УТВЕРЖДЕН

643.18184162.00006-02 91-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ЭЛЕКТРОННЫЙ ЗАМОК «ВИТЯЗЬ»,

ВЕРСИЯ 2.2

Руководство пользователя

643.18184162.00006-02 91

Листов 135

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

2024

Литера

АННОТАЦИЯ

Настоящий документ содержит сведения по эксплуатации программного комплекса «Электронный замок «Витязь», версия 2.2 (далее – ПК «ЭЗ «ВИТЯЗЬ» 2.2) пользователями всех типов.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 поставляется интегрированным в низкоуровневое программное обеспечение (ПО) материнской платы.

В документе содержится информация о назначении, составе и работе с ПК «ЭЗ «ВИТЯЗЬ» 2.2, а также приводятся информационные сообщения и сообщения об ошибочных действиях пользователя и способы их устранения.

Информация о порядке приемки ПК «ЭЗ «ВИТЯЗЬ» 2.2, его безопасной установке и настройке, требованиям к среде функционирования и настройке функций безопасности среды функционирования, процедурам устранения недостатков, регламенте информирования о выявленных уязвимостях, регламенте обновления, а также мерам блокирования возможных уязвимостей приведена в документе «Руководство администратора» 643.18184162.00006-02 90.

Данное руководство предназначено для пользователей, эксплуатирующих ПК «ЭЗ «ВИТЯЗЬ» 2.2 как в роли рядового пользователя, так и в роли привилегированного пользователя (администратора).

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПК «ЭЗ «ВИТЯЗЬ» 2.2

1.1. Наименование и обозначение

Наименование программного изделия – Программный комплекс «Электронный замок «Витязь» версия 2.2.

Обозначение программного изделия – 643.18184162.00006-02.

Наименование предприятия-изготовителя – АО «Крафтвэй корпорэйшн ПЛС».

Фактический адрес – 249032, Калужская область, г. Обнинск, Киевское ш., д. 64.

1.2. Назначение

ПК «ЭЗ «ВИТЯЗЬ» 2.2 – это средство доверенной загрузки (СДЗ) уровня UEFI BIOS второго класса защиты со встроенным средством антивирусной защиты (САВЗ) типа «Г» второго класса защиты, разработанный согласно «Заданию по безопасности» 643.18184162.00006-02 94 и руководящих документов ФСТЭК России.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 предустановлен в ПО уровня UEFI BIOS компьютера и предназначено для использования в автоматизированных системах обработки информации, содержащей сведения, составляющие государственную тайну, а также в государственных информационных системах и информационных системах персональных данных всех классов и уровней защищенности.

1.3. Программные модули ПК «ЭЗ «ВИТЯЗЬ» 2.2

ПК «ЭЗ «ВИТЯЗЬ» 2.2 включает в себя следующие программные модули:

1) модуль *Электронный замок «Витязь»* (TrustedBoot.efi), выполняющий основные функции комплекса – взаимодействие с аутентифицирующими носителями (АН) для обеспечения двухфакторной аутентификации и аутентификацию по цифровому сертификату пользователя до загрузки операционной системы (ОС);

2) модуль *Управление сертификатами* (CertificateMenu.efi) для работы с сертификатами удостоверяющего центра (УЦ), которые используются для проверки на подлинность сертификатов пользователей при прохождении ими процедуры аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

3) модуль *Контроль целостности файловой системы* (FileSystemIntegrity.efi) для формирования списков объектов файловых систем (ФС), выбранных для контроля целостности (КЦ), и их контрольных сумм (КС), а также для вывода результата проверки КЦ;

4) модуль *Контроль целостности оборудования* (HardwareIntegrity.efi) для формирования списков оборудования и КС оборудования для КЦ, а также для вывода результата проверки КЦ;

5) модуль *Журнал событий* (EventLog.efi), выполняющий выгрузку журнала регистрации событий безопасности и отчета о состоянии ПК «ЭЗ «ВИТЯЗЬ» 2.2;

6) модуль *Антивирус Касперского для UEFI*[1)] (Kav_for_kss_rus_sign_2.0.0.136.efi) для антивирусной защиты на уровне UEFI до загрузки ОС, для борьбы с руткитами/буткитами и другими вредоносными программами, адаптированными для противодействия антивирусам уровня ОС;

7) вспомогательный модуль (FsiManager.efi) для процедуры КЦ;

8) вспомогательный драйвер (NetworkCredentialProvider.efi) для доступа к АН пользователей.

1.4. Ролевая модель пользователей

Доступ к функционалу ПК «ЭЗ «ВИТЯЗЬ» 2.2 зависит от роли, получаемой пользователем при аутентификации.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 обеспечивает разделение пользователей на группы со следующими ролями:

1) «администратор»;

2) «пользователь»;

3) «гость».

ВАЖНО! ПЕРВОЙ УЧЕТНОЙ ЗАПИСЬЮ, СОЗДАВАЕМОЙ В ПК «ЭЗ «ВИТЯЗЬ» 2.2 ОБЯЗАТЕЛЬНО ДОЛЖНА БЫТЬ УЧЕТНАЯ ЗАПИСЬ ПОЛЬЗОВАТЕЛЯ С РОЛЬЮ «АДМИНИСТРАТОР». ПОЛЬЗОВАТЕЛЬ С ЭТОЙ РОЛЬЮ ИМЕЕТ ВОЗМОЖНОСТЬ ВЫПОЛНЯТЬ ВСЕ НАСТРОЙКИ, В ТОМ ЧИСЛЕ СОЗДАВАТЬ ДРУГИЕ УЧЕТНЫЕ ЗАПИСИ С РОЛЬЮ КАК «ПОЛЬЗОВАТЕЛЬ», ТАК И «АДМИНИСТРАТОР».

1.5. Среда функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2 – оболочка KSS и UEFI BIOS

Условные обозначения при описании последовательности действий:

1) названия клавиш клавиатуры приводятся в квадратных скобках, например, [Enter];

2) названия страниц, разделов, пунктов (параметров) оболочки KSS, а также экранных кнопок управления выделяются *курсивом*;

3) значения параметров указываются в кавычках (« »).

1.5.1. Вход в оболочку KSS

Оболочка KSS, интегрированная в UEFI – это среда защищенного запуска и управления модулями безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2 до загрузки ОС. Для входа в оболочку имеются следующие варианты действий:

[1)] Модуль *Антивирус Касперского для UEFI* разработан и поддерживается АО «Лаборатория Касперского». Поставляется на основании Лицензионного договора № 15054 от 02.09.2013 г.

1) вариант 1. При первом запуске компьютера или при выключенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно в процессе загрузки ОС, при появлении окна *Приглашение на вход в KSS* (рис. 1), нажать клавишу [F1] для входа в оболочку KSS, отображается страница *Kraftway Secure Shell* (рис. 2);

Приглашение на вход в KSS

Рис. 1

2) вариант 2. При включенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. подраздел 2.1). При появлении окна *Приглашение на вход в KSS* (см. рис. 1) нажать клавишу [F1] для входа в KSS, отображается страница *Kraftway Secure Shell* (рис. 2).

Страница Kraftway Secure Shell, главное меню оболочки KSS

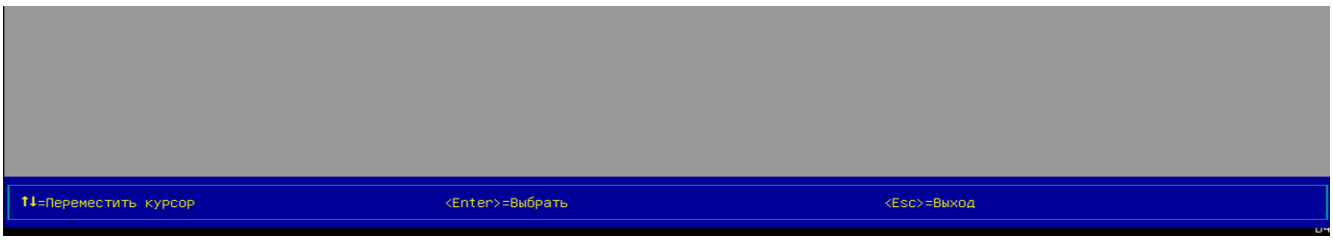

Рис. 2

Примечания:

1. Если ранее не было выполнено никаких настроек в ПК «ЭЗ «ВИТЯЗЬ» 2.2, то сразу же после отображения Logo-изображения материнской платы предлагается дождаться начала загрузки ОС или войти в оболочку KSS (см. рис. 1).

2. Все дальнейшие операции, связанные с ПК «ЭЗ «ВИТЯЗЬ» 2.2, сертификатами пользователей и КЦ файловой системы и так далее, доступны администратору только после включения соответствующих модулей безопасности.

3. Набор модулей безопасности определяется спецификацией поставки и может отличаться в различных установках.

1.5.2. Интерфейс пользователя оболочки KSS

Экранная страница оболочки KSS (рис. 3) состоит из следующих областей:

1) область № 1 – для отображения названия экранных страниц оболочки;

2) область № 2 – для отображения:

– в левой ее части названия разделов, пунктов, а также значений пунктов меню оболочки;

– в правой ее части дополнительной или справочной информация о пункте (параметре) меню, выбранном в левой части данной области;

– результаты КЦ объектов и отчет о состоянии ПК «ЭЗ «ВИТЯЗЬ» 2.2;

3) область № 3 – для отображения информации об используемых на странице клавишах клавиатуры, предназначенных для выполнения определенных действий по навигации в оболочке, выбору пунктов меню, присвоению значений параметрам.

Области оболочки KSS

1 - область для названия пункта/подпункта меню; 2 - область для пунктов/подпунктов меню, дополнительной или справочной информации; 3 - область для подсказок

Рис. 3

Для того чтобы просмотреть данные, которые не уместились в области № 2, следует воспользоваться клавишами [↑], [↓] – для пролистывания данных, для выбора первой строки на странице следует нажать клавишу [Page Up], а для выбора последней строки – клавишу [Page Down].

Главное меню оболочки KSS (см. рис. 2) состоит из двух основных разделов, содержащих следующие пункты:

1) раздел Модули безопасности:

– *Электронный замок «Витязь»*;

– *Управление сертификатами (см. подраздел 2.4);*

– *Контроль целостности файловой системы (см. подраздел 2.5);*

– *Контроль целостности оборудования (см. подраздел 2.6);*

– *Контроль программной среды (см. подраздел 2.7);*

– *Контроль целостности реестра Windows (см. подраздел 2.8);*

– *Журнал событий (см. подраздел 2.9);*

– *Антивирус Касперского для UEFI (см. подраздел 2.10);*

2) раздел Конфигурация:

– *Контроль модулей безопасности*;

– *Управление ограничением доступа;*

– *Настройки.*

1.5.3. Выход из оболочки KSS

Для выхода из оболочки KSS следует:

1) перейти в главное меню оболочки KSS (см. рис. 2);

2) нажать клавишу [Esc], отображается окно (рис. 4) для подтверждения выхода из оболочки;

Рис. 4

3) нажать клавишу [Enter], администратору предлагается дождаться загрузки ОС.

Примечание. При выходе из оболочки KSS осуществляется очистка оперативной памяти от остаточной информации ПК «ЭЗ «ВИТЯЗЬ» 2.2.

1.5.4. Вход в программу настройки UEFI BIOS материнской платы

Пользователи с ролью «администратор», могут входить в программу настройки UEFI BIOS материнской платы (например, для ввода системного времени компьютера).

Для входа в интерфейс настройки UEFI BIOS материнской платы при выключенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно:

1) включить компьютер, на экране отображается Logo-изображение материнской платы, на следующем шаге загрузки отображается приглашение на вход в KSS (см. рис. 1);

2) нажать клавишу [Delete] в момент вывода на экран приглашения на вход в KSS, приглашение на вход в KSS пропадает с экрана;

3) повторно нажать клавишу [Delete], отображается интерфейс UEFI BIOS материнской платы.

Для входа в интерфейс настройки UEFI BIOS материнской платы при включенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно:

1) включить компьютер и пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

2) нажать клавишу [Delete] при выводе на экран приглашения на вход в KSS (см. рис. 1), приглашение на вход в KSS пропадает с экрана;

3) повторно нажать клавишу [Delete], отображается интерфейс UEFI BIOS материнской платы.

2. РАБОТА ПОЛЬЗОВАТЕЛЯ С РОЛЬЮ «АДМИНИСТРАТОР» С ПК «ЭЗ «ВИТЯЗЬ» 2.2

Описание установки ПК «ЭЗ «ВИТЯЗЬ» 2.2, методов его активации (включения)/деактивации (выключения) и первоначальной настройки его параметров приведено в документе 643.18184162.00006-02 90 «Руководство администратора».

2.1. Аутентификация администратора в ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для выполнения любых действий необходимо пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

В ПК «ЭЗ «ВИТЯЗЬ» 2.2 реализовано три способа аутентификации:

1) по электронному ключу (серийный номер АН) (см. п. 2.1.2);

2) по цифровому сертификату (см. п. 2.1.3);

3) по цифровому сертификату и электронному ключу (см. п. 2.1.4).

ВНИМАНИЕ! СПОСОБ АУТЕНТИФИКАЦИИ ВЫБИРАЕТСЯ ОДНОВРЕМЕННО ДЛЯ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРА В МОМЕНТ СОЗДАНИЯ ПРОФИЛЯ ПЕРВОГО АДМИНИСТРАТОРА. ИЗМЕНЕНИЕ СПОСОБА АУТЕНТИФИКАЦИИ ВЛЕЧЕТ ЗА СОБОЙ УДАЛЕНИЕ ВСЕХ ДАННЫХ О ПОЛЬЗОВАТЕЛЯХ.

В ПК «ЭЗ «ВИТЯЗЬ» 2.2 аутентификация пользователей проводится посредством предъявления АН на этапе загрузки ОС и дополнительного фактора.

Одному пользователю соответствует один АН.

Для всех АН выбирается один общий способ аутентификации.

При предъявлении АН выполняется проверка наличия серийного номера АН в базе данных (БД) ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся серийные номера АН, зарегистрированные ранее в БД.

Занесение серийного номера АН в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2 выполняется на этапе создания профиля нового пользователя. При выборе способа аутентификации только по цифровому сертификату данная проверка не выполняется.

В ПК «ЭЗ «ВИТЯЗЬ» 2.2 реализована аутентификация по одному из трех факторов: по PIN-коду к АН, по ключевому полю цифрового сертификата пользователя, по PIN-коду к АН и ключевому полю цифрового сертификата пользователя (см. таблицу 1).

Вариант 1. *Цифровой сертификат*. 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 ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы профили пользователей в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

При данном варианте аутентификации количество попыток ввода пароля пользователя ограничивается политикой безопасности организации.

Вариант 2. *Электронный ключ*. Аутентификация пользователя осуществляется посредством предъявления PIN-кода к АН, который является паролем пользователя. Количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

Вариант 3. *Цифровой сертификат и электронный ключ*. 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 ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы профили пользователей в ПК «ЭЗ «ВИТЯЗЬ» 2.2. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

Таблица 1 – Способы аутентификации

Вариант аутентификации	Ключевое поле по выбору	Фактор аутентификации	Действие
Цифровой сертификат	Универсальное имя (UPN) Общее имя (CN) Серийный номер сертификата	Пароль и выбор сертификата	Проверка ключевого поля
Электронный ключ	-	Пароль	Проверка s/n ключа
Цифровой сертификат и электронный ключ	Универсальное имя (UPN) Общее имя (CN) Серийный номер сертификата	Пароль и выбор сертификата	Проверка ключевого поля и s/n ключа

Примечание. При аутентификации предусмотрены следующие ограничения:
1) проверка минимального количества знаков пароля (минимальное 4, по умолчанию 6);
2) неуспешные попытки аутентификации (количество попыток ввода пароля) от 1 до 4;
3) ограничение времени данного на ввод пароля (секунд).

В случае положительной аутентификации происходит авторизация пользователя, необходимая для доступа к настройкам ПК «ЭЗ «ВИТЯЗЬ» 2.2, UEFI, которая выполняется в соответствии с ролевой моделью, описанной в подразделе 1.4.

Если условия успешной аутентификации пользователя не выполнены, дальнейший запуск ОС невозможен.

2.1.1. Создание профиля первого администратора

После входа в оболочку KSS и первого включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2) пользователю предоставляются права администратора. В ПК «ЭЗ «ВИТЯЗЬ» 2.2 изначально профиль администратора не создан.

Только после создания профиля первого администратора можно: создавать профили новых и изменять профили существующих пользователей, блокировать и разблокировать профили пользователей, просматривать детальную информацию о профилях пользователей, удалять профили пользователей.

Если данный профиль является единственным профилем администратора, то в этом случае его невозможно заблокировать или удалить.

Создание профиля первого администратора возможно при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)», использование АН пользователя для создания профиля администратора.

ВНИМАНИЕ! ПРИ ИСПОЛЬЗОВАНИИ СПОСОБОВ АУТЕНТИФИКАЦИИ «ЦИФРОВОЙ СЕРТИФИКАТ» ИЛИ «ЦИФРОВОЙ СЕРТИФИКАТ И ЭЛЕКТРОННЫЙ КЛЮЧ» ДОЛЖЕН БЫТЬ ВКЛЮЧЕН МОДУЛЬ БЕЗОПАСНОСТИ «УПРАВЛЕНИЕ СЕРТИФИКАТАМИ», В КОТОРЫЙ ДОЛЖЕН БЫТЬ ДОБАВЛЕН СЕРТИФИКАТ УЦ (СМ. ПОДРАЗДЕЛ 2.4).

Для создания профиля первого администратора следует:

1) выбрать п. *Электронный замок «Витязь»* раздела *Модули безопасности* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (рис. 5);

Страница *Электронный замок «Витязь»* (вид 2), до создания первого администратора

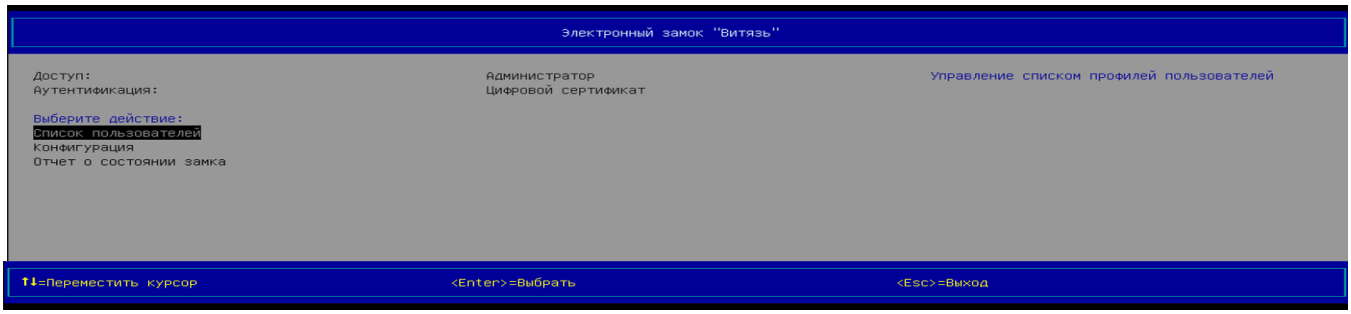

Рис. 5

3) выбрать п. *Список пользователей* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: список пользователей* (рис. 6), на которой предлагается создать профиль нового пользователя;

Страница Электронный замок «Витязь»: список пользователей (вид 5),

профили пользователей еще не создавались

Рис. 6

5) выбрать п. *Создать профиль нового пользователя* раздела *Управление пользователями*;

6) нажать клавишу [Enter], отображается окно (рис. 7), предлагающее администратору выбрать одно из следующих действий:

– использовать АН пользователя при создании профиля администратора;

– вручную - не использовать АН при создании профиля администратора;

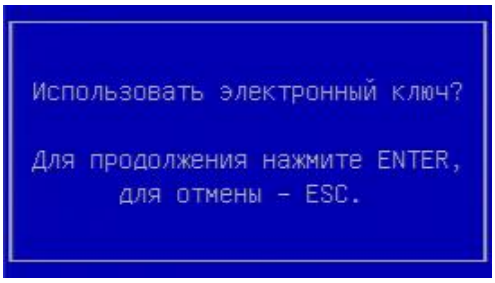

Рис. 7

7) нажать клавишу [Enter], отображается окно (рис. 8), предлагающее подключить АН пользователя к USB-порту;

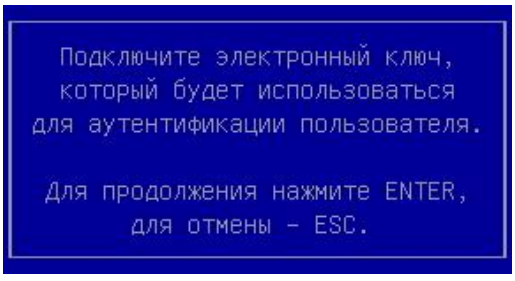

Рис. 8

8) подключить АН первого администратора к USB-порту;

9) нажать клавишу [Enter], отображается окно ввода пароля пользователя (рис. 9);

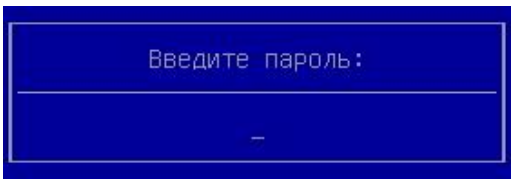

Рис. 9

10) ввести пароль администратора в окне ввода;

11) нажать клавишу [Enter], отображается окно, информирующее о поиске сертификатов пользователей, после завершения процесса поиска сертификатов отображается окно (рис. 10), в котором администратору предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов;

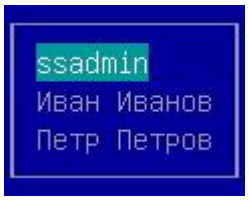

Рис. 10

12) выбрать нужное значение в окне выбора;

13) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: создание нового профиля пользователя* (рис. 11);

Страница Электронный замок «Витязь»: создание нового профиля пользователя

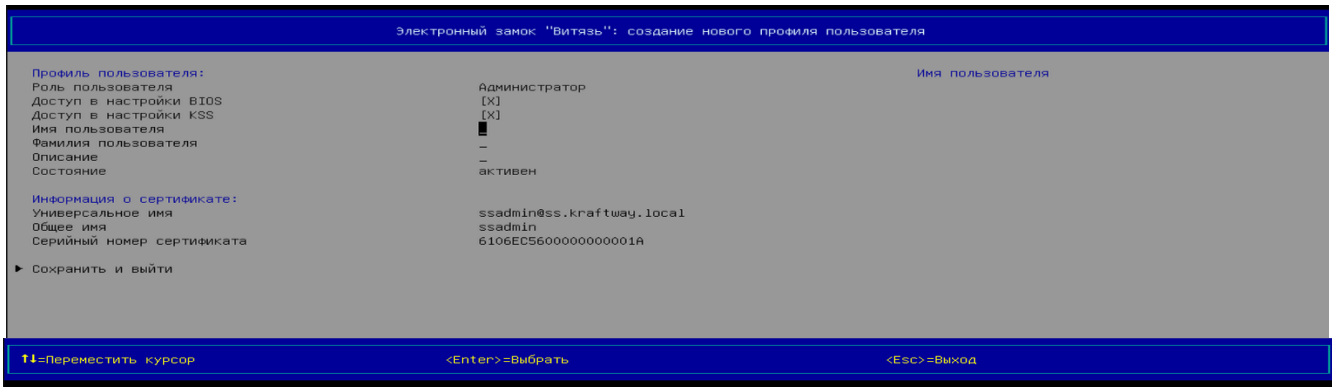

Рис. 11

14) выбрать параметр *Имя пользователя*;

15) нажать клавишу [Enter], отображается окно (рис. 12), предлагающее ввести имя пользователя;

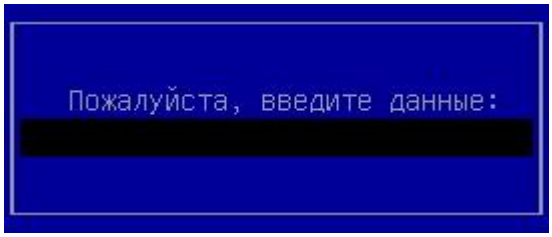

Рис. 12

16) ввести имя администратора и нажать клавишу [Enter];

17) выбрать параметр *Фамилия пользователя*;

18) нажать клавишу [Enter], отображается окно (см. рис. 12), предлагающее ввести фамилию пользователя;

19) ввести фамилию администратора и нажать клавишу [Enter];

20) выбрать параметр *Описание*;

21) нажать клавишу [Enter], отображается окно (рис. 13) для ввода описания пользователя;

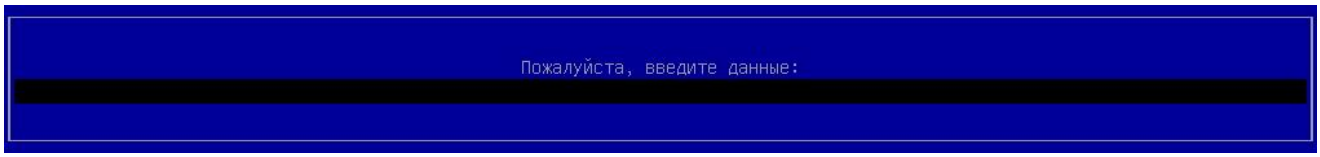

Рис. 13

22) ввести описание администратора и нажать клавишу [Enter];

23) выбрать п. *Сохранить и выйти*;

24) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: список пользователей* (рис. 14), на которой появился первый созданный пользователь и предлагается создать профиль нового пользователя;

Страница *Электронный замок «Витязь»: список пользователей* (вид 6),

профиль пользователя создан

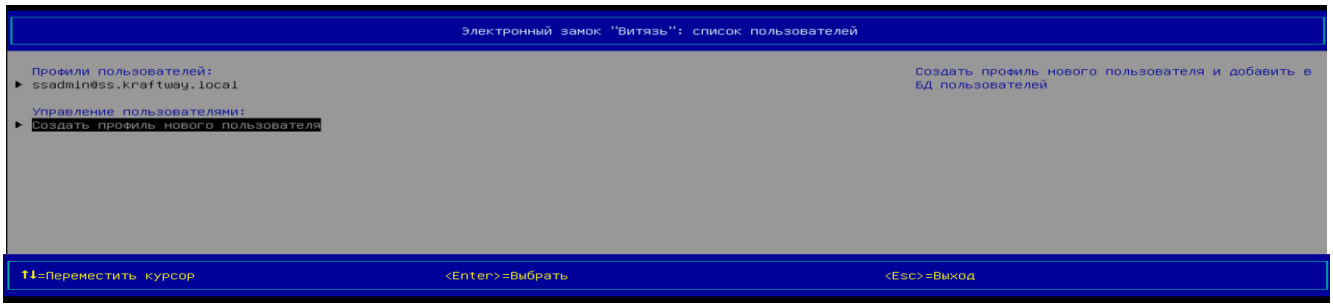

Рис. 14

Примечания:

1. Создание профиля первого администратора возможно только после включения модуля *Электронный замок «Витязь»* (см. подраздел 2.1.1).

