время ввода пароля

Решение: пройдите процедуру ввода пароля ещё раз.