2. Если при создании профиля первого администратора было принято решение о создании данного профиля без использования АН администратора, т.е. была нажата клавиша [Esc] (см. рис. 14), то тогда создание профиля первого администратора продолжается на странице *Электронный замок «Витязь»: создание нового профиля пользователя* (рис. 15).

3. При создании профиля первого администратора без использования АН следующим параметрам следует присвоить значения: *Имя пользователя*, *Фамилия пользователя*, *Описание*, *Универсальное имя*, *Общее имя*, *Серийный номер сертификата*, *Ключ*, *Серийный номер ключа*. Ввод значений параметров, перечисленных выше, выполняется в открывающихся окнах для ввода данных.

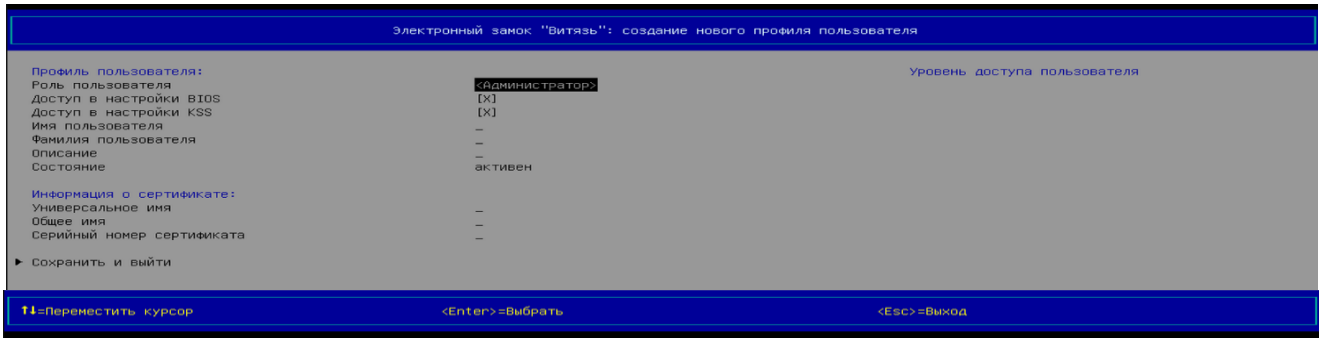

Рис. 15

4. Администратору следует быть предельно внимательным при вводе PIN-кода к АН. При инициализации (форматировании) АН с помощью ПО, идущего в комплекте с АН, администратором устанавливается максимальное количество попыток ввода PIN-кода. Максимальное количество попыток ввода PIN-кода различается для разных типов АН и определено в эксплуатационной документации на АН. Данное количество попыток накладывает ограничение со стороны конкретного АН, а не ПК «ЭЗ «ВИТЯЗЬ» 2.2. Превышение данного количества попыток ввода PIN-кода к АН приводит к блокировке этого АН на аппаратном уровне и к необходимости его повторной инициализации (форматированию).

5. Изменение языка ввода с английского на русский и наоборот выполняется клавишей [F9].

6. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: Электронный замок «Витязь» – «Вкл», Способ аутентификации – «Электронный ключ» – администратору не предлагается выбрать значение ключевого поля сертификата, и он не выполняет действия перечислений 11), 12) п. 2.1.1.

7. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: Электронный замок «Витязь» – «Вкл», Способ аутентификации – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», Ключевое поле – «Универсальное имя (UPN)» – после завершения поиска сертификатов пользователей (см. действие перечисления 11) п. 2.1.1), администратору предлагается выбрать универсальное имя из списка (рис. 16).

Рис. 16

8. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: Электронный замок «Витязь» – «Вкл», Способ аутентификации – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», Ключевое поле – «Серийный номер сертификата» – после завершения поиска сертификатов пользователей (см. действие перечисления 11) п. 2.1.1), администратору предлагается выбрать требуемый серийный номер одного из найденных сертификатов (рис. 17).

Рис. 17

9. При создании профиля первого администратора нельзя изменить значения следующих параметров: Роль пользователя, Доступ в настройки BIOS, Доступ в настройки KSS, т.к. данные параметры недоступны для изменения (см. рис. 11, 15). Таким образом, администратор, для которого был создан профиль первого администратора, всегда имеет доступ к настройкам BIOS материнской платы и настройкам оболочки KSS.

10. При создании профилей для второго и последующих администраторов становятся доступными для изменения следующие параметры: Роль пользователя, Доступ в настройки BIOS, Доступ в настройки KSS.

2.1.2. Аутентификация администратора, вариант 1

Прохождение аутентификации созданным пользователем при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ», *Модули контроля целостности* – «Вкл», создан контрольный список файлов для КЦ.

Для прохождения аутентификации следует:

1) включить компьютер, на экране отображается Logo-изображение материнской платы (рис. 18), после этого запускаются модули ПК «ЭЗ «ВИТЯЗЬ» 2.2;

Пример Logo-изображения материнской платы

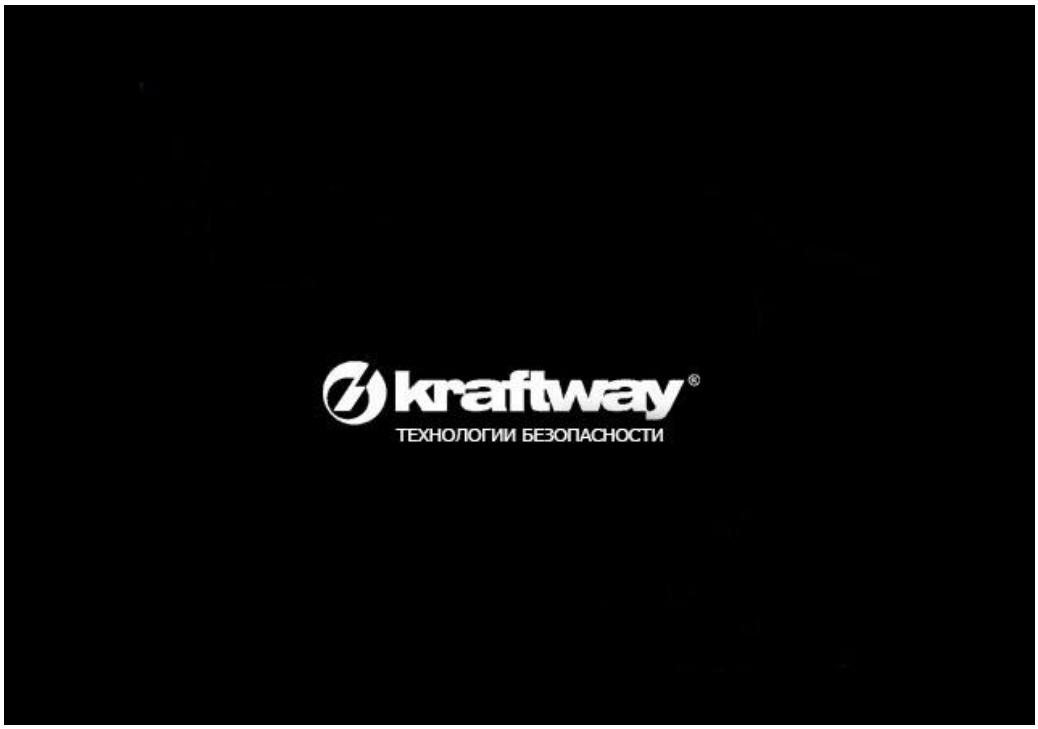

Рис. 18

2) предлагается подключить АН к USB-порту (рис. 19);

Страница Локальная аутентификация (вид 1), предложение на подключение АН

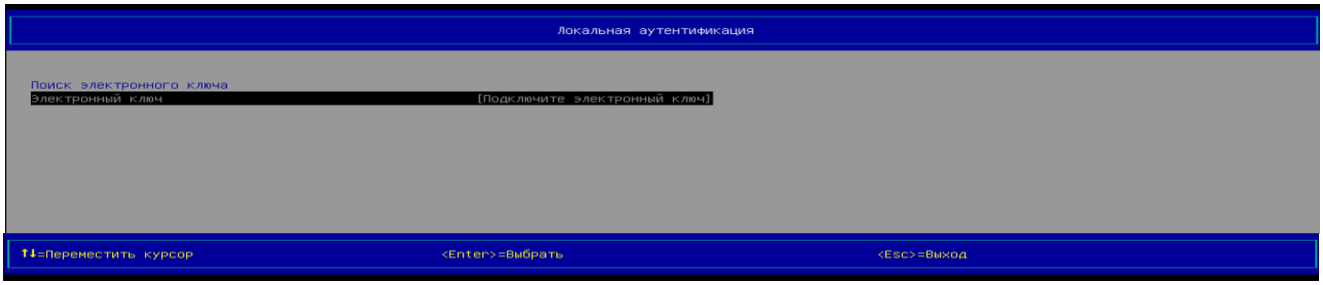

Рис. 19

3) подключить АН к USB-порту;

4) после обнаружения системой подключенного АН предлагается ввести пароль (рис. 20);

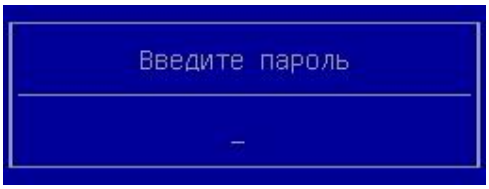

Рис. 20

5) ввести пароль пользователя;

6) нажать клавишу [Enter], после выполнения успешной аутентификации пользователя, предлагается дождаться загрузки ОС или войти в оболочку KSS нажатием клавиши [F1] (рис. 21).

Приглашение на вход в KSS

Рис. 21

Примечание. Процесс аутентификации пользователя выполняется после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2).

2.1.3. Аутентификация администратора, вариант 2

Прохождение аутентификации созданным пользователем при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Общее имя (CN)», *Модули контроля целостности* – «Вкл», создан контрольный список файлов, подлежащих КЦ.

Для прохождения аутентификации:

1) включить компьютер, отображается Logo-изображение материнской платы (см. рис. 18);

2) предлагается подключить АН к USB-порту (см. рис. 19);

3) подключить АН к USB-порту;

4) после обнаружении подключенного АН пользователю предлагается ввести пароль (см. рис. 20);

Примечание. Несмотря на то, что в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2 был выбран способ аутентификации по цифровому сертификату, пользователю предлагается ввести пароль. Это связано с тем, что сертификат пользователя, по которому выполняется аутентификация пользователя в ПК «ЭЗ «ВИТЯЗЬ» 2.2, размещен в защищенной области АН, доступ к которой, и соответственно к сертификату, осуществляется только после ввода PIN-кода.

5) ввести пароль пользователя;

6) нажать клавишу [Enter], осуществляется поиск сертификатов пользователей, расположенных на АН, во время поиска сертификатов отображается окно, приведенное на рис. 22;

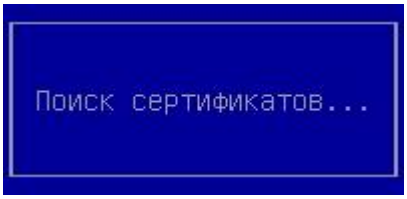

Рис. 22

7) после завершения поиска сертификатов пользователю предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов на странице *Локальная аутентификации* (рис. 23);

Страница Локальная аутентификация (вид 2),

выбор значения ключевого поля Общее имя (CN) из списка сертификатов пользователя

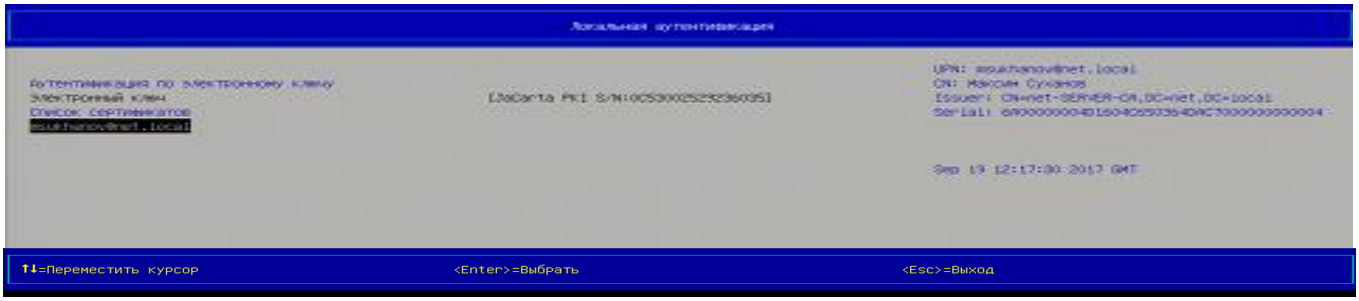

Рис. 23

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

9) нажать клавишу [Enter], после выполнения успешной аутентификации пользователю предлагается дождаться загрузки ОС или войти в оболочку KSS по клавише [F1] (см. рис. 21).

Примечания:

1. Процесс аутентификации пользователя выполняется после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2).

2. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)», – после завершения поиска сертификатов, пользователю предлагается выбрать универсальное имя из списка (рис. 24).

Страница Локальная аутентификация (вид 3),

выбор универсального имени сертификата

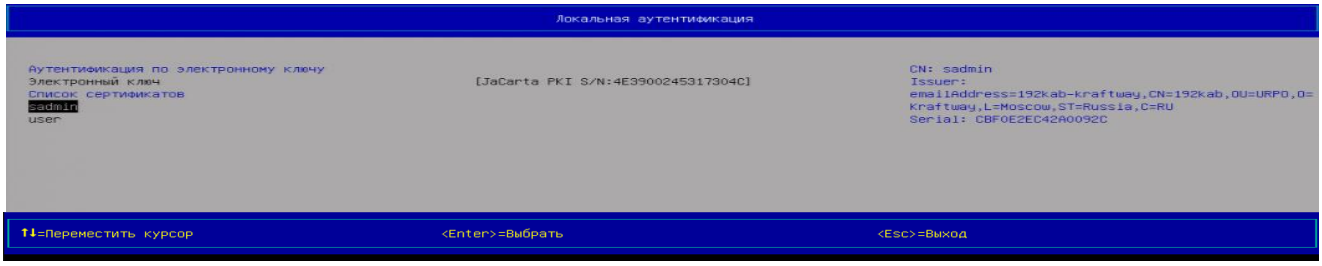

Рис. 24

3. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата», – после завершения поиска сертификатов, пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (рис. 25).

Страница Локальная аутентификация (вид 4), выбор серийного номера сертификата

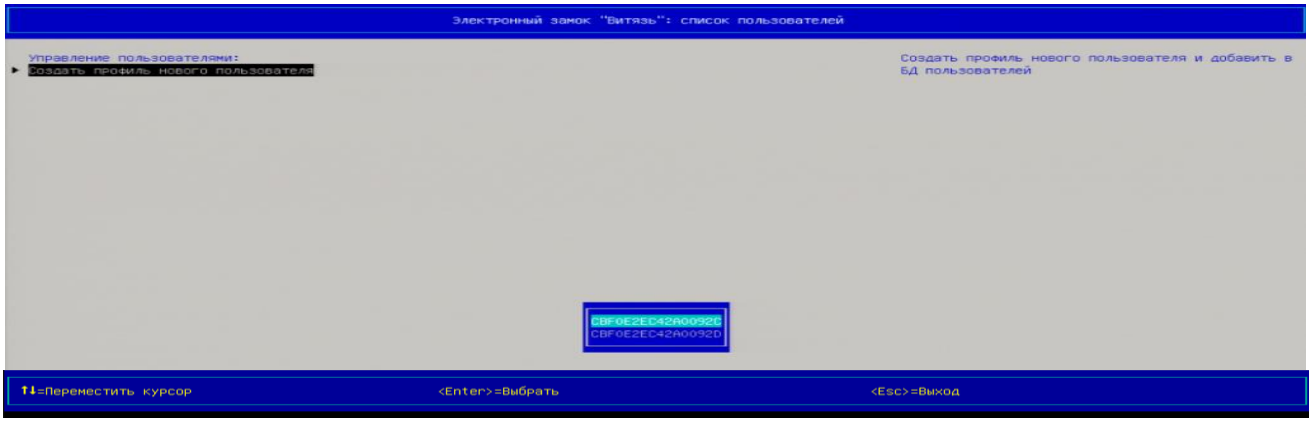

Рис. 25

2.1.4. Аутентификация администратора, вариант 3

Прохождение аутентификации пользователем при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)».

Для прохождения аутентификации следует выполнить действия, описанные в п. 2.1.3.

Примечания:

1. Процесс аутентификации пользователя выполняется после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006- 02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2).

2. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», – после завершения поиска сертификатов, пользователю предлагается выбрать универсальное имя из списка (см. рис. 24).

3. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Серийный номер сертификата», – после завершения поиска сертификатов, пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. рис. 25).

2.1.5. Дополнительные сведения о процедуре аутентификации

2.1.5.1. Проблемы при создании первого пользователя

При создании первого пользователя, если у администратора нет АН, и он вводит все параметры вручную, необходимо предельно точно вводить следующие значения:

серийный номер АН для авторизации по электронному ключу и уникальное имя;

общее имя и серийный номер сертификата для авторизации по цифровому сертификату.

Если данные будут введены с ошибкой, зайти в ПК «ЭЗ «ВИТЯЗЬ» 2.2 больше будет невозможно.

2.1.5.2. Аутентификация пользователей без сертификата УЦ

Аутентификация пользователей без сертификата допустима. Но так как добавление сертификата влечет выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2, то добавление некорректного УЦ влечет за собой отсутствие возможности включить модуль ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Отсутствие УЦ небезопасно, но аутентификация пользователей возможна.

При добавлении пользователя без УЦ выводится сообщение с предупреждением о том, что нет сертификатов УЦ и это небезопасно, хотя возможно.

Если добавлять сертификат УЦ с включенным ПК «ЭЗ «ВИТЯЗЬ» 2.2, то ПК «ЭЗ «ВИТЯЗЬ» 2.2 выключается. Это сделано для того, чтобы после добавления УЦ не заблокировать всех пользователей. Т.е. придется попытаться включить ПК «ЭЗ «ВИТЯЗЬ» 2.2, но если в нем уже заведены пользователи, то при включении будет производится авторизация с учетом нового сертификата УЦ.

2.1.5.3. Аутентификация пользователей с сертификатом УЦ

Если ранее в ПК «ЭЗ «ВИТЯЗЬ» 2.2 администратором был добавлен сертификат УЦ (см. п. 2.4.3), то во время аутентификации пользователя выполняется 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 KSS (см. рис. 1).

2.1.5.4. Особенности работы с картами Микрон

В картах Микрон PIN-код, если ранее не меняли, может быть задан в шестнадцатеричном представлении, что не позволяет ввести его в ПК «ЭЗ «ВИТЯЗЬ» 2.2. В этом случае PIN-код нужно сменить, используя стороннюю программу Smart Card Shell, скачать которую можно по адресу: http://www.openscdp.org/scsh3/.

Существуют два вида карт Микрон, с объектами 0x0B и 0x07:

1) card.sendApdu(0x00, 0x20, 0x00, 0x0B, new ByteString("949D1257815C6C64", HEX));

2) card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("0E2FC22362BCBC7D", HEX));

где, 949D1257815C6C64 – заводской PIN-код карты.

Последовательность команд для смены PIN-кода (для PIN-кода объекта 0x07, аналогично для 0x0B) следующая:

1) проверить, что заводской PIN-код подходит:

```
card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("0E2FC22362BCBC7D", HEX))
```

2) сменить на «12345678»:

```
card.sendApdu(0x00, 0x24, 0x00, 0x07, new ByteString("0E2FC22362BCBC7D3132333435363738", HEX))
```

3) проверить новый PIN-код «12345678»:

```
card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("3132333435363738", HEX))
```

Примечание. Результат проверки сертификата пользователя на подлинность считается положительным, если сертификат пользователя, размещенный в защищенной области АН, был подписан с помощью сертификата УЦ, а данный сертификат УЦ, в свою очередь, был добавлен в ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. п. 2.4.3). Результат проверки сертификата пользователя на подлинность считается отрицательным, если:

1) сертификат пользователя, размещенный в защищенной области АН, был подписан с помощью сертификата УЦ, который не был добавлен в ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. п. 2.4.3);

2) сертификат пользователя, размещенный в защищенной области АН, не был подписан с помощью какого-либо сертификата УЦ, а является самозаверенным сертификатом.

2.2. Работа со списком пользователей

2.2.1. Просмотр списка пользователей

Для просмотра списка пользователей следует:

1) выбрать п. *Электронный замок «Витязь»* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (рис. 26);

Страница *Электронный замок «Витязь»* (вид 1), после создания первого администратора

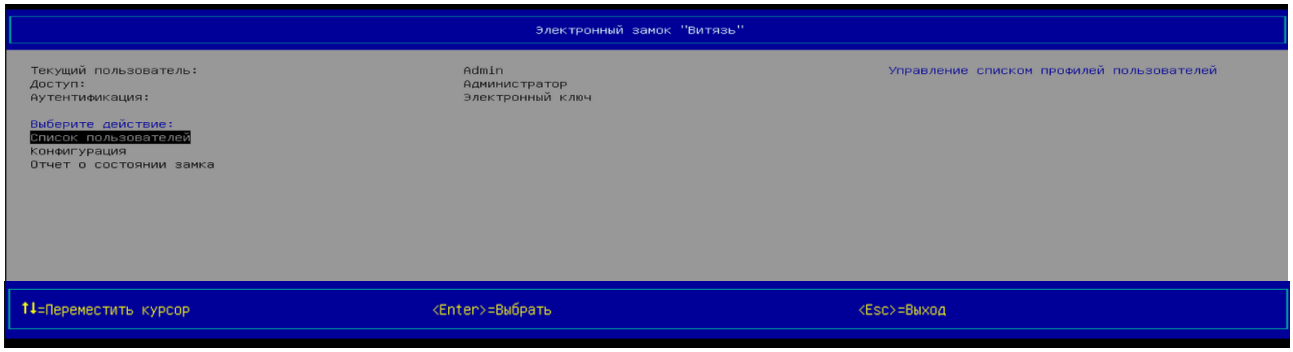

Рис. 26

3) выбрать п. *Список пользователей* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: список пользователей* (рис. 27 - 30), на которой представлен список профилей пользователей;

Страница *Электронный замок «Витязь»: список пользователей* (вид 1),

созданы профили пользователей, *Способ аутентификации* – «Электронный ключ»

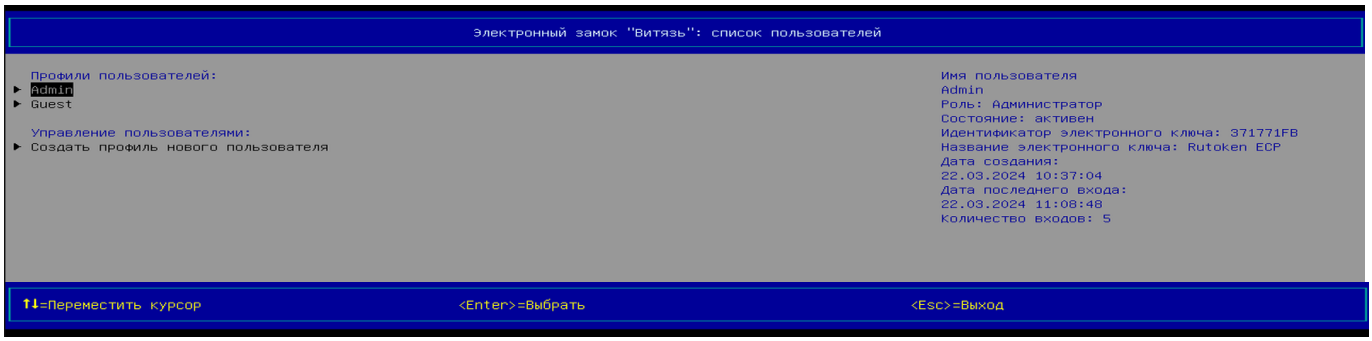

Рис. 27

Страница *Электронный замок «Витязь»: список пользователей* (вид 2),

созданы профили пользователей, *Способ аутентификации* – «Цифровой сертификат»,

Ключевое поле – «Общее имя (CN)»

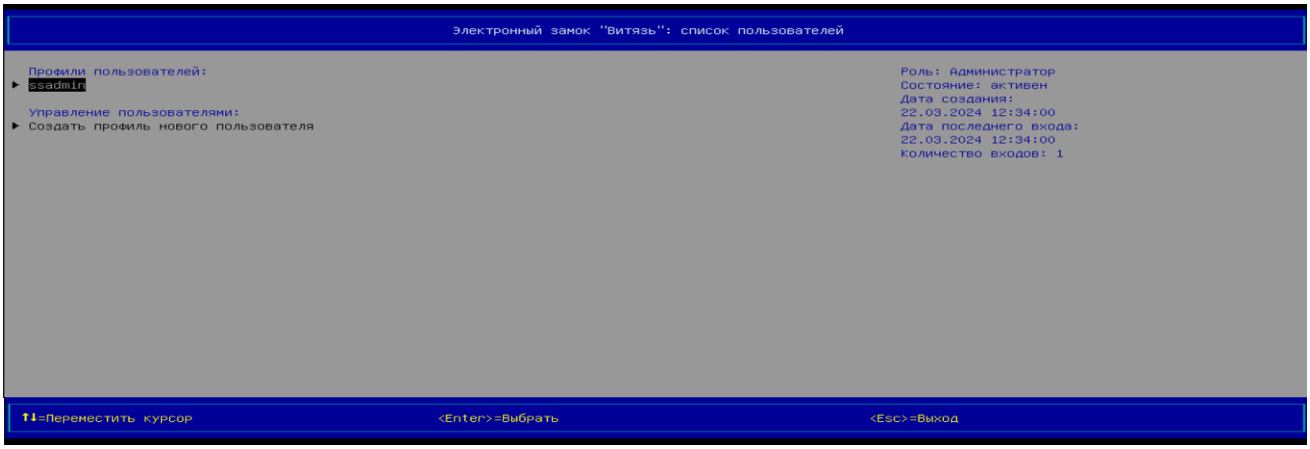

Рис. 28

Страница Электронный замок «Витязь»: список пользователей (вид 3),

созданы профили пользователей, Способ аутентификации – «Цифровой сертификат»,

Ключевое поле – «Универсальное имя (UPN)»

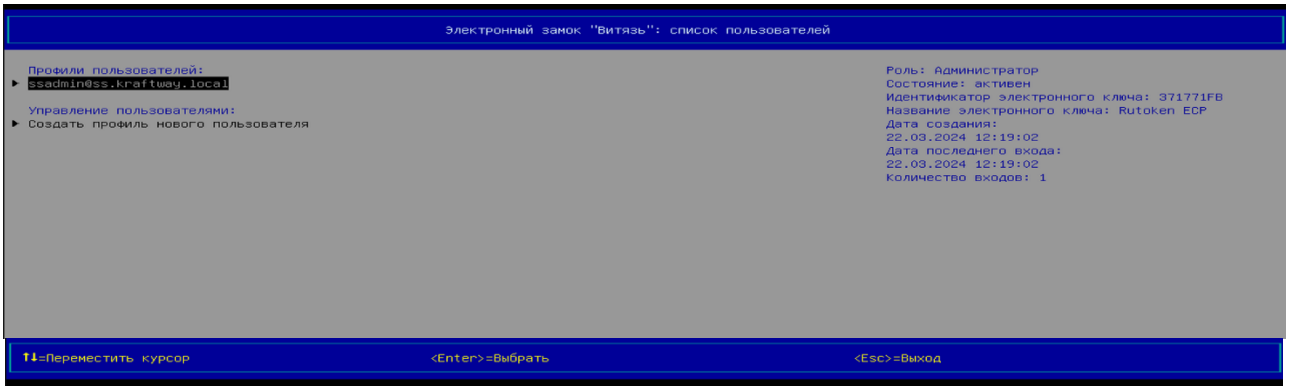

Рис. 29

Страница Электронный замок «Витязь»: список пользователей (вид 4),

созданы профили пользователей, Способ аутентификации – «Цифровой сертификат»,

Ключевое поле – «Серийный номер сертификата»

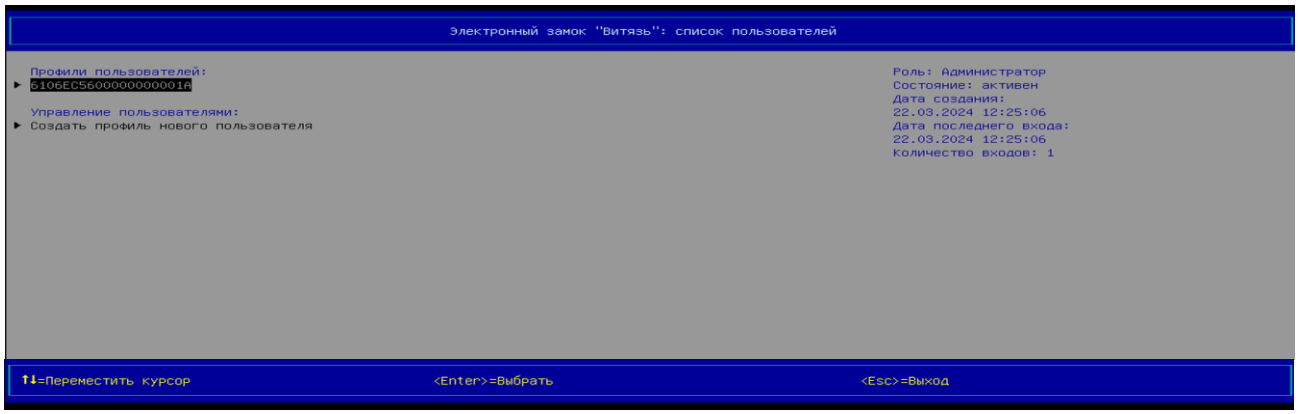

Рис. 30

Примечания:

1. Просмотр списка пользователей возможен только после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2), создания хотя бы одного профиля пользователя.

2. При выборе профиля пользователя из списка профилей в правой части области № 2 страницы 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, определенное для пользователя администратором*.

Объем выводимой дополнительной информации о профиле пользователя зависит от способа аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 и роли пользователя.

3. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *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 аналогична тем страницам, что представлены на рис. 26 - 30, когда параметру *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 страницы. Т.е. представление дополнительной информации о профиле пользователя в правой части области № 2 страницы *Электронный замок «Витязь»: список пользователей* идентично представлению дополнительной информации при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ» (см. рис. 27).

2.2.2. Создание профиля нового пользователя

Процедура создания профиля нового пользователя практически идентична процедуре создания профиля первого администратора (см. п. 2.1.1). При создании профиля нового пользователя можно присваивать значения параметру *Роль пользователя* (см. рис. 11, 15).

Создание профиля пользователя при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)», использование АН пользователя при создании профиля пользователя.

Для создания профиля нового пользователя следует:

1) выбрать п. *Электронный замок «Витязь»* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»*;

3) выбрать п. *Список пользователей* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: список пользователей* (рис. 31), на которой предлагается создать профиль нового пользователя;

Страница *Электронный замок «Витязь»: список пользователей* (вид 6),

создан профиль первого администратора

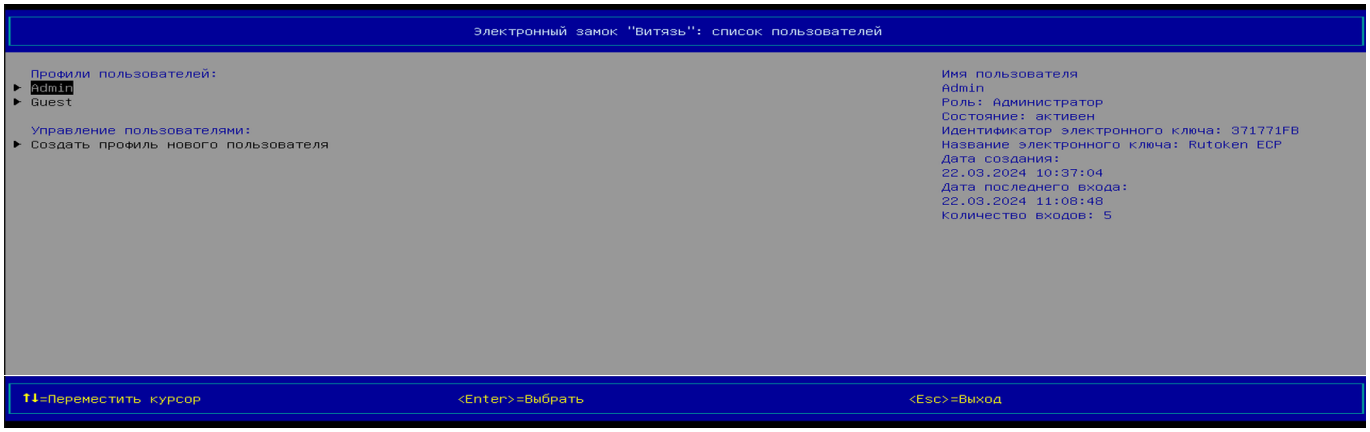

Рис. 31

5) выбрать п. *Создать профиль нового пользователя* раздела *Управление пользователями*;

6) нажать клавишу [Enter], отображается окно (см. рис. 7), предлагающее администратору выбрать одно из следующих действий: использовать АН при создании профиля пользователя, не использовать АН при создании профиля пользователя;

7) нажать клавишу [Enter], отображается окно (см. рис. 8), предлагающее подключить АН пользователя к USB-порту;

8) подключить АН пользователя, для которого создается профиль, к USB-порту;

9) нажать клавишу [Enter], отображается окно для ввода пароля пользователя (см. рис. 9);

10) ввести пароль пользователя;

11) нажать клавишу [Enter], отображается окно, информирующее о чтении списка сертификатов пользователей, после завершения чтения списка сертификатов отображается окно (см. рис. 10), в котором администратору предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов;

12) выбрать нужное значение и нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: создание нового профиля пользователя* (рис. 32);

Страница Электронный замок «Витязь»:

создание нового профиля пользователя (вид 3)

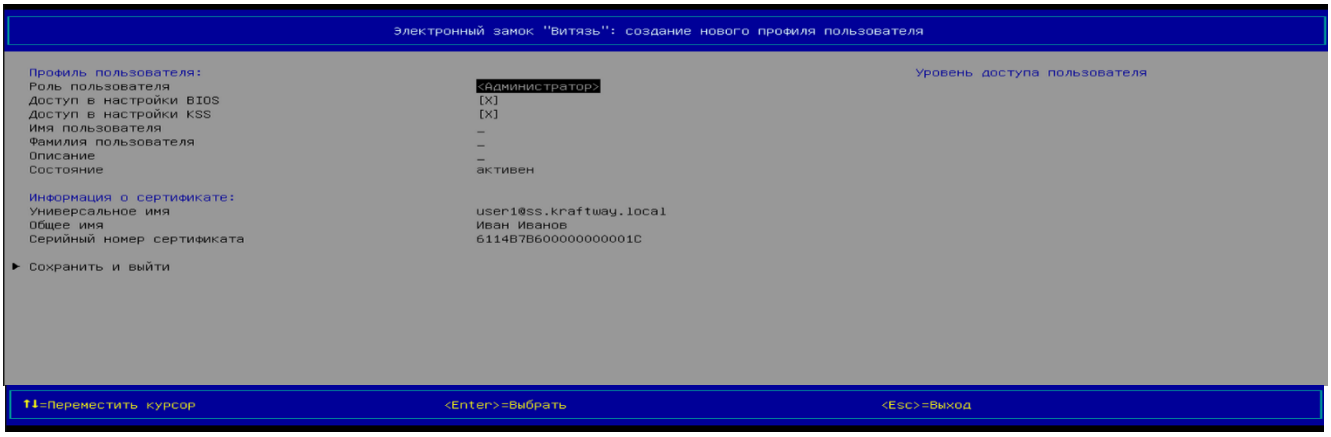

Рис. 32

13) выбрать параметр *Роль пользователя*;

14) нажать клавишу [Enter], отображается окно (рис. 33) для выбора роли пользователя;

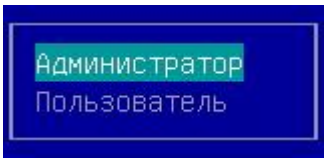

Рис. 33

15) выбрать требуемую роль пользователя и нажать клавишу [Enter];

16) выбрать параметр *Доступ в настройки BIOS* (параметр доступен только после присвоения параметру *Роль пользователя* значения «Администратор»);

17) разрешить или запретить доступ к настройкам BIOS (действие выполняется нажатием на клавишу [Пробел] после выбора параметра *Доступ в настройки BIOS*);

18) выбрать параметр *Доступ в настройки KSS* (параметр доступен только после присвоения параметру *Роль пользователя* значения «Администратор»);

19) разрешить или запретить доступ к настройкам KSS (действие выполняется нажатием на клавишу [Пробел] после выбора параметра *Доступ в настройки KSS*);

Примечание. Если на этом этапе создания нового профиля для способа аутентификации «Электронный ключ» выбрать п. *Сохранить и выйти*, то откроется окно предупреждения с текстом «Недостаточно информации». Необходимо ввести дополнительную информацию о пользователе (рис. 34).

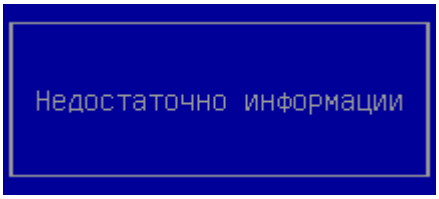

Рис. 34

20) выбрать параметр *Имя пользователя*, нажать клавишу [Enter], отображается окно для ввода имени пользователя;

21) ввести имя пользователя и нажать клавишу [Enter];

22) выбрать параметр *Фамилия пользователя*, нажать клавишу [Enter], отображается окно для ввода фамилии пользователя;

23) ввести фамилию пользователя и нажать клавишу [Enter];

24) выбрать параметр *Описание*, нажать клавишу [Enter], отображается окно для ввода описания пользователя;

25) ввести описание пользователя и нажать клавишу [Enter];

26) выбрать параметр *Максимальное количество попыток ввода пароля* (параметр доступен только после присвоения параметру *Роль пользователя* значения «Пользователь»);

27) нажать клавишу [Enter];

28) установить требуемое максимальное количество попыток ввода пароля клавишами цифрового блока клавиатуры (допустимые значения параметра: 1-4) и нажать клавишу [Enter];

29) выбрать п. *Сохранить и выйти* и нажать клавишу [Enter].

Примечания:

1. Создание профиля нового пользователя возможно только после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2), создания профиля первого администратора (см. п. 2.1.1).

2. Если при создании профиля пользователя было принято решение о создании данного профиля без использования АН, т.е. была нажата клавиша [ESC] (см. рис. 31), то тогда создание профиля пользователя продолжается на странице *Электронный замок «Витязь»: создание нового профиля пользователя* (см. рис. 15). При создании профиля пользователя без использования АН следует присвоить значения следующим параметрам:

– *Имя пользователя*;
– *Фамилия пользователя*;
– *Описание*;
– *Универсальное имя*;
– *Общее имя*;
– *Серийный номер сертификата*;
– *Ключ*;
– *Серийный номер ключа*.

Ввод значений перечисленных выше параметров выполняется в окнах, которые практически аналогичны тем, что представлены на рис. 12, 13, и отличаются только размерами.

3. Администратору следует быть предельно внимательным при вводе PIN-кода к АН. При инициализации (форматировании) АН с помощью ПК «ЭЗ «ВИТЯЗЬ» 2.2, идущего в комплекте с АН, администратором устанавливается максимальное количество попыток ввода PIN-кода. Максимальное количество попыток ввода PIN-кода различается для разных типов АН и определено в эксплуатационной документации на АН. Максимальное количество попыток ввода PIN-кода – это количество, как ранее было описано, которое задается в ПК «ЭЗ «ВИТЯЗЬ» 2.2, поставляемом с АН, и не имеет ничего общего со значением параметра *Максимальное количество попыток ввода пароля*, которое присваивается данному параметру при создании профиля нового пользователя.

4. Следует избегать ситуации, когда максимальное количество попыток ввода PIN-кода и значение, присваиваемое параметру *Максимальное количество попыток ввода пароля*, совпадают, т.к. при превышении значения любого из данных параметров (максимальное количество попыток ввода PIN-кода, *Максимальное количество попыток ввода пароля*) ПК «ЭЗ «ВИТЯЗЬ» 2.2 будет заблокирован профиль пользователя и заблокирован АН на аппаратном уровне. Максимальное количество попыток ввода PIN-кода накладывает ограничение со стороны конкретного АН, а не ПК «ЭЗ «ВИТЯЗЬ» 2.2. Превышение данного количества попыток ввода PIN-кода к АН приводит к блокировке этого АН на аппаратном уровне и к необходимости его повторной инициализации (форматированию).

5. Изменение языка ввода с английского на русский и наоборот выполняется клавишей [F9].

6. При следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ» – администратору не предлагается выбрать значение ключевого поля сертификата, и он не выполняет действия перечислений 11), 12) п. 2.1.1.

7. При следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Универсальное имя (UPN)» – администратору предлагается выбрать универсальное имя из списка (см. рис. 16).

8. При следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Серийный номер сертификата» – администратору предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. рис. 17).

9. При создании профилей для второго и последующих администраторов становятся доступными для изменения следующие параметры: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*.

10. При создании профиля пользователя с ролью *Администратор* параметр *Максимальное количество попыток ввода пароля* отсутствует на странице *Электронный замок «Витязь»: создание профиля нового пользователя* (см. рис. 11, 15, 32), а при создании профиля пользователя данный параметр присутствует (см. рис. 35), т.к. на администраторов не накладывается ограничение ПК «ЭЗ «ВИТЯЗЬ» 2.2 относительно максимального количества попыток ввода пароля. Ограничение относительно максимального количества попыток ввода пароля накладывается на администраторов только со стороны используемого АН. Данное количество устанавливается при инициализации АН с помощью программного обеспечения, идущего в комплекте с АН, и определенно в эксплуатационной документации на АН.

11. Общее количество пользователей, созданных в ПК «ЭЗ «ВИТЯЗЬ» 2.2, зависит от свободного объема памяти на микросхеме SPI Flash.

Страница Электронный замок «Витязь»: создание нового профиля пользователя (вид 4)

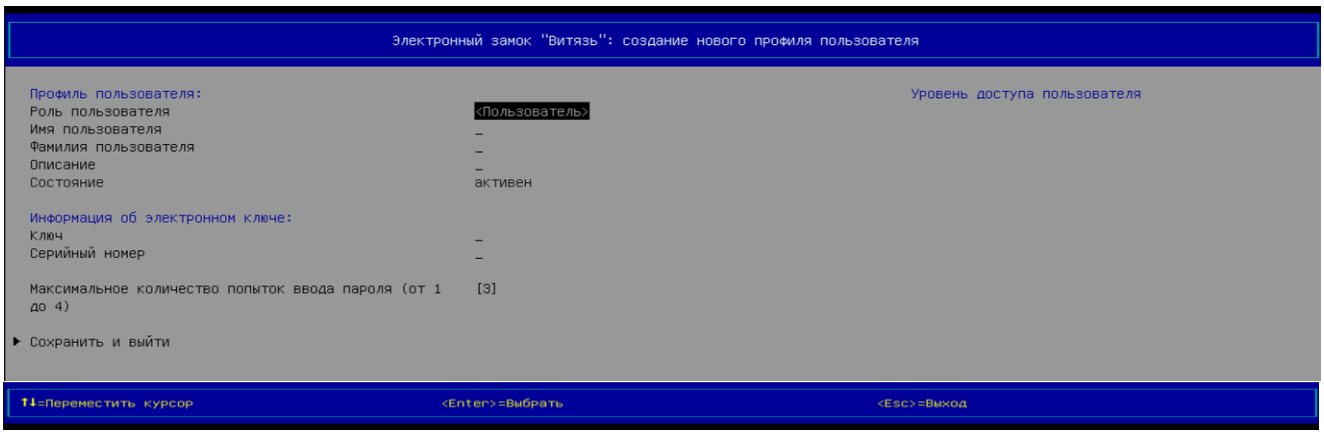

Рис. 35

2.2.3. Изменение способа аутентификации пользователя

Для изменения способа аутентификации пользователя следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (рис. 36);

Страница *Kraftway Secure Shell*, главное меню оболочки KSS

Рис. 36

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

Страница *Настройки*

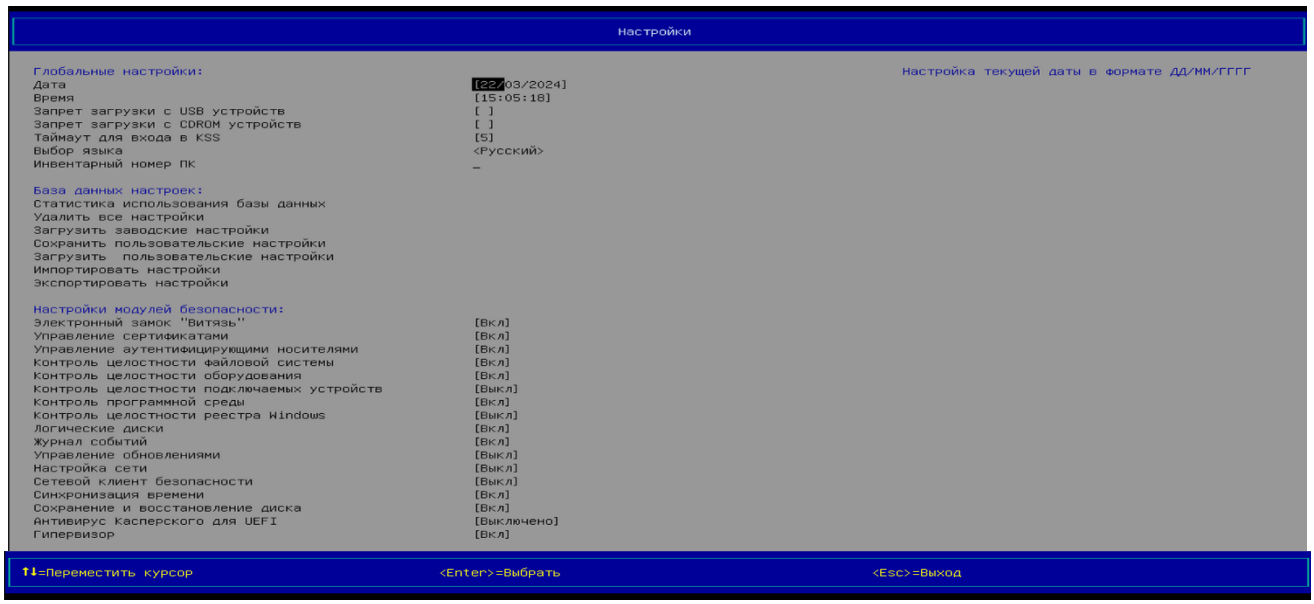

Рис. 37

3) выбрать п. *Электронный замок «Витязь»* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: Настройки* (см. рис. 38);

Страница Электронный замок «Витязь»: Настройки,

Способ аутентификации – «Цифровой сертификат», Ключевое поле – «Универсальное имя (UPN)»

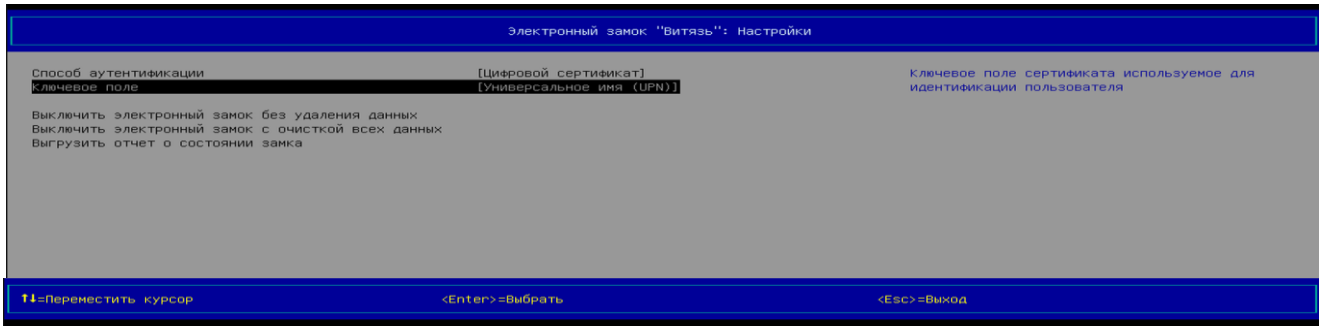

Рис. 38

5) выбрать п. *Способ аутентификации*;

6) нажать клавишу [Enter], отображается окно (рис. 39), предлагающее выбрать способ аутентификации пользователя (доступные значения параметра: «Цифровой сертификат», «Электронный ключ», «Цифровой сертификат и электронный ключ»);

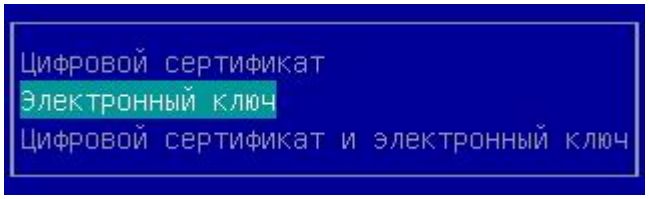

Рис. 39

7) выбрать требуемый способ аутентификации в окне;

8) нажать клавишу [Enter];

9) выбрать п. *Ключевое поле* (см. рис. 38, данный пункт отображается только, если параметру *Способ аутентификации* было присвоено значение «Цифровой сертификат» или «Цифровой сертификат и электронный ключ»;

10) нажать клавишу [Enter], отображается окно (рис. 40), предлагающее выбрать ключевое поле сертификата пользователя, с помощью которого будет выполняться аутентификация пользователя (доступные значения параметра: «Универсальное имя (UPN)», «Общее имя (CN)», «Серийный номер сертификата»);

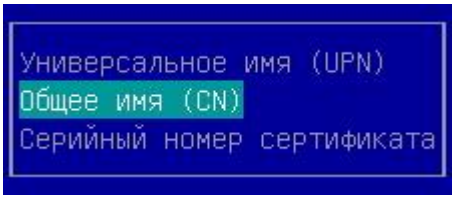

Рис. 40

11) выбрать ключевое поле и нажать клавишу [Enter].

Примечания:

1. При попытке назначения параметрам: *Способ аутентификации*, *Ключевое поле* новых значений, отображается окно (рис. 41), запрашивающее подтверждение на внесение изменений.

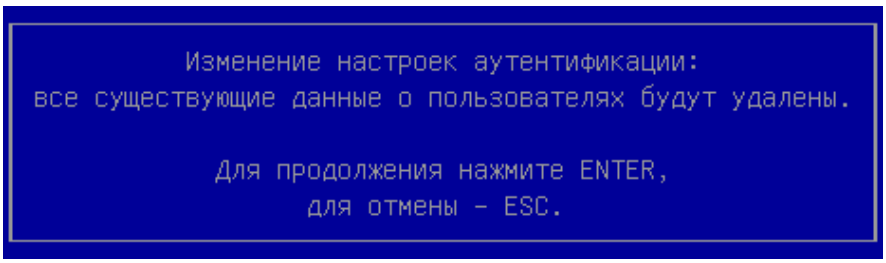

Рис. 41

2. Пункт *Ключевое поле* не выводится на странице *Электронный замок «Витязь»: Настройки* (рис. 42), если параметру *Способ аутентификации* было присвоено значение «Электронный ключ».

Страница *Электронный замок «Витязь»: Настройки* (вид 3),

подтверждения на внесение изменений

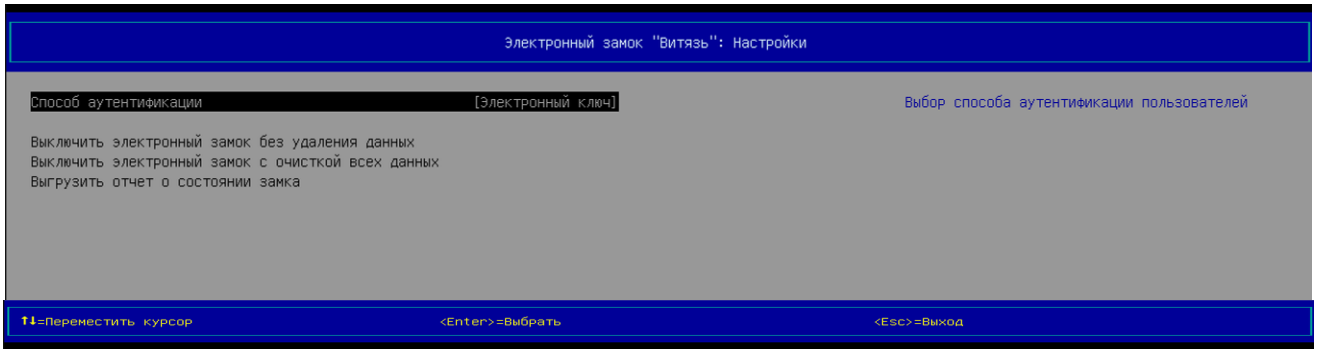

Рис. 42

3. После включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 отображение статуса модуля *Электронный замок «Витязь»* меняется с «Выкл» на «Вкл» на странице *Настройки* (рис. 37).

4. Настоятельно рекомендуется создать профиль для второго администратора (второй профиль с ролью «администратор»). Вторым профилем с ролью «администратор» можно воспользоваться при невозможности аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 при использовании первого профиля с ролью «администратор», например, если: АН первого администратора инициализировано или испорчено, или утеряно.

5. Изменение способа аутентификации пользователя возможно только после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2).

2.2.4. Изменение профиля пользователя

Для изменения профиля пользователя следует:

1) выполнить действия перечислений 1) – 4) п. 2.2.1;

2) выбрать требуемый профиль пользователя раздела *Профили пользователей* (см. рис. 27 - 30);

3) нажать клавишу [Enter], отображается окно (рис. 43, 57), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

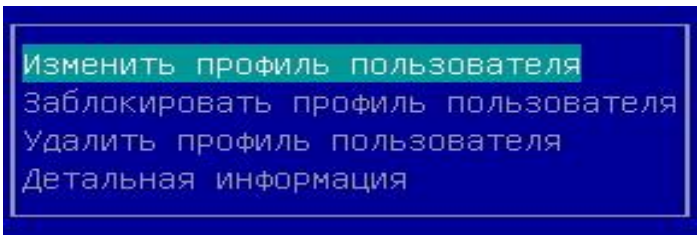

Рис. 43

4) выбрать п. *Изменить профиль пользователя* в окне выбора;

5) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»*: изменение профиля пользователя (рис. 44 - 49);

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

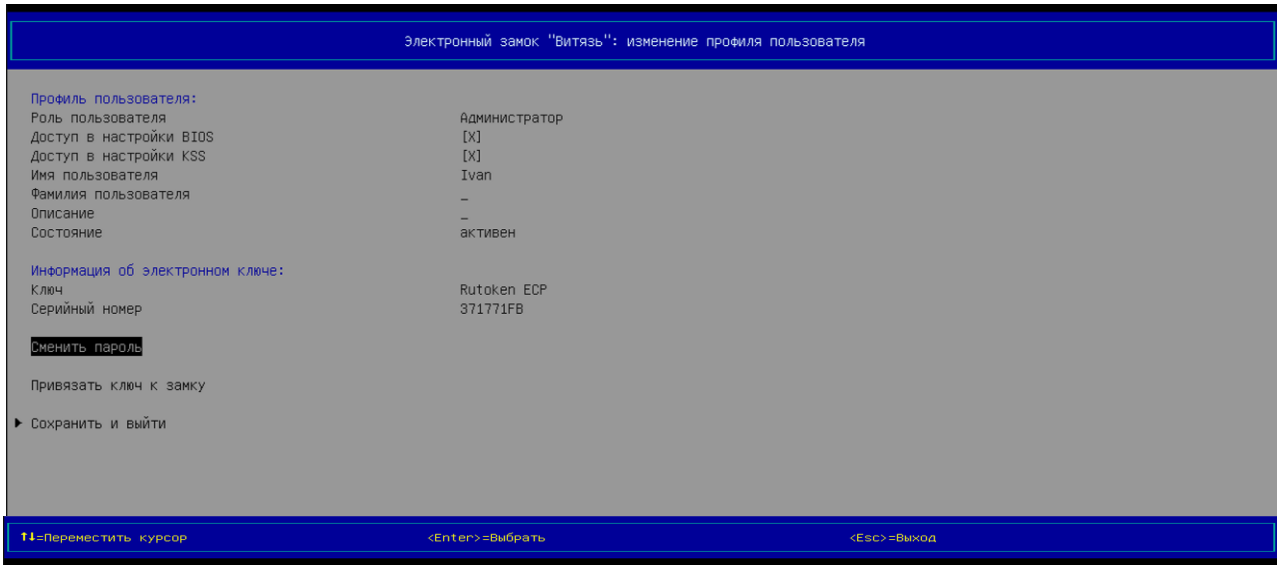

Рис. 44

Страница *Электронный замок «Витязь»: изменения профиля пользователя*, профиль администратора, *Способ аутентификации* – «Электронный ключ»

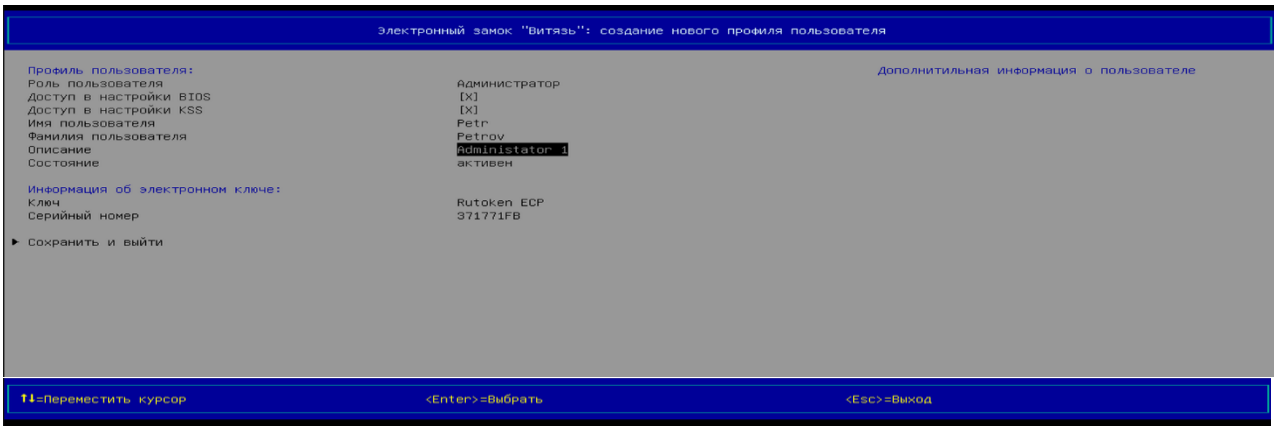

Рис. 45

Страница *Электронный замок «Витязь»: изменения профиля пользователя* (вид 3), профиль пользователя, *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

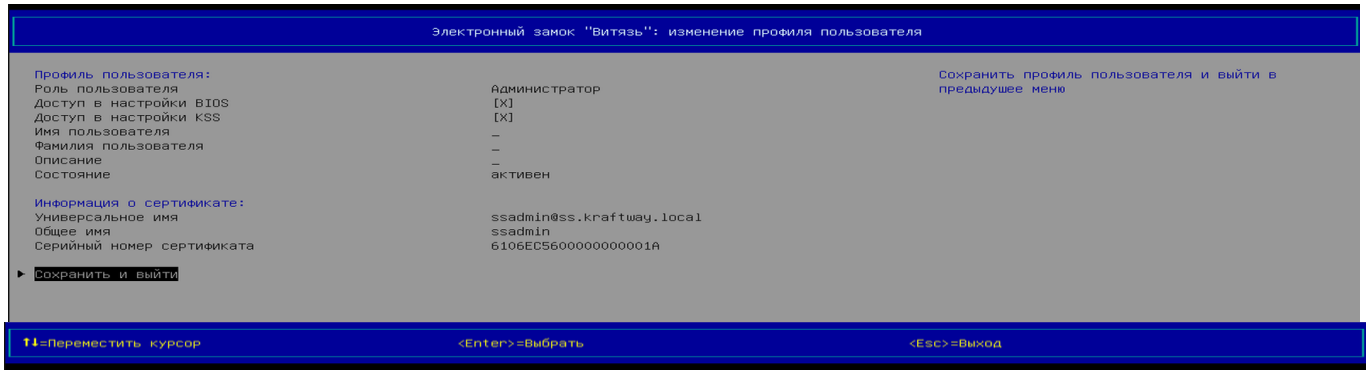

Рис. 46

Страница *Электронный замок «Витязь»: изменения профиля пользователя* (вид 4), профиль администратора, *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

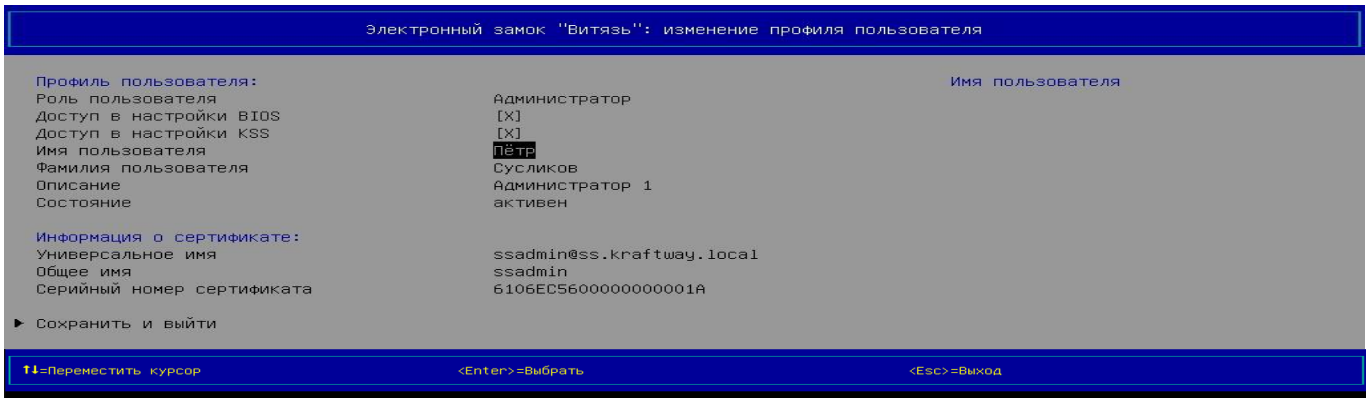

Рис. 47

Страница *Электронный замок «Витязь»: изменения профиля пользователя* (вид 5), профиль пользователя, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)» или «Универсальное имя (UPN)» или «Серийный номер сертификата»

Рис. 48

Страница *Электронный замок «Витязь»: изменения профиля пользователя* (вид 6), профиль администратора, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)» или «Универсальное имя (UPN)» или «Серийный номер сертификата»

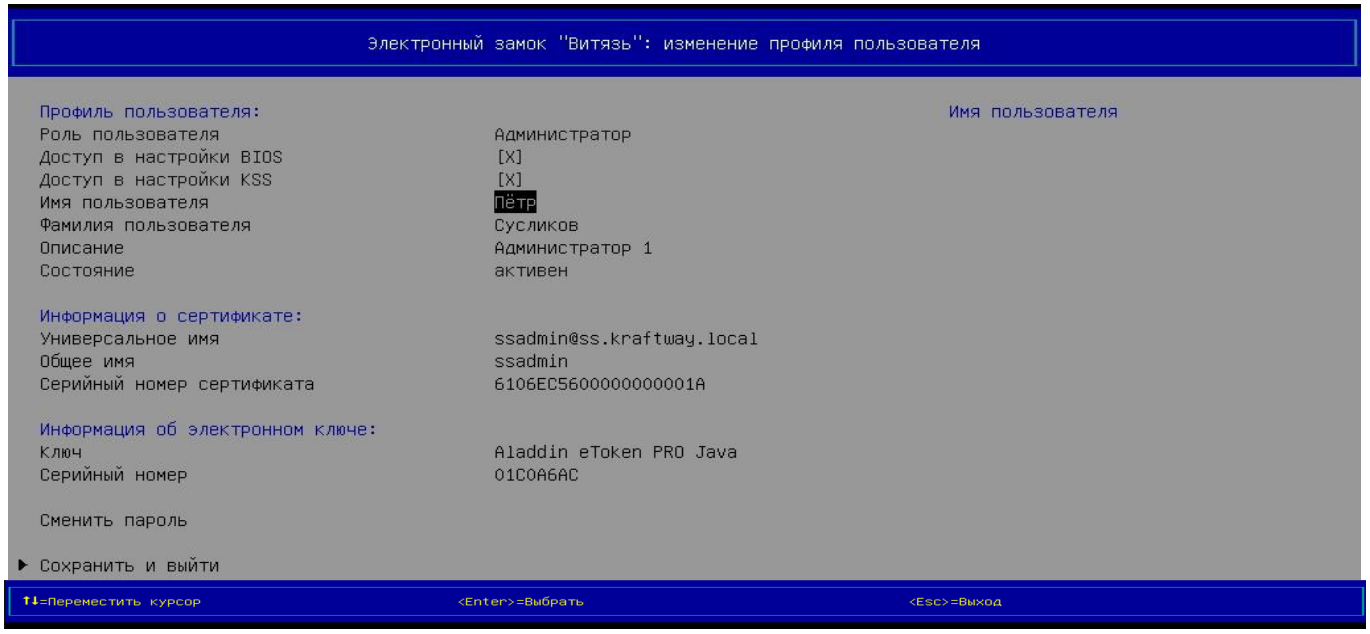

Рис. 49

6) изменить значения требуемых параметров (*Роль пользователя, Имя пользователя, Фамилия пользователя, Описание, Универсальное имя, Общее имя, Серийный номер сертификата, Ключ, Серийный номер, Максимальное количество попыток ввода пароля*) аналогичным способом, что описан в подразделе 2.2;

7) изменить пароль пользователя при необходимости (см. п. 3.2.1);

8) выбрать п. *Сохранить и выйти* и нажать клавишу [Enter].

Примечания:

1. Изменение профиля пользователя возможно только после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2), создания профиля первого администратора (см. п. 2.1.1).

2. При изменении профиля администратора, созданного первым, нельзя изменить значения следующих параметров: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*, т.к. данные параметры недоступны для изменения (см. рис. 11, 15). Таким образом, администратор, для которого был создан профиль первого администратора, всегда имеет доступ к настройкам BIOS материнской платы и к настройкам оболочки KSS.

3. При изменении профилей второго и последующих администраторов ПК «ЭЗ «ВИТЯЗЬ» 2.2 становятся доступными для изменения следующие параметры: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*.

4. Администратор, который прошел процедуру аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 и обладает правом доступа к настройкам KSS, имеет возможность изменить значения параметров профиля администратора, созданного первым, кроме следующих: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*.

5. Администратор, который прошел процедуру аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 и обладает правом доступа к настройкам KSS, имеет возможность изменить значения любых параметров профиля какого-либо другого администратора, кроме профиля первого администратора (см. п. 4 данного примечания) и самого себя.

6. Изменять значения параметра *Роль пользователя* можно в профилях пользователей и в профилях администраторов (кроме первого).

7. При присвоении значений параметрам: *Универсальное имя*, *Общее имя*, *Серийный номер сертификата*, *Ключ*, *Серийный номер* – администратору следует быть предельно внимательным.

8. При следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок «Витязь»: изменения профиля пользователя* (см. рис. 46, 47). При данном способе аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 изменить пароль пользователя нельзя (см. п. 3.2.1).

9. При изменении профиля пользователя с ролью *Администратор* параметр *Максимальное количество попыток ввода пароля* отсутствует на странице *Электронный замок «Витязь»: изменение профиля пользователя* (см. рис. 45, 47, 49), т.к. на администраторов ПК «ЭЗ «ВИТЯЗЬ» 2.2 не накладывается ограничение ПК «ЭЗ «ВИТЯЗЬ» 2.2 относительно максимального количества попыток ввода пароля. Ограничение относительно максимального количества попыток ввода пароля накладывается на администраторов ПК «ЭЗ «ВИТЯЗЬ» 2.2 только со стороны используемого АН. Данное количество устанавливается при инициализации АН с помощью программного обеспечения, идущего в комплекте с АН, и определено в эксплуатационной документации на АН.

2.2.5. Изменение пароля пользователя

Для изменения пароля пользователя следует:

1) выполнить действия перечислений 1) – 4) п. 2.2.1;

2) выбрать параметр *Сменить пароль*;

3) подключить АН пользователя к USB-порту, PIN-код которого подлежит изменению;

4) нажать клавишу [Enter], отображается окно для ввода старого пароля пользователя (рис. 50);

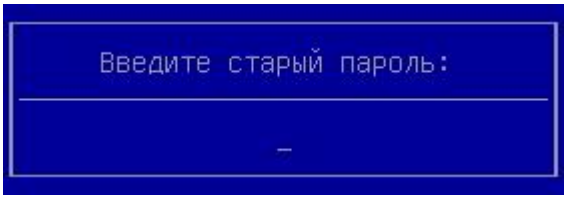

Рис. 50

5) ввести старый пароль в окно;

6) нажать клавишу [Enter], отображается окно для ввода нового пароля пользователя (рис. 51);

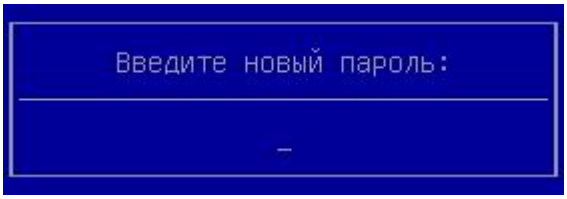

Рис. 51

7) ввести новый пароль пользователя;

8) нажать клавишу [Enter], отображается окно для подтверждения нового пароля пользователя (рис. 52);

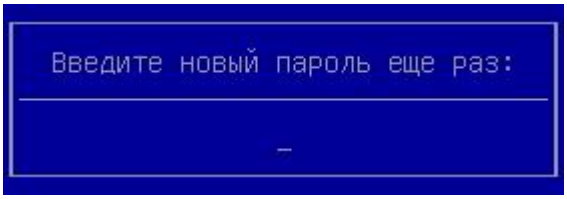

Рис. 52

9) ввести новый пароль пользователя;

10) нажать клавишу [Enter], отображается окно (рис. 53), информирующее об успешном изменении пароля;

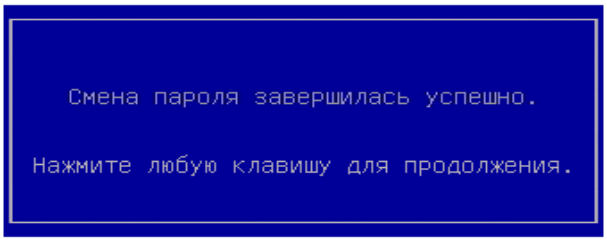

Рис. 53

11) нажать любую клавишу на клавиатуре.

Примечания:

1. Изменение пароля пользователя возможно только после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2), создания профиля первого администратора (см. п. 2.1.1).

2. Администратору предоставляется возможность изменения пароля пользователя при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – или «Электронный ключ», «Цифровой сертификат и электронный ключ».

3. При следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок «Витязь»: изменения профиля пользователя* (см. рис. 46, 47).

2.2.6. Блокировка профиля пользователя

Для выполнения блокировки профиля пользователя следует:

1) выполнить действия перечислений 1) – 3) п. 2.2.1;

2) выбрать п. Заблокировать профиль пользователя в окне (см. рис. 43);

3) нажать клавишу [Enter], отображается диалоговое окно (рис. 54), запрашивающее подтверждение на блокировку профиля пользователя;

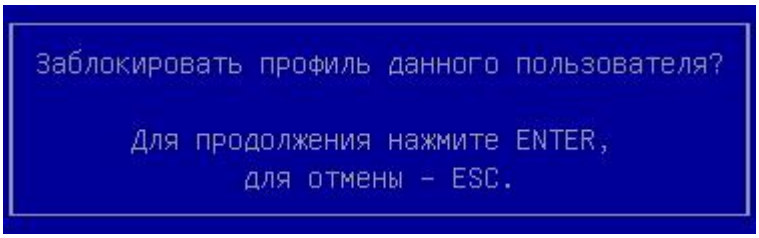

Рис. 54

4) нажать клавишу [Enter], состояние пользователя меняется с «активен» на «заблокирован» (см. рис. 55).

Страница *Электронный замок «Витязь»: список пользователей* (вид 7),

состояние профиля пользователя – «заблокирован»

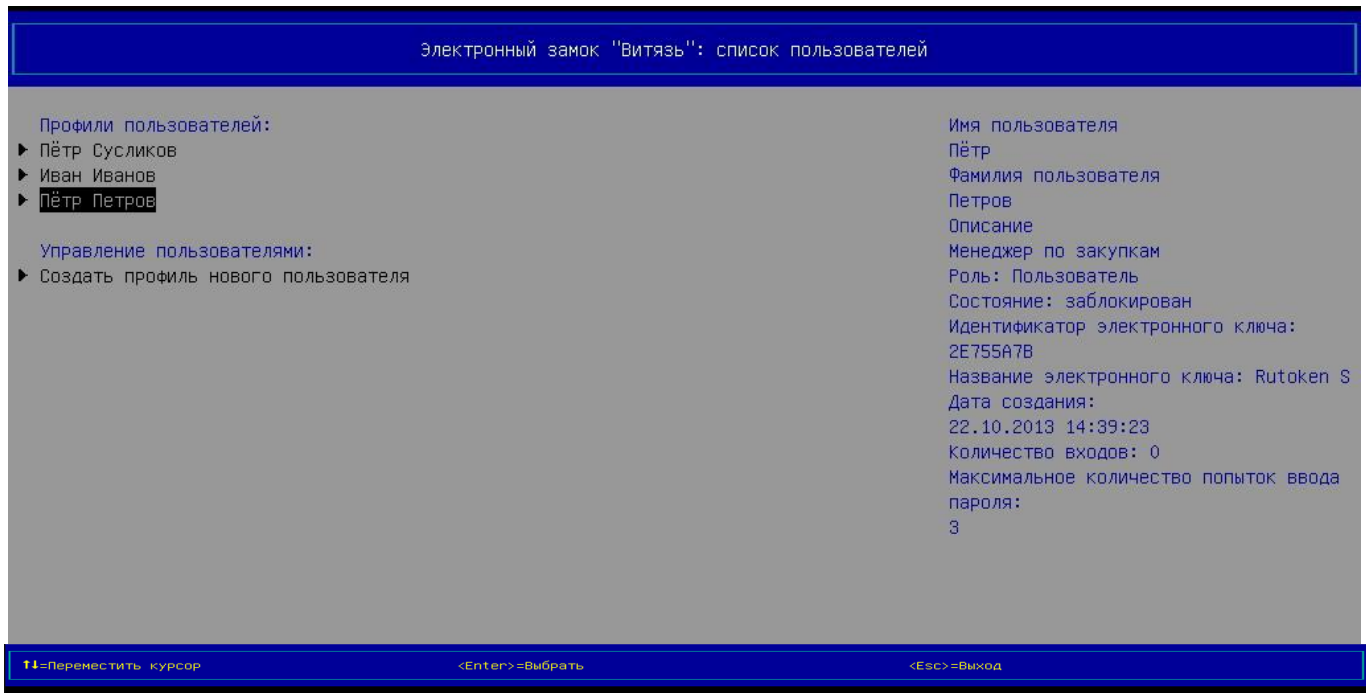

Рис. 55

Примечания:

1. Блокировка профиля пользователя возможна только при следующих условиях:

– включен модуль безопасности *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2);

– создан профиль первого администратора (см. п. 2.1.1);

– создан хотя бы один профиль пользователя или второй профиль администратора, который обладает правом доступа к настройкам KSS.

2. При последовательном, неправильном вводе PIN-кода к АН максимально допустимое число раз, определенное администратором для профиля пользователя, профиль пользователя блокируется ПК «ЭЗ «ВИТЯЗЬ» 2.2.

3. Если в ПК «ЭЗ «ВИТЯЗЬ» 2.2 был создан профиль только для одного администратора, то выполнить блокировку его профиля невозможно. При попытке заблокировать единственный профиль администратора отображается окно следующего вида (рис. 56).

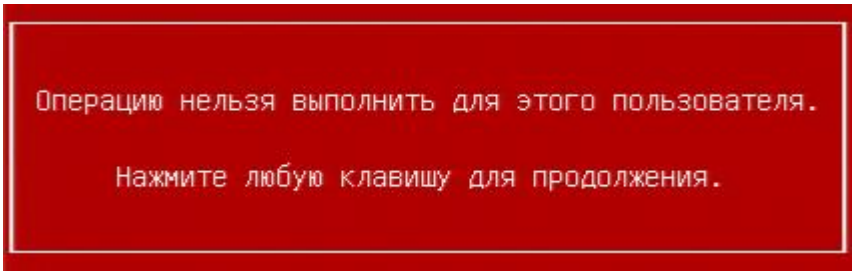

Рис. 56

4. Невозможно заблокировать профиль администратора, который выполнил вход в оболочку KSS. При попытке блокировки его профиля отображается окно следующего вида (см. рис. 56).

2.2.7. Разблокировка профиля пользователя

Для разблокировки профиля пользователя следует:

1) выполнить действия перечислений 1) – 4) п. 2.2.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см. рис. 27 - 30);

3) нажать клавишу [Enter], отображается окно (рис. 57), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

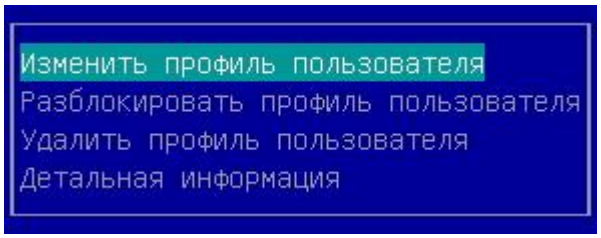

Рис. 57

4) выбрать п. *Разблокировать профиль пользователя* в окне выбора;

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 58), запрашивающее подтверждение на разблокировку профиля пользователя;

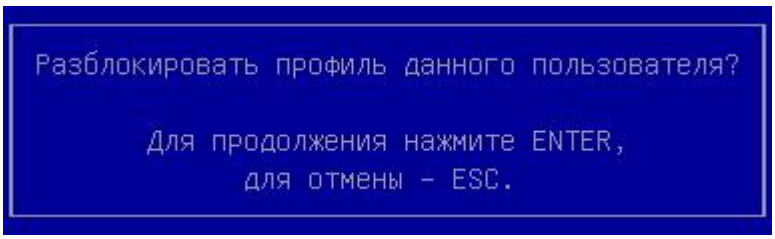

Рис. 58

6) нажать клавишу [Enter], состояние профиля пользователя меняется с «заблокирован» на «активен» (рис. 59).

Страница *Электронный замок «Витязь»: список пользователей* (вид 8),

состояние профиля пользователя – «активен»

Рис. 59

Примечание. Разблокировка профиля пользователя возможна только при выполнении следующих условий:

– включен модуль *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2);

– создан профиль первого администратора (см. п. 2.1.1);

– создан хотя бы один профиль пользователя или второй профиль администратора, который обладает правом доступа к настройкам KSS.

2.2.8. Удаление профиля пользователя

Для удаления профиля пользователя следует:

1) выполнить действия перечислений 1) – 4) п. 2.2.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см. рис. 27 - 30);

3) нажать клавишу [Enter], отображается окно (см. рис. 43, 57), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

4) выбрать п. *Удалить профиль пользователя* в окне (см. рис. 43, 57);

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 60) для подтверждения удаления профиля пользователя;

Рис. 60

6) нажать клавишу [Enter], профиль пользователя удаляется.

Примечания:

1. Удаление профиля пользователя возможно только при выполнении следующих условий:

–создан профиль первого администратора (см. п. 2.1.1);

–создан хотя бы один профиль пользователя или второй профиль администратора, который обладает правом доступа к настройкам KSS.

2. Если в ПК «ЭЗ «ВИТЯЗЬ» 2.2 был создан только один администратор, то выполнить удаление его профиля невозможно. При попытке удалить единственный профиль администратора отображается окно следующего вида (см. рис. 56).

3. Невозможно удалить профиль администратора, который выполнил вход в оболочку KSS. При попытке удаления его профиля отображается окно следующего вида (см. рис. 56).

4. Какой-либо администратор, который обладает правом доступа к настройкам KSS, после удаления профиля первого администратора становится первым администратором, а его профиль становиться профилем первого администратора, т.е. профилем, в котором нельзя изменять значения следующих параметров: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*.

2.2.9. Вывод детальной информации о пользователе

Для вывода детальной информации о пользователе следует:

1) выполнить действия перечислений 1) – 4) п. 2.2.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см. рис. 27 - 30);

3) нажать клавишу [Enter], отображается окно (см. рис. 43, 57), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

4) выбрать п. *Детальная информация* в диалоговом окне;

5) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: детальная информация о пользователе* (рис. 61, 62).

Страница *Электронный замок «Витязь»: детальная информация о пользователе*, профиль пользователя, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

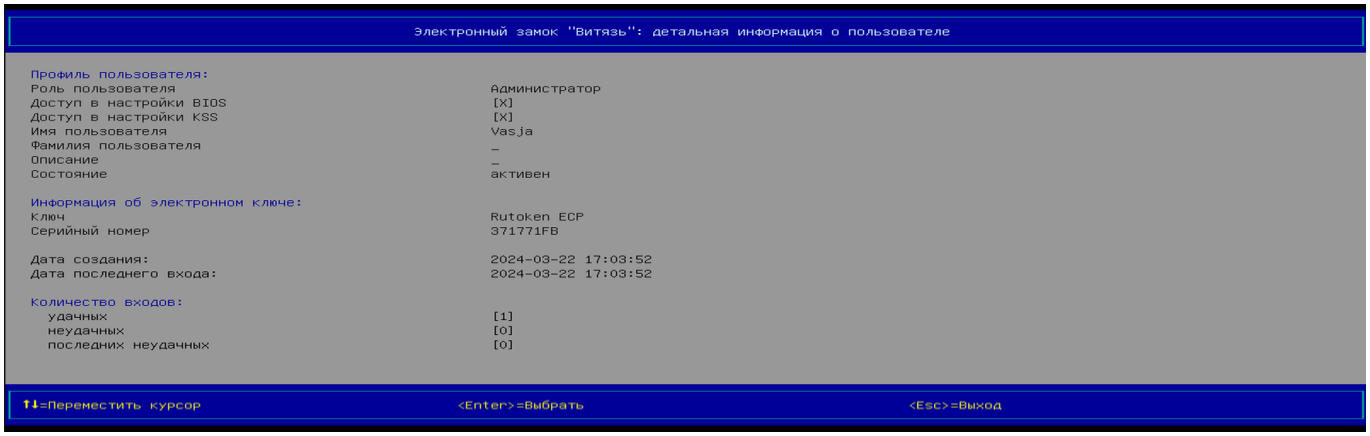

Рис. 61

Страница *Электронный замок «Витязь»: детальная информация о пользователе*, профиль администратора, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

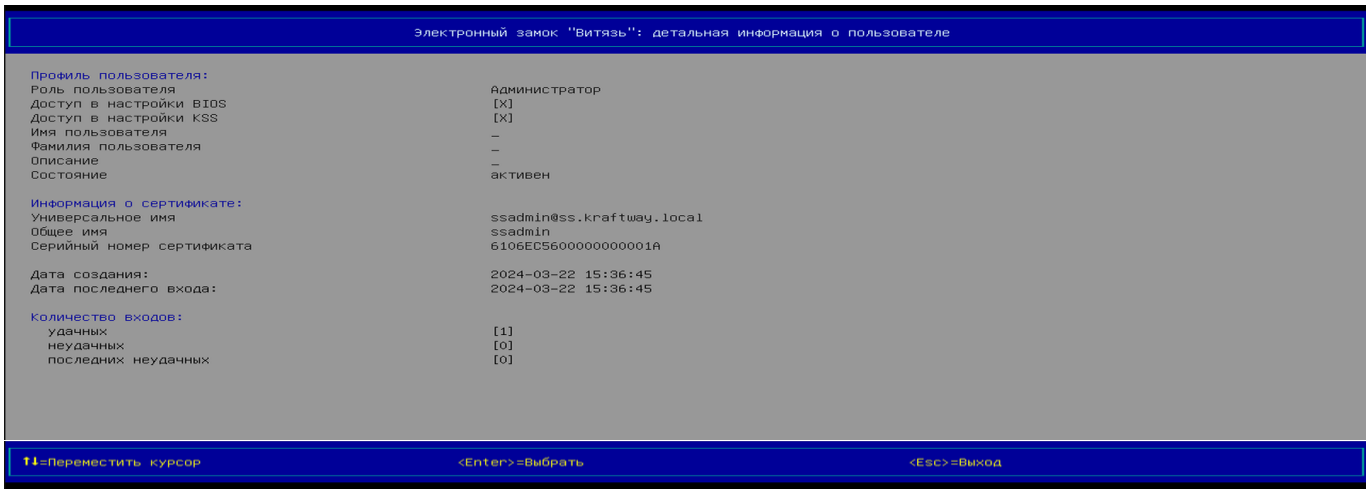

Рис. 62

Примечания:

1. Вывод детальной информации о пользователе возможен после включения модуля *Электронный замок «Витязь»* (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2), создания профиля первого администратора (см. п. 2.1.1).

2. Количество параметров и их значений, выводимых на странице *Электронный замок «Витязь»: детальная информация о пользователе* (см. рис. 61, 62), зависит от способа аутентификации, который был установлен администратором в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2, и от профиля пользователя, детальную информацию о котором требуется вывести и просмотреть. Может быть выведена следующая информация о пользователе:

– роль пользователя (Администратор или Пользователь);

– доступ к настройкам BIOS (только для профиля пользователя с ролью Администратор);

– доступ к настройкам KSS (только для профиля пользователя с ролью Администратор);

– имя пользователя;

– фамилия пользователя;

– описание пользователя (например, должность);

– состояние профиля пользователя (активен или заблокирован);

– информация о сертификате – универсальное имя, общее имя, серийный номер сертификата;

– информация об электронном ключе – ключ и серийный номер;

– даты создания и последнего входа пользователя;

– количество входов – удачных, неудачных и последних неудачных;

– максимальное количество попыток ввода пароля.

3. Количество последних неудачных входов – это количество попыток аутентификации, результаты которых были отрицательными. Если хотя бы один раз, после нескольких неудачных попыток аутентификации, пользователь прошел процедуру аутентификации с положительным результатом, то количество последних неудачных входов обнуляется.

4. Сведения о максимальном количестве попыток ввода пароля приводится только для профилей пользователей, а для профилей администраторов данная информация не приводится.

2.3. Контроль целостности ПК «ЭЗ «ВИТЯЗЬ» 2.2

При каждом включении компьютера выполняется процедура КЦ программных модулей ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Для вывода результата последней процедуры КЦ следует:

1) выбрать п. *Контроль модулей безопасности* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль модулей безопасности* (рис. 63);

Страница *Контроль модулей безопасности*

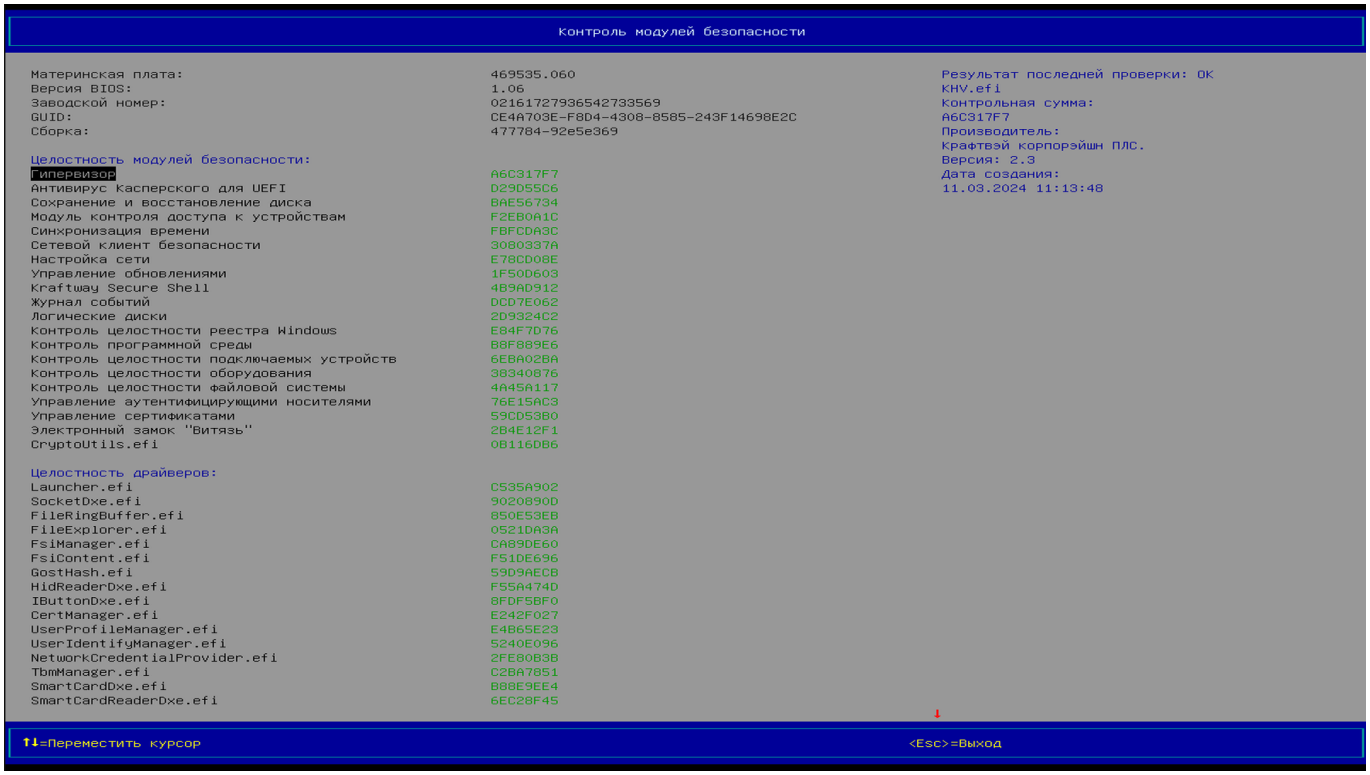

Рис. 63

3) выбрать модуль безопасности в разделе *Целостность модулей безопасности* или драйвер в разделе *Целостность драйверов* клавишами [↑], [↓], для отображения КС и дополнительной информации по выбранному модулю/драйверу.

Примечания:

1. Справа от названия модуля/драйвера ПК «ЭЗ «ВИТЯЗЬ» 2.2 (или оболочки KSS) приводится его КС в формате: XXXXXXXX, где X – шестнадцатеричная цифра в диапазоне от 0 до F, например, 40DA2C67.

2. После выбора требуемого модуля/драйвера в правой части области № 2 страницы выводится также следующая дополнительная информация:

– результат последней проверки;
– название модуля/драйвера, прошедшего процедуру КЦ;
– КС модуля/драйвера;
– название производителя;
– номер версии модуля/драйвера и дата создания.

3. Для выбора первого модуля безопасности на странице *Контроль модулей безопасности* нажмите клавишу [Page Up], а для выбора последнего драйвера – клавишу [Page Down];

4. Администратор должен периодически, не реже одного раза в два месяца, проводить сверку отображаемых КС модулей ПК «ЭЗ «ВИТЯЗЬ» 2.2 с КС, приведенными в документе 643.18184162.00006-02 30 «Формуляр», раздел 4. Технические характеристики».

2.4. Управление сертификатами

Модуль реализует работу с сертификатами семейства X.509 и сертификатами с хранением закрытого ключа на смарт-карте. Вся работа с сертификатами выполняется средствами смарт-карты. Модуль использует возможности, предоставляемые используемыми смарт-картами.

2.4.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Управление сертификатами* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление сертификатами: Настройки* (рис. 64);

Страница *Управление сертификатами: Настройки* (вид 1),

пункт для включения модуля

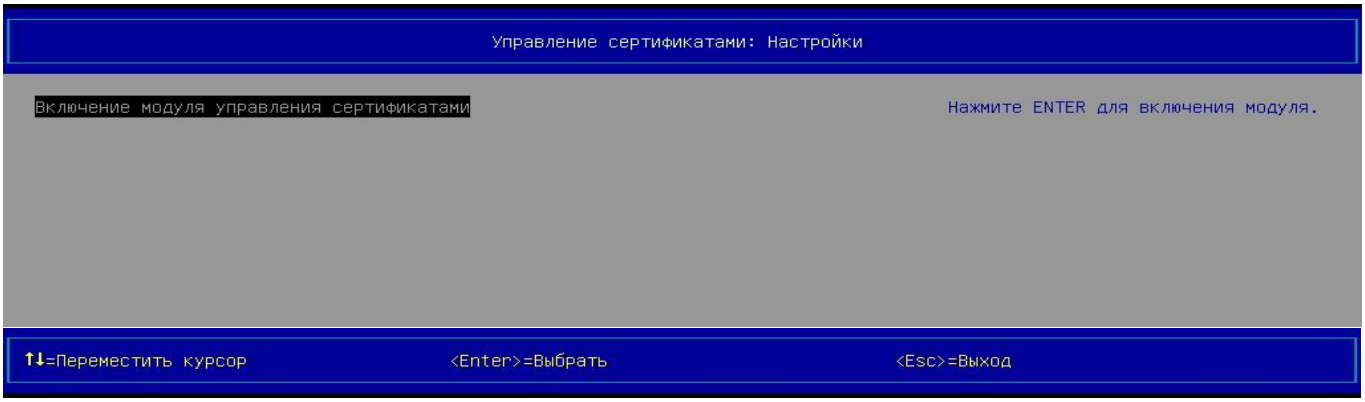

Рис. 64

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 65) для подтверждения включение модуля;

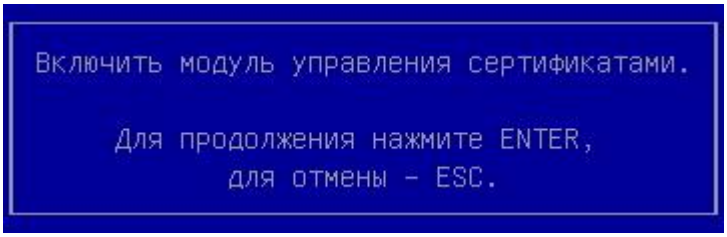

Рис. 65

6) нажать клавишу [Enter], выполняется включение модуля *Управление сертификатами*, отображается страница *Настройки*, отображение статуса модуля изменяется с «Выкл» на «Вкл».

2.4.2. Выключение модуля

Для выключения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Управление сертификатами* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление сертификатами: Настройки* (рис. 66) с пунктом выключения модуля;

Страница *Управление сертификатами: Настройки* (вид 2),

пункт выключения модуля

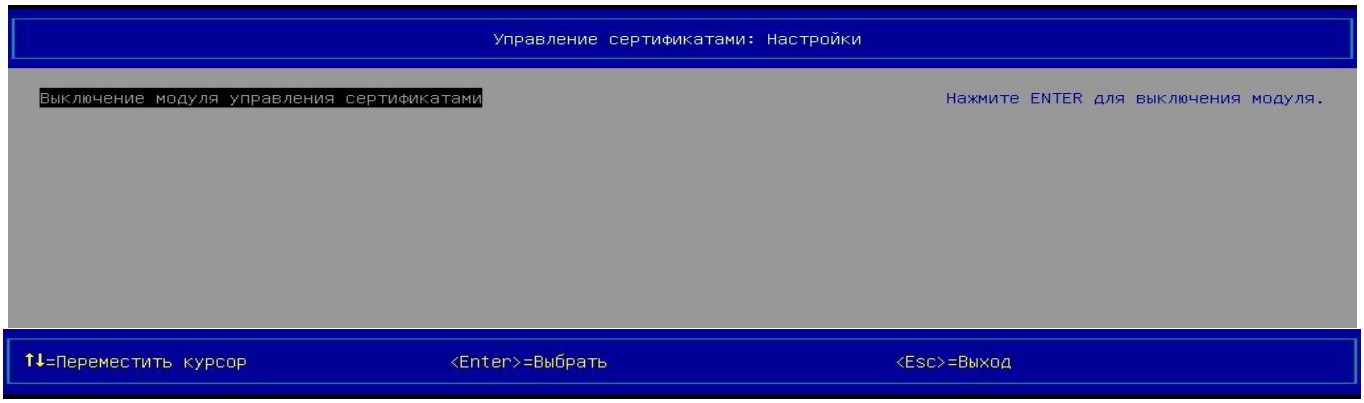

Рис. 66

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 67) для подтверждения выключения модуля;

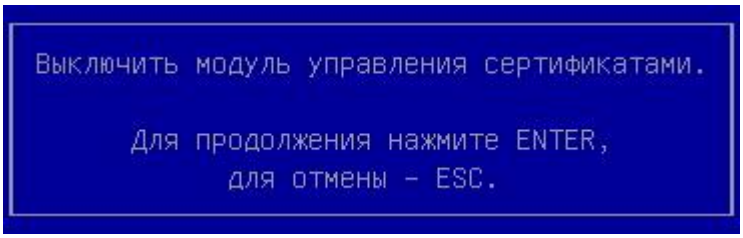

Рис. 67

6) нажать клавишу [Enter], выполняется выключение модуля *Управление сертификатами*, отображается страница *Настройки*, отображение статуса модуля изменяется с «Вкл» на «Выкл».

2.4.3. Добавление сертификата удостоверяющего центра

ВНИМАНИЕ! АДМИНИСТРАТОР ДОЛЖЕН ДОБАВЛЯТЬ ТОЛЬКО ТЕ СЕРТИФИКАТЫ УЦ, С ПОМОЩЬЮ КОТОРЫХ БЫЛИ ПОДПИСАНЫ СЕРТИФИКАТЫ ПОЛЬЗОВАТЕЛЕЙ, ХРАНЯЩИЕСЯ НА АН. НЕСОБЛЮДЕНИЕ ДАННОГО ТРЕБОВАНИЯ ПРИВЕДЕТ К НЕВОЗМОЖНОСТИ АУТЕНТИФИКАЦИИ В ПК «ЭЗ «ВИТЯЗЬ» 2.2!

Для добавления сертификата УЦ в ПК «ЭЗ «ВИТЯЗЬ» 2.2 следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами* (рис. 68, 71);

Страница *Управление сертификатами* (вид 1),

сертификаты УЦ отсутствуют

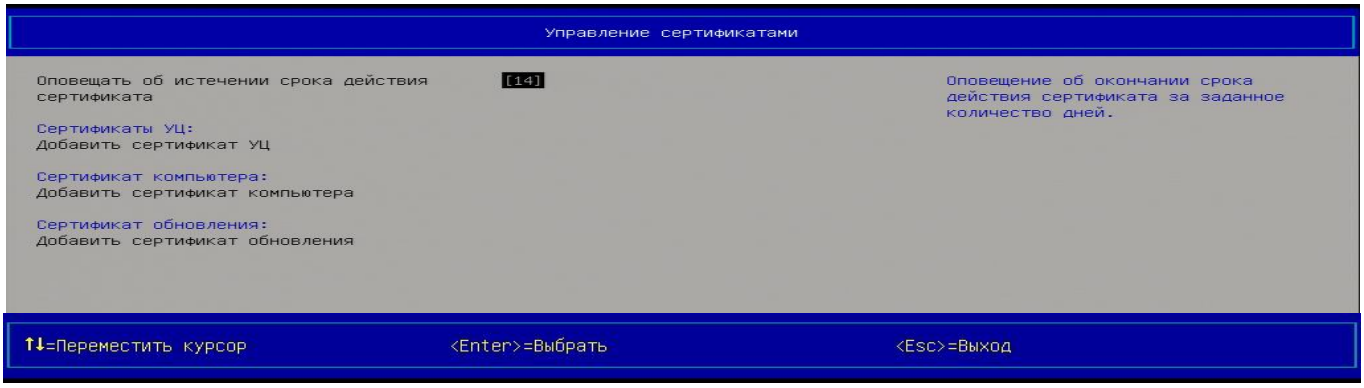

Рис. 68

3) подключить USB-диск в порт, если необходимый сертификат УЦ расположен на нем (при добавлении сертификата УЦ с разделов жестких дисков данный пункт следует пропустить);

4) выбрать п. *Добавить сертификат УЦ* (см. рис. 68, 71, 75, 76);

5) нажать клавишу [Enter], отображается страница *Файловый менеджер* (рис. 69);

Страница *Файловый менеджер*

Рис. 69

6) выбрать локальный диск, на котором расположен сертификат УЦ;

7) нажать клавишу [Enter];

8) открыть папку или подпапку, в которой расположен сертификат УЦ, при необходимости;

9) выделить необходимый файл, который является сертификатом УЦ;

10) нажать клавишу [Пробел], отображается окно (рис. 70), информирующее о добавлении сертификата УЦ в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

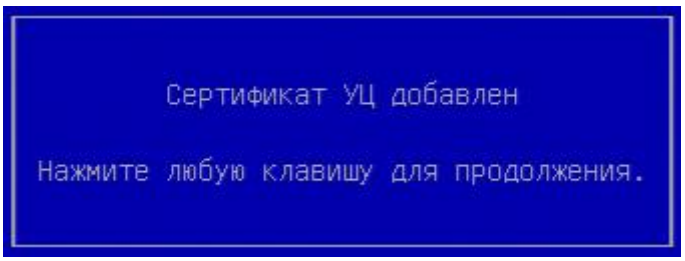

Рис. 70

11) нажать клавишу [Enter].

Примечания:

1. Добавление сертификата УЦ в ПК «ЭЗ «ВИТЯЗЬ» 2.2 возможно только после включения модуля *Управление сертификатами*.

2. Действия на странице *Файловый менеджер* (см. рис. 69): перемещение по объектам (локальные диски, папки, подпапки, файлы) страницы выполняется клавишами [↑], [↓], а открытие папки, подпапки, переход в родительский каталог, выбор элемента – клавишей [Пробел].

2.4.4. Просмотр информации о сертификате удостоверяющего центра

Для просмотра информации о сертификате УЦ следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами* (рис. 71);

Страница *Управление сертификатами* (вид 2),

сертификат УЦ добавлен

Рис. 71

3) выбрать сертификат УЦ, информацию о котором требуется просмотреть; в правой части области № 2 страницы выводится информация о выбранном сертификате УЦ, а именно: серийный номер сертификата, кем выдан, кому выдан, даты и время начала срока действия сертификата, даты и время окончания срока действия сертификата;

4) просмотреть и проанализировать данную информацию.

Примечания:

1. Просмотр информации о сертификате УЦ возможен только после включения модуля *Управление сертификатами* и добавления хотя бы одного сертификата УЦ.

2. Для просмотра справочной информации о разрешенном минимальном и максимальном количестве дней для п. *Оповещать об истечении срока действия сертификата*:

1) перейти в меню *Управление сертификатами*;

2) проверить информацию в пункте *Оповещать об истечении срока действия сертификата*;

3) проверить границы значений.

Первоначальное количество дней задано по умолчанию, диапазон возможных значений от 4 до 255.

2.4.5. Удаление всех сертификатов удостоверяющего центра из ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для удаления всех сертификатов УЦ из ПК «ЭЗ «ВИТЯЗЬ» 2.2 следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами* (см. рис. 71);

3) выбрать п. *Удалить все сертификаты УЦ* раздела *Сертификаты УЦ*;

4) нажать клавишу [Enter], отображается окно (рис. 72), запрашивающее подтверждение на удаление всех сертификатов УЦ, ранее добавленных в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

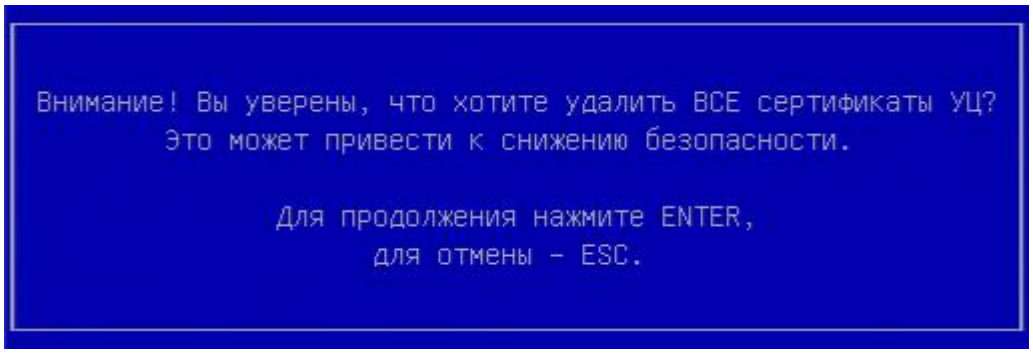

Рис. 72

5) нажать клавишу [Enter], все сертификаты УЦ, ранее добавленные в ПК «ЭЗ «ВИТЯЗЬ» 2.2, удаляются из ПК «ЭЗ «ВИТЯЗЬ» 2.2, и отображается окно (рис. 73), информирующее об удалении всех сертификатов УЦ;

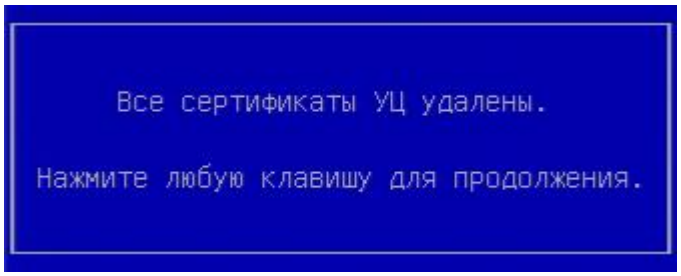

Рис. 73

6) нажать клавишу [Enter].

Примечание. Удаление всех сертификатов УЦ из ПК «ЭЗ «ВИТЯЗЬ» 2.2 возможно только после включения модуля *Управление сертификатами* и добавления хотя бы одного сертификата УЦ в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2.4.6. Добавление сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для добавления сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2 следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами* (см. рис. 68, 71);

3) подключить USB-диск в порт, если необходимый сертификат компьютера расположен на нем (при добавлении сертификата компьютера с разделов жестких дисков данный пункт следует пропустить);

4) выбрать п. *Добавить сертификат компьютера* раздела *Сертификат компьютера* (см. рис. 68, 71);

5) нажать клавишу [Enter], отображается страница *Файловый менеджер* (см. рис. 69);

6) выбрать локальный диск, на котором расположен сертификат компьютера;

7) нажать клавишу [Enter];

8) открыть папку или подпапку, в которой расположен сертификат компьютера, при необходимости;

9) выделить необходимый файл, который является сертификатом компьютера;

10) нажать клавишу [Пробел], отображается окно (см. рис. 20), предлагающее ввести пароль для выделенного файла сертификата;

11) ввести пароль для выделенного файла сертификата;

12) нажать клавишу [Enter], отображается окно (рис. 74), информирующее о добавлении сертификата в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

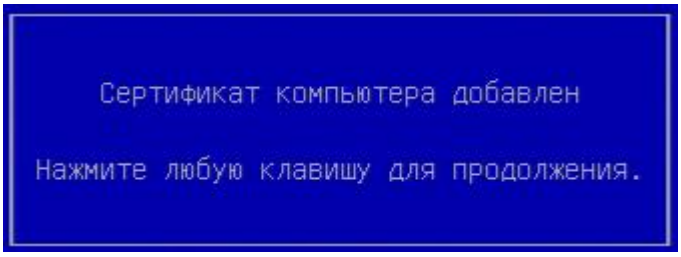

Рис. 74

13) нажать клавишу [Enter].

Примечания:

1. Добавление сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2 возможно только после включения модуля *Управление сертификатами*.

2. Действия на странице *Файловый менеджер* (см. рис. 69): перемещение по объектам (локальные диски, папки, подпапки, файлы) страницы выполняется клавишами [↑], [↓], а открытие папки, подпапки, переход в родительский каталог, выбор выделенного элемента – клавишей [Пробел].

3. В ПК «ЭЗ «ВИТЯЗЬ» 2.2 можно добавить только один сертификат компьютера.

2.4.7. Просмотр информации о сертификате компьютера

Для просмотра сертификата компьютера следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами* (рис. 75);

Страница *Управление сертификатами* (вид 3),

сертификат компьютера добавлен

Рис. 75

3) выбрать сертификат компьютера, информацию о котором требуется просмотреть; в правой части области № 2 страницы выводится информация о выбранном сертификате, а именно:

– серийный номер сертификата, кем выдан, кому выдан;

– дата и время начала срока действия сертификата;

– дата и время окончания срока действия сертификата (рис. 76);

Страница *Управление сертификатами*,

информация о сертификате компьютера выведена

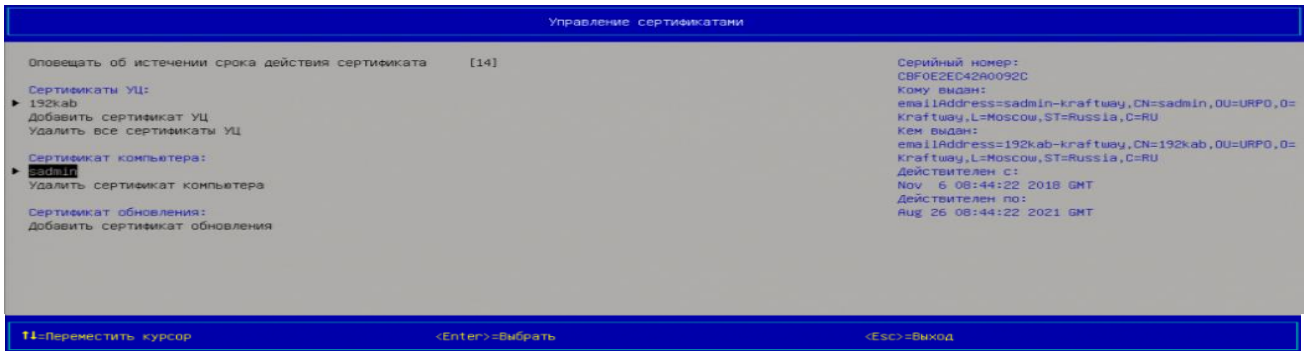

Рис. 76

4) просмотреть и проанализировать данную информацию.

Примечание. Просмотр информации о сертификате компьютера возможен только после включения модуля *Управление сертификатами* и добавления сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2.4.8. Удаление сертификата компьютера из ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для удаления сертификата из ПК «ЭЗ «ВИТЯЗЬ» 2.2 следует:

1) выбрать п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Управление сертификатами*;

3) выбрать п. *Удалить сертификат компьютера* раздела *Сертификат компьютера* (см. рис. 75, 76);

4) нажать клавишу [Enter], отображается окно (рис. 77), запрашивающее подтверждение на удаление сертификата, ранее добавленного в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

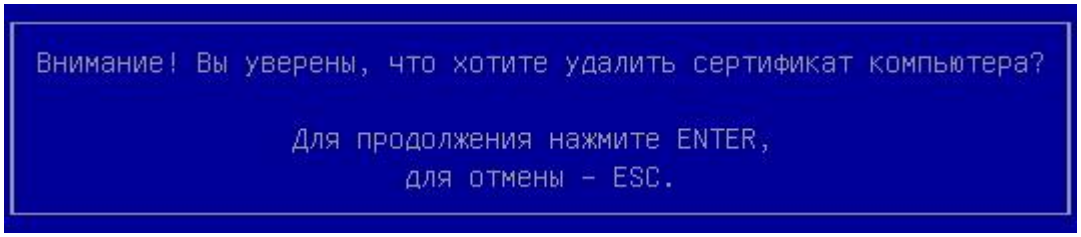

Рис. 77

5) нажать клавишу [Enter], сертификат компьютера, ранее добавленный в ПК «ЭЗ «ВИТЯЗЬ» 2.2, удаляется из ПК «ЭЗ «ВИТЯЗЬ» 2.2, и отображается окно (рис. 78), информирующее об удалении сертификата;

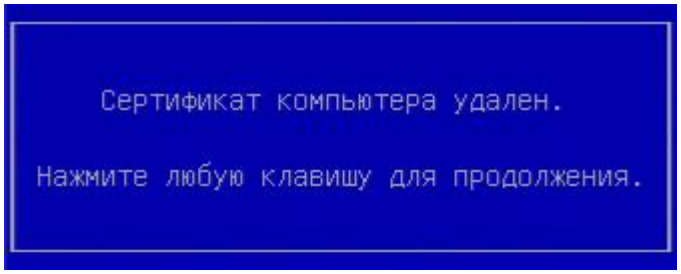

Рис. 78

6) нажать клавишу [Enter].

Примечание. Удаление сертификата компьютера из ПК «ЭЗ «ВИТЯЗЬ» 2.2 возможно только после включения модуля *Управление сертификатами* и добавления сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2.5. Контроль целостности файловой системы

2.5.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности файловой системы* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы: Настройки* с пунктом включения модуля (рис. 79);

Страница *Контроль целостности файловой системы: Настройки* (вид 1),

пункт для включения модуля КЦ ФС

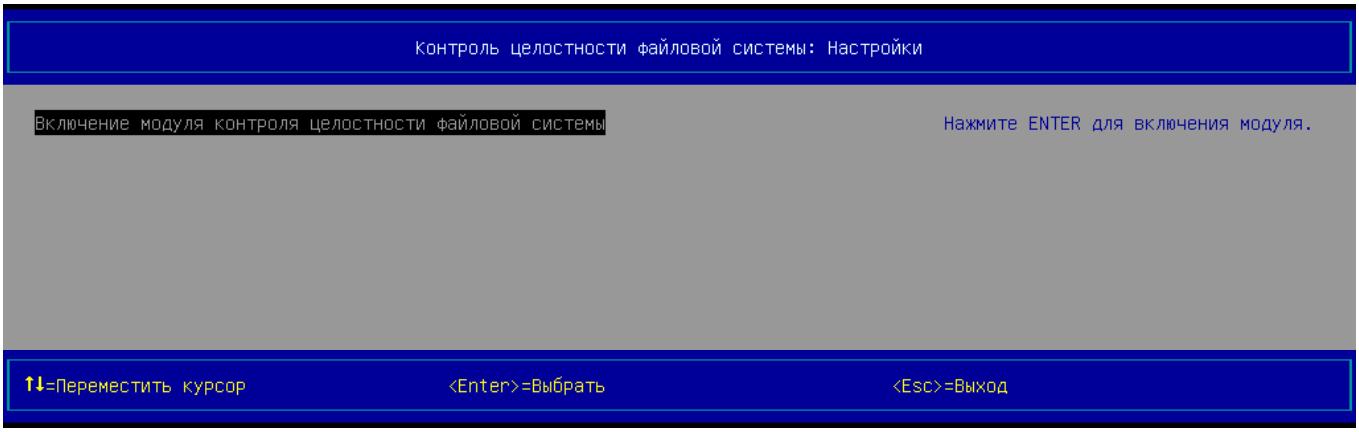

Рис. 79

5) нажать клавишу [Enter], отображается окно (рис. 80) для подтверждения включения модуля;

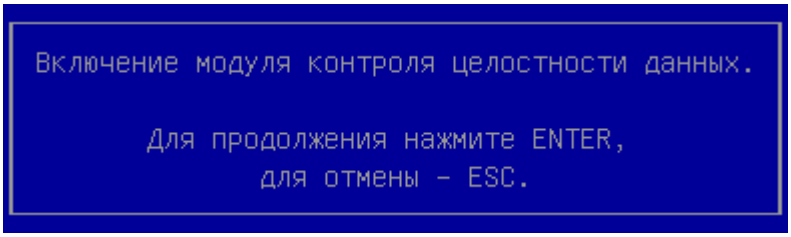

Рис. 80

6) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы: Настройки*, с возможностью выбора хеш-функции (рис. 81);

Страница *Контроль целостности файловой системы: Настройки*,

пункт выбора хеш-функции

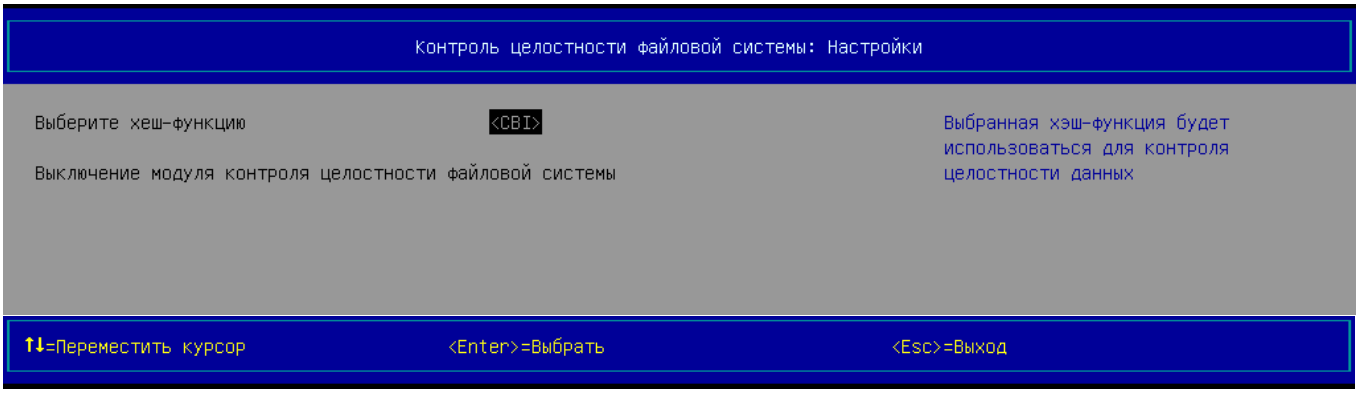

Рис. 81

7) выбрать п. *Выберите хеш-функцию*;

8) нажать клавишу [Enter], отображается окно (рис. 82) для выбора хеш-функции из списка;

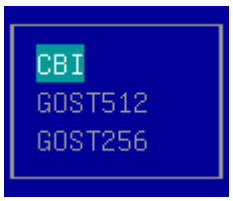

Рис. 82

9) выбрать требуемую хэш-функцию клавишами [↑], [↓] для процедуры КЦ данных;

10) нажать клавишу [Enter];

11) если хеш-функция изменилась, то будет диалоговое окно на подтверждение изменений;

12) нажать клавишу [Esc], отображается страница *Настройки* (см. рис. 37), отображение статуса модуля *Контроль целостности файловой системы* изменяется с «Выкл» на «Вкл».

Примечания:
1. Выбор хеш-функции осуществляется исходя из политики безопасности в организации.
2. По умолчанию выбрана хеш-функция «CBI».

2.5.2. Выбор хеш-функции

Для выбора значения хеш-функции, отличающегося от значения по умолчанию, следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности файловой системы* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы: Настройки* (см. рис. 81) с пунктом для выбора хеш-функции;

5) выбрать п. *Выберите хеш-функцию*;

6) нажать клавишу [Enter], отображается окно (см. рис. 82) для выбора хеш-функции из списка;

7) выбрать требуемую хэш-функцию клавишами [↑], [↓]. Выбранная хеш-функция будет использоваться для КЦ данных;

8) нажать клавишу [Enter];

9) нажать клавишу [Esc], отображается страница *Настройки* (рис. 37).

2.5.3. Выключение модуля

Для выключения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности файловой системы* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы: Настройки* (рис. 83) с пунктом для выключения модуля и удаления всех списков КЦ;

Страница *Контроль целостности файловой системы: Настройки*,

пункт для выключения модуля

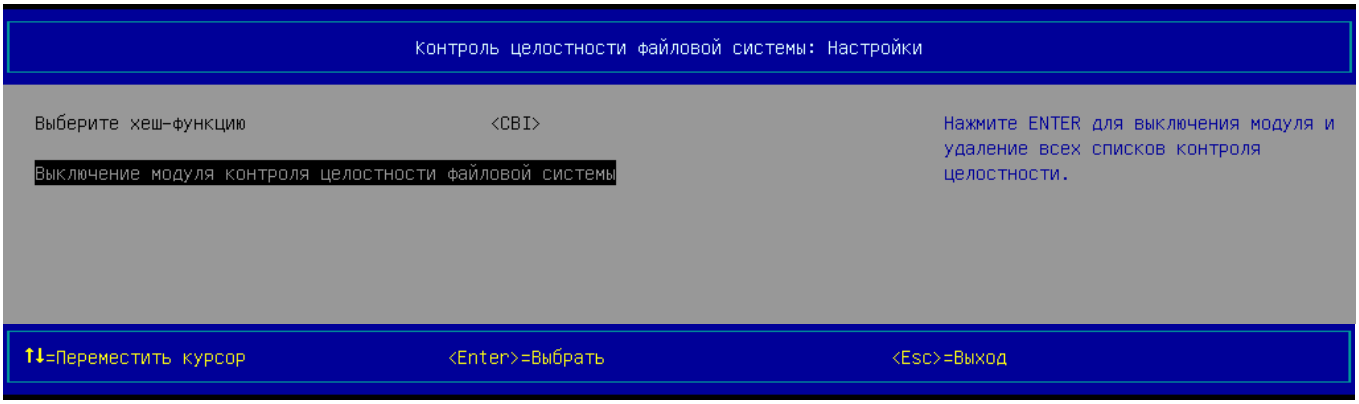

Рис. 83

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 84), запрашивающее подтверждение на выключение модуля и удаления всех списков КЦ;

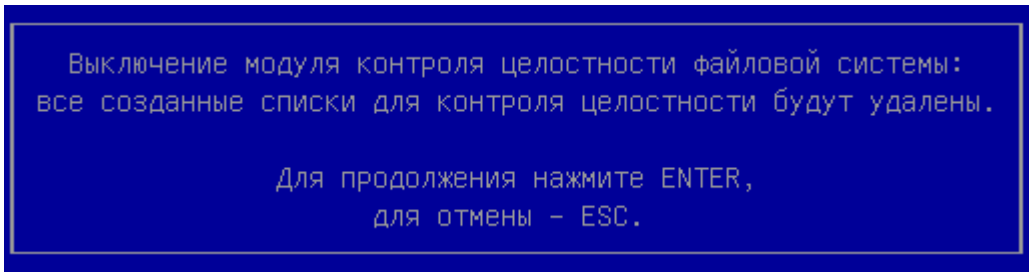

Рис. 84

6) нажать клавишу [Enter], выполняется выключение модуля *Контроль целостности файловой системы* и удаление всех списков КЦ, отображается страница *Настройки*, отображение статуса модуля меняется с «Вкл» на «Выкл».

2.5.4. Создание списка файлов, подлежащих КЦ

Для создания списка файлов, подлежащих КЦ, следует:

1) выбрать п. *Контроль целостности файловой системы* в главном меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы* (рис. 85);

Страница *Контроль целостности файловой системы* (вид 1),

ни одного списка файлов, подлежащих КЦ, не было создано

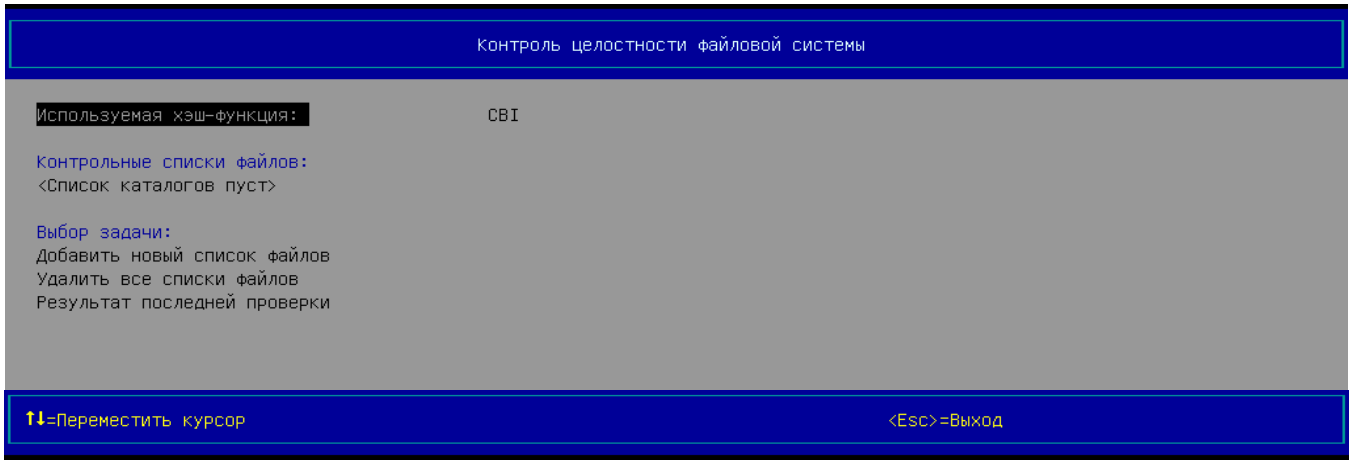

Рис. 85

3) выбрать п. *Добавить новый список файлов* раздела *Выбор задачи*;

4) нажать клавишу [Enter], отображается страница *Создание списка файлов* (рис. 86);

Страница *Создание списка файлов*

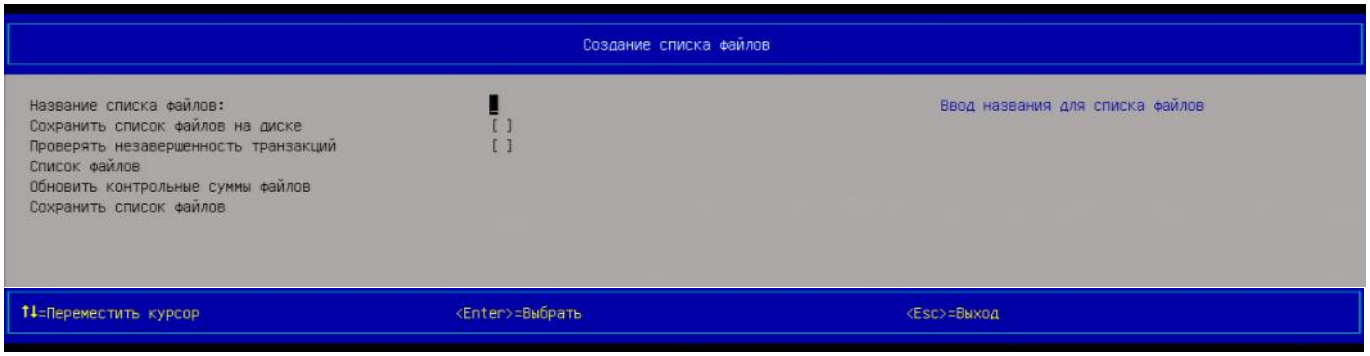

Рис. 86

5) выбрать п. *Название списка файлов*;

6) нажать клавишу [Enter], отображается окно для ввода названия списка файлов (рис. 87);

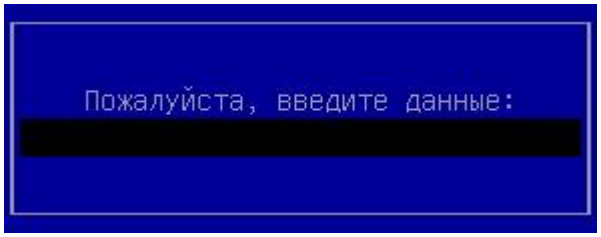

Рис. 87

7) ввести название списка файлов и нажать клавишу [Enter];

8) выбрать п. С*писок файлов* (см. рис. 86);

9) нажать клавишу [Enter], отображается окно файлового менеджера (рис. 88), в котором предлагается выбрать объекты (файлы, папки), подлежащие КЦ;

Окно файлового менеджера

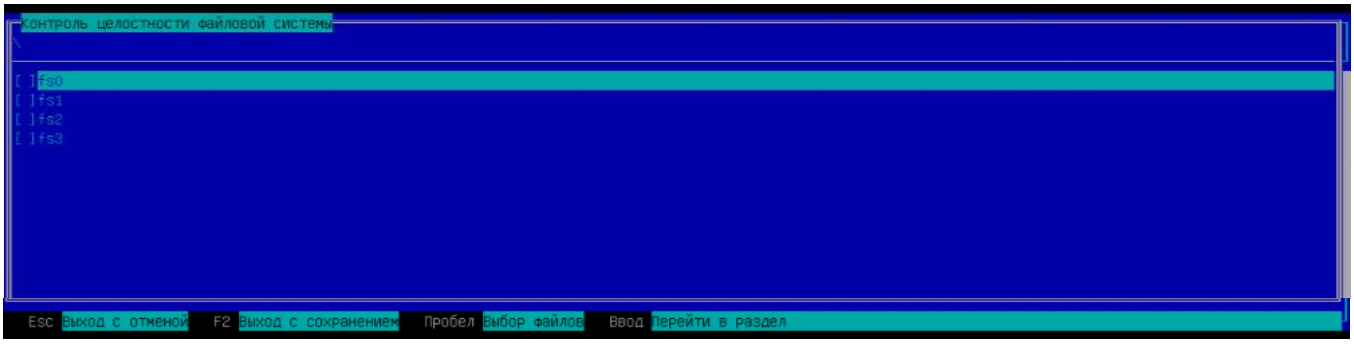

Рис. 88

10) выбрать требуемые локальные диски клавишами [↑], [↓];

11) при необходимости выполнять КЦ целых дисков, выделить диски, подлежащие КЦ, клавишей [Пробел];

12) при необходимости выбрать другие объекты (файлы, папки), подлежащие КЦ, расположенные на определенном локальном диске, нажать клавишу [Enter] на данном диске для входа в ФС диска;

13) выделить объекты (файлы, папки), подлежащие КЦ, клавишей [Пробел];

14) для возврата на уровень выше (выход из папки, выход из диска) следует использовать клавишу [Esc];

15) при необходимости, удалить объект или объекты, которые не подлежат КЦ из панели *Список файлов*;

16) нажать клавишу [F2] для сохранения сделанных изменений и выхода из файлового менеджера;

17) отображается окно (рис. 89), информирующее об успешном обновлении (создании) КС файлов;

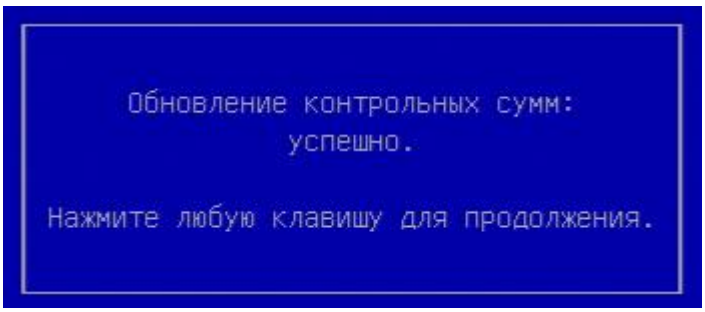

Рис. 89

18) нажать клавишу [Enter];

19) выбрать п. *Сохранить список файлов* (см. рис. 86);

20) нажать клавишу [Enter], отображается окно (рис. 90), информирующее о выполнении сохранения списка файлов;

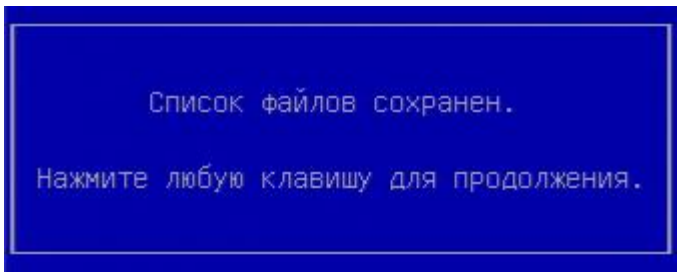

Рис. 90

21) нажать клавишу [Enter], отображается окно *Контроль целостности файловой системы*, с именем созданного списка в разделе *Контрольные списки файлов* (рис. 91). Справа вверху высветится информация о списке – даты и времена создания, изменения и последней проверки, а также общее число элементов, путь хранения списка (если при создании списка выбрано место хранения).

Примечания:

1. Создание списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5).

2. Выбор требуемых объектов выполняется клавишами [↑], [↓] (рис. 88).

3. Выделение объектов выполняется следующим образом:

1) выбрать объект, который подлежит КЦ;

2) нажать клавишу [Пробел].

4. Чтобы выйти из окна файлового менеджера без сохранения сделанных изменений следует воспользоваться клавишей [Esc].

2.5.5. Сохранение списка файлов, по которым проводится КЦ ФС

Для сохранения на диске списка файлов, по которому проводится КЦ ФС (путь на диске и КЦ), нужно:

1) на странице *Создание списка файлов* (см. рис. 86) клавишами [↑], [↓] выбрать п. *Сохранить список файлов на диске*;

2) нажать клавишу [Пробел], откроется файловый менеджер (см. рис. 88), в котором нужно клавишами [↑], [↓] выбрать диск для записи списка и нажать клавишу [Enter];

3) передвигаясь по ФС выбранного диска с помощью клавиш [↑], [↓], [Enter], [Esc], выбрать папку для записи и нажать клавишу [Пробел], список будет записан в выбранную папку.

Примечания:

1. Создание списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5).

2. Запись возможна только на устройства с ФС: FAT32, NTFS, ext/ext2/ext3/ext4.

2.5.6. Проверка завершенности транзакций журналируемых файловых систем

При контроле журналируемых ФС (NTFS, ext3/ext4) имеется возможность проверять факт наличия в них незавершенных транзакций, возникающих при обрыве записи на диск (например, из-за внезапного пропадания электропитания), для чего:

1) на странице *Создание списка файлов* (рис. 86) клавишами [↑], [↓] выбрать п. *Проверять незавершенность транзакций*;

2) нажать клавишу [Пробел].

Если имеются незавершенные транзакции, то целостность ФС нужно восстанавливать из журнала журналируемой ФС. Драйвер в UEFI корректно сделать это не может, а ФС в UEFI монтируется как READ-ONLY. Восстановление целостности ФС можно осуществить после загрузки ОС с помощью штатных утилит используемой ОС.

Примечания:

1. Проверка завершенности транзакций возможна только после включения модуля *Контроль целостности файловой системы* (подраздел 2.5) и создания хотя бы одного списка файлов, подлежащих КЦ.
2. Контролируются ФС (из числа поддерживаемых) только тех дисков, файлы которых входят хотя бы в один список КЦ ФС.
3. Если задана проверка завершенности транзакций и обнаружены незавершенные транзакции, загрузка ОС блокируется и вход возможен только администратору.
4. Информация о работе модуля *Контроль целостности файловой системы* в части контроля завершенности транзакций записывается в журнал событий.

2.5.7. Просмотр списка файлов, подлежащих КЦ

Для просмотра списка файлов, подлежащих КЦ, следует:

1) выбрать п. *Контроль целостности файловой системы* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности файловой системы* (рис. 91);

Страница *Контроль целостности файловой системы*,

создан список файлов для КЦ

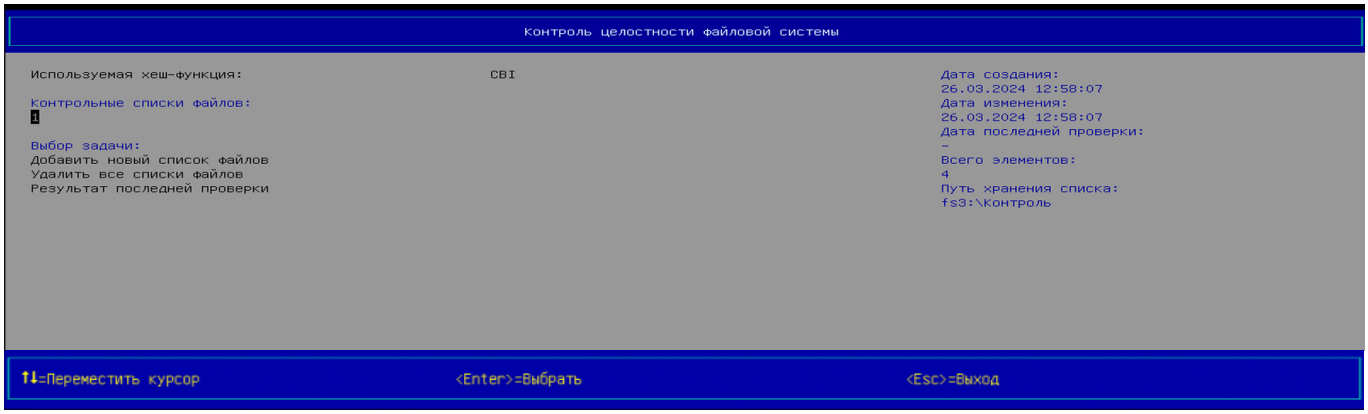

Рис. 91

3) выбрать требуемый список файлов, подлежащих КЦ, клавишами [↑], [↓];

4) нажать клавишу [Enter], отображается окно (рис. 92) для выбора действия, которое необходимо выполнить над выбранным списком;

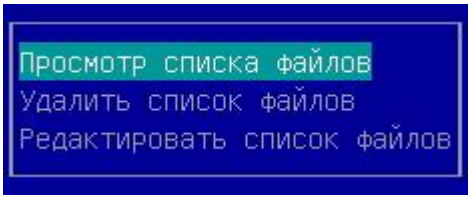

Рис. 92

5) выбрать п. *Просмотр списка файлов* в окне выбора;

6) нажать клавишу [Enter], отображается страница *Просмотр списка файлов* (рис. 93).

Страница *Просмотр списка файлов*

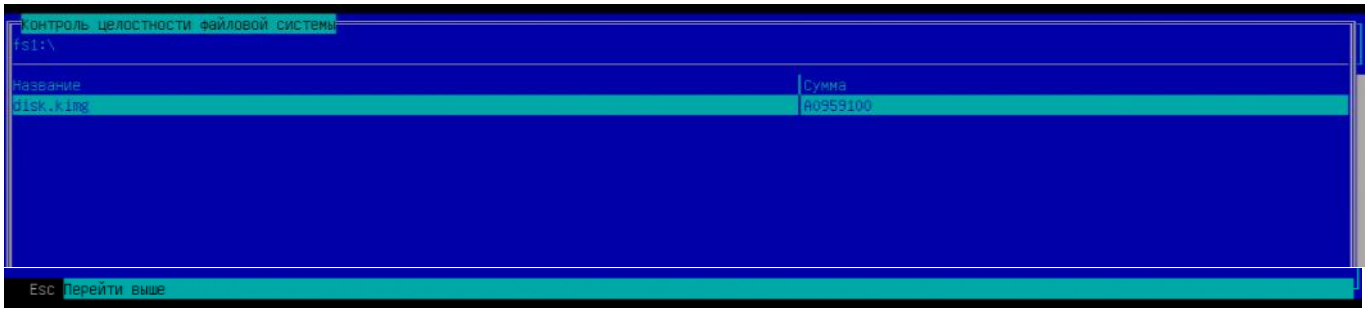

Рис. 93

Примечания:

1. Просмотр списка файлов, подлежащих КЦ, возможен только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5) и создания хотя бы одного списка файлов, подлежащих КЦ.

2. Перемещение по записям списка файлов выполняется клавишами [↑], [↓], а постраничный вывод записей списка – клавишами [Page Up], [Page Down].

3. После выбора какой-либо записи списка файлов, в правой части выводится КС объекта, указанного в выбранной записи.

2.5.8. Редактирование списка файлов, подлежащих КЦ

Для редактирования списка файлов, подлежащих КЦ, следует:

1) выполнить действия перечислений 1) – 4) п. 2.5.7,

2) выбрать п. *Редактировать список файлов* в окне (см. рис. 92);

3) нажать клавишу [Enter], отображается страница *Редактировать список файлов* (рис. 94);

Страница *Редактировать список файлов*

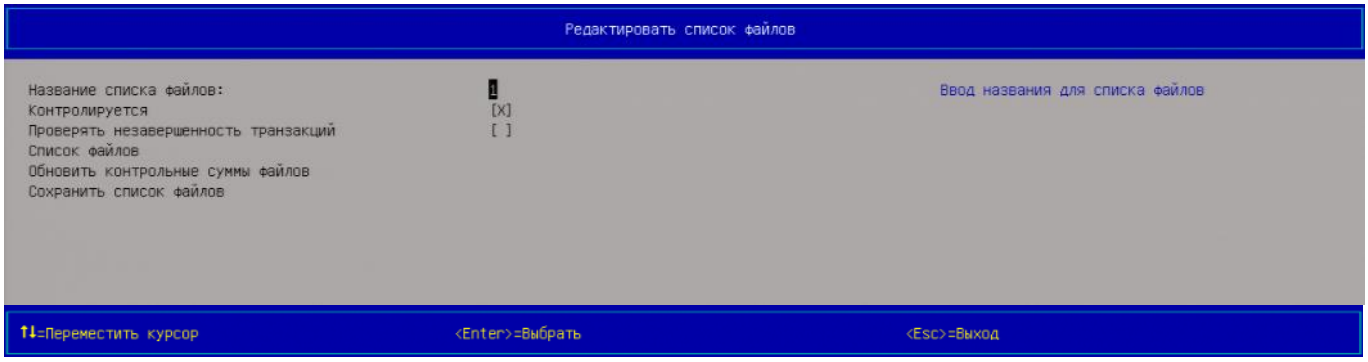

Рис. 94

4) изменить название списка файлов при необходимости (см. действия перечислений 6) – 9) п. 2.5.4);

5) изменить состав списка файлов при необходимости (см. действия перечислений 10) – 21) п. 2.5.4);

6) если состав списка файлов был изменен, то обновление КС происходит само;

7) сохранить список файлов, если состав списка файлов был изменен.

Примечание. Редактирование списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5) и создания хотя бы одного списка файлов, подлежащих КЦ.

2.5.9. Удаление списка файлов, подлежащих КЦ

Для удаления списка файлов, подлежащих КЦ, следует:

1) выполнить действия перечислений 1) – 4) п. 2.5.4,

2) выбрать п. *Удалить список файлов* в окне (рис. 92);

3) нажать клавишу [Enter], отображается окно (рис. 95) для подтверждения удаления выбранного списка файлов;

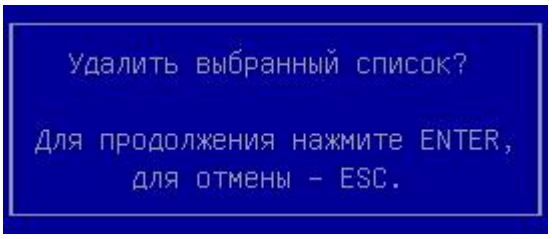

Рис. 95

4) нажать клавишу [Enter], происходит удаление выбранного списка файлов.

Примечание. Удаление списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5) и создания хотя бы одного списка файлов, подлежащих КЦ.

2.5.10. Вывод результата последней процедуры КЦ файлов

Для вывода результата последней процедуры КЦ файлов следует:

1) выполнить действия перечислений 1) – 2) п. 2.5.4;

2) выбрать п. *Результат последней проверки* (рис. 91);

3) нажать клавишу [Enter], отображается страница *Результат последней проверки* (рис. 96);

Страница *Результат последней проверки* (вид 1),

файлы с отрицательным результатом проверки отсутствуют

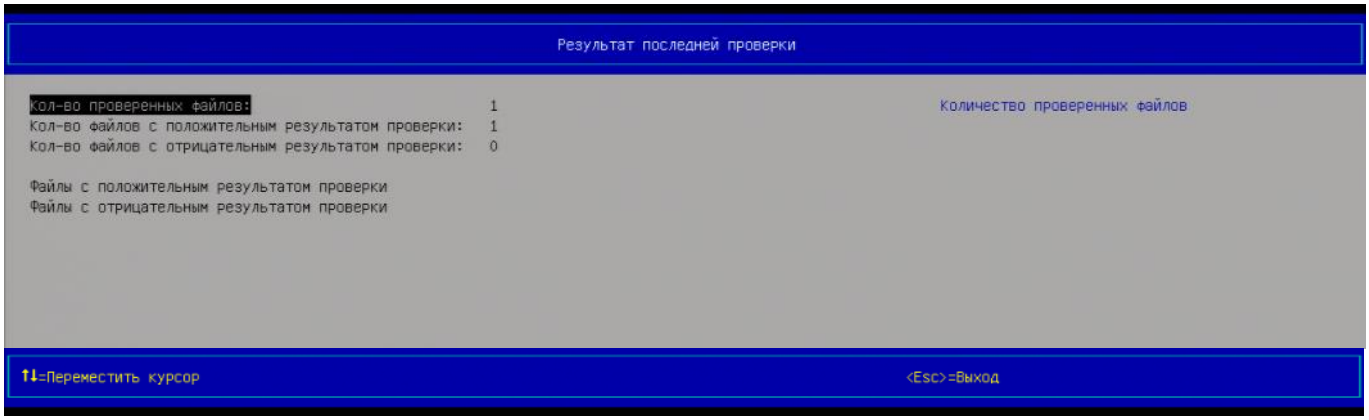

Рис. 96

4) выбрать раздел *Файлы с отрицательным результатом проверки* клавишами [↑], [↓] и нажать клавишу [Enter] для вывода дополнительной информации (имя устройства хранения, на котором размещается требуемый файл и его КС);

5) выбрать раздел *Файлы с положительным результатом проверки* клавишами [↑], [↓] и нажать клавишу [Enter] для вывода дополнительной информации (имя устройства хранения, на котором размещается требуемый файл и его КС).

Примечания:

1. Вывод результата последнего выполнения процедуры КЦ файлов возможен только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5), создания хотя бы одного списка файлов для КЦ и перезагрузки ОС.

2. Перемещение по записям выполняется клавишами [↑], [↓], а постраничный вывод записей – клавишами [Page Up], [Page Down].

2.5.11. Удаление всех списков файлов, подлежащих КЦ

Для удаления всех списков файлов, подлежащих КЦ, следует:

1) выполнить 1) – 2) п. 2.5.4;

2) выбрать п. *Удалить все списки файлов* (см. рис. 91);

3) нажать клавишу [Enter], отображается окно (рис. 97) для подтверждения удаления всех списков файлов;

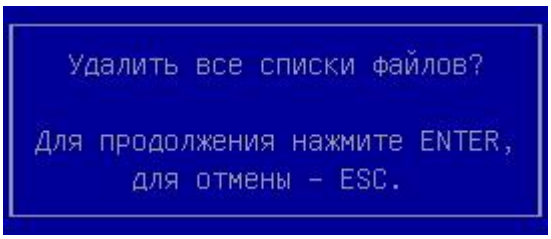

Рис. 97

4) нажать клавишу [Enter], происходит удаление всех ранее созданных списков файлов, подлежащих КЦ.

Примечание. Удаление всех списков файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. подраздел 2.5) и создания хотя бы одного списка файлов, подлежащих КЦ.

2.6. Контроль целостности оборудования

2.6.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности оборудования* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль целостности оборудования: Настройки* с пунктом включения модуля (рис. 98);

Страница *Контроль целостности оборудования: Настройки* (вид 1),

пункт для включения модуля

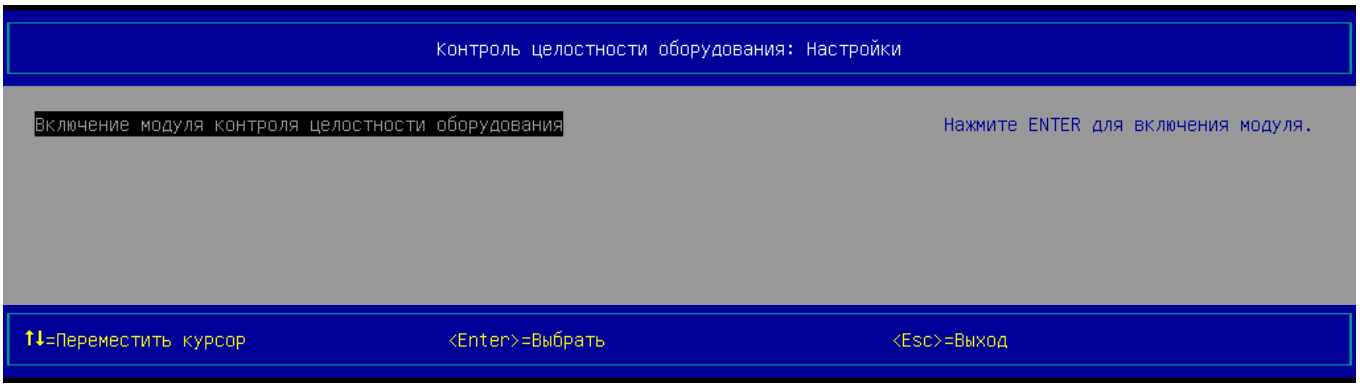

Рис. 98

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 99), запрашивающее подтверждение на включение модуля;

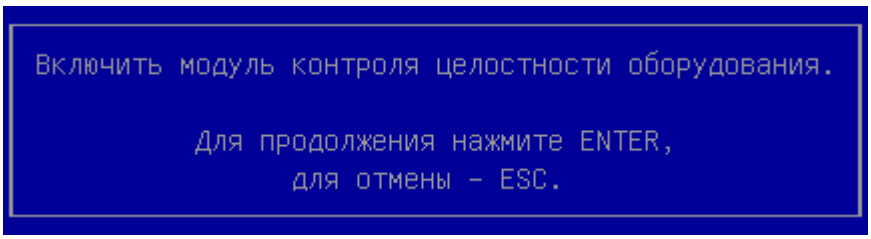

Рис. 99

6) нажать клавишу [Enter], выполняется включение модуля *Контроль целостности оборудования*, отображение статуса модуля меняется с «Выкл» на «Вкл».

2.6.2. Выбор объектов для КЦ оборудования

Для выбора объектов проверки следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности оборудования* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль целостности оборудования: Настройки* с пунктом выключения модуля (рис. 100);

Страница *Контроль целостности оборудования: Настройки*,

выбор объектов для КЦ оборудования

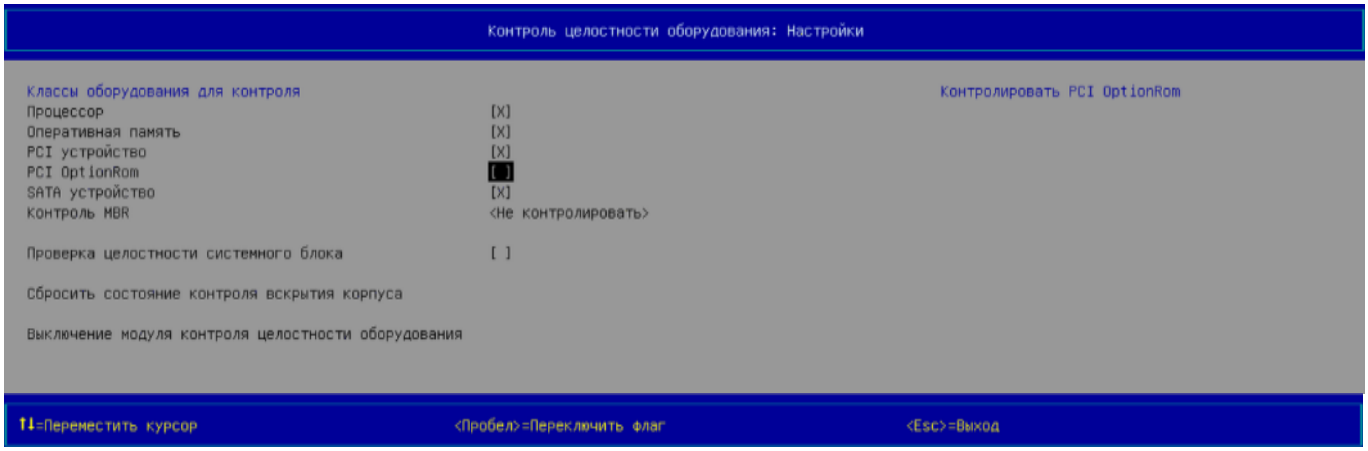

Рис. 100

5) выбрать требуемые объекты для контроля из следующего списка:

– *Процессор*;

– *Оперативная память*;

– *PCI устройство* (устройства на шине PCI);

– *PCI OptionRom* (ресурсы конфигурационного пространства PCI/PCIe);

– *SATA устройство* (устройства с интерфейсом SATA);

– *Контроль MBR* (главная загрузочная запись, см. п. 2.6.4);

– целостность системного блока (см. п. 2.6.3);

6) чтобы активировать или деактивировать функцию КЦ соответствующего объекта следует выбрать эту функцию и нажать клавишу [Пробел], будет установлен или снят флажок «X».

2.6.3. Проверка целостности системного блока

Администратору предоставляется право использования функции КЦ системного блока. Включение функции позволяет фиксировать вскрытие корпуса системного блока при наличии установленного датчика вскрытия. После включения функции и вскрытии корпуса системного блока, датчик срабатывает и пройти процедуру аутентификации сможет лишь пользователь с правами администратора.

Для активации функции КЦ системного блока следует:

1) выбрать п. *Контроль целостности оборудования* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности оборудования: Настройки* (рис. 101);

Страница *Контроль целостности оборудования: Настройки* (вид 3),

п. *Проверка целостности системного блока*

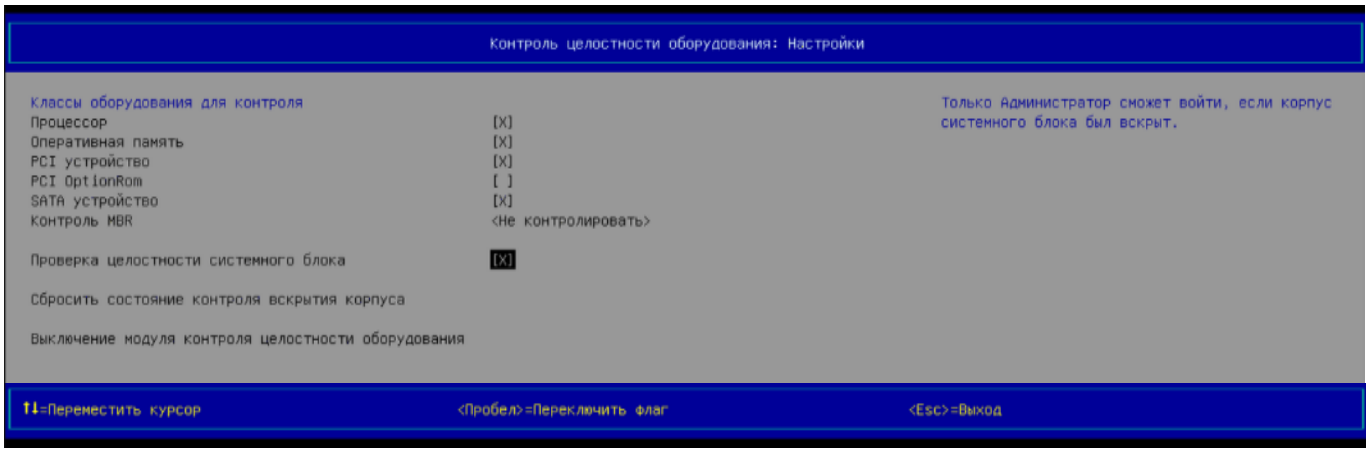

Рис. 101

3) выбрать п. *Проверка целостности системного блока*;

4) для включения функции КЦ системного блока нажать клавишу [Пробел], будет установлен флажок «X»;

5) для выключения функции КЦ системного блока повторно нажать клавишу [Пробел], флажок «X» будет снят;

6) если необходимо, можно сбросить сработавший флажок состоявшегося вскрытия системного блока с помощью п. *Сбросить состояние контроля вскрытия корпуса*, нажав клавишу [Enter] на этом пункте;

7) нажать клавишу [Esc] для выхода.

Примечания:

1. Активация функции КЦ системного блока возможна только после включения модуля *Контроль целостности оборудования* (см. п. 2.6.1).

2. Нарушение целостности системного блока аналогично нарушению целостности ФС и оборудования и приводит к блокировке загрузки ОС.

3. Информация о работе модуля *Контроль целостности оборудования* в части КЦ системного блока записывается в журнал событий. Сигнал поступает от датчика вскрытия корпуса системного блока при снятии защитного кожуха с возможностью доступа к компонентам компьютера.

4. Данная функция доступна только для материнских плат, поддерживающих подключение датчика вскрытия корпуса системного блока.

2.6.4. Контроль MBR

Администратору предоставляется возможность активации функции контроля MBR загрузочного диска. Эта функция реагирует на изменение содержимого MBR.

Для активации функции контроля MBR следует:

1) выбрать п. *Контроль целостности оборудования* в главном меню KSS (см. рис. 2);

2) выбрать строку *Контроль MBR*;

3) нажать клавишу [Enter], отображается меню доступных действий (рис. 102);

Страница *Контроль целостности оборудования: Настройки*,

п. *Контроль MBR*

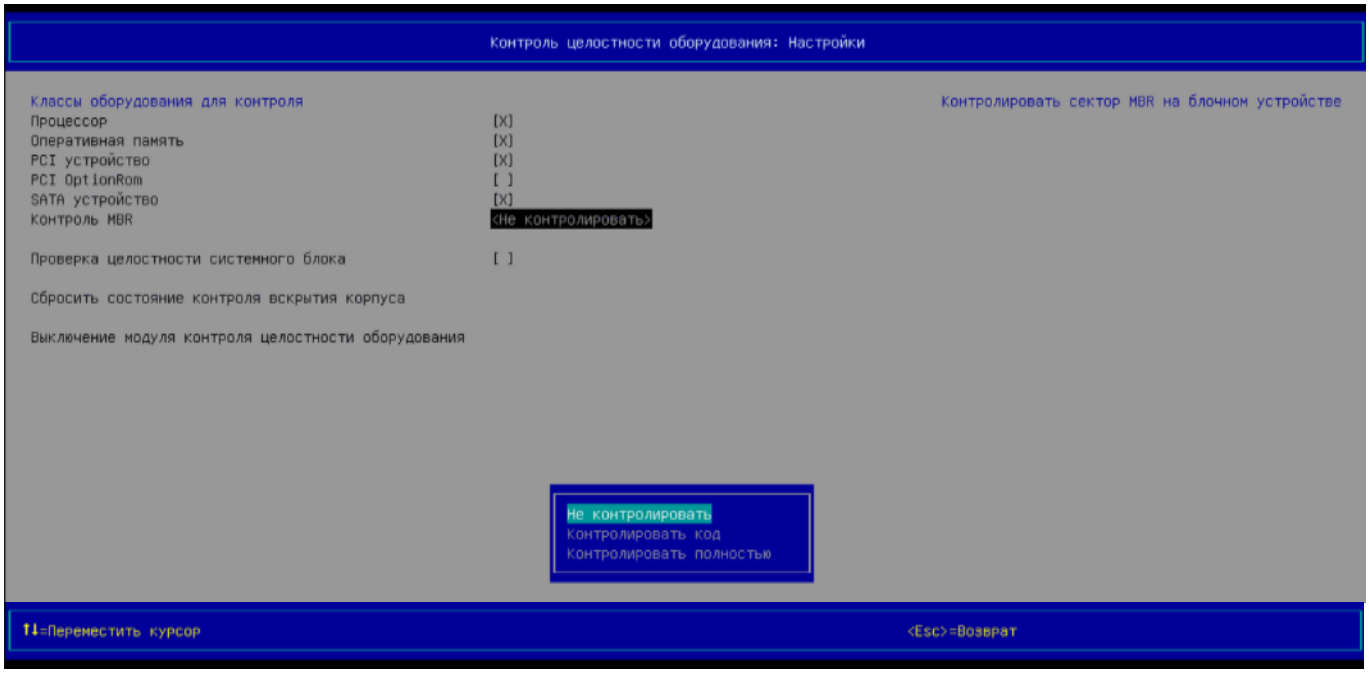

Рис. 102

4) выбрать действие клавишами [↑], [↓] и нажать клавишу [Enter]. Имеются следующие возможности:

– *Не контролировать* - любые изменения MBR игнорируются;

– *Контролировать код* - проверяется неизменность расположенного внутри MBR загрузочного исполняемого кода;

– *Контролировать полностью* - проверяется не только неизменность расположенного внутри MBR загрузочного исполняемого кода, но и целостность всей схемы форматирования разделов;

5) нажать клавишу [Esc] для выхода.

Примечания:

1. Активация функции контроля MBR возможна только после включения модуля *Контроль целостности оборудования* (см. п. 2.6.1).

2. Если задан контроль MBR (код или полностью) и обнаружено изменение отслеживаемой составляющей, загрузка ОС блокируется и вход возможен только администратору.

3. Информация о работе модуля *Контроль целостности оборудования* в части контроля MBR записывается в журнал событий.

2.6.5. Выключение модуля

Для выключения модуля следует:

1) выбрать п. *Настройки* в главном меню KSS (рис. 4);

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 37);

3) выбрать п. *Выключение модуля контроля целостности оборудования*;

4) нажать клавишу [Enter], отображается диалоговое окно (рис. 103) для подтверждения выключения модуля;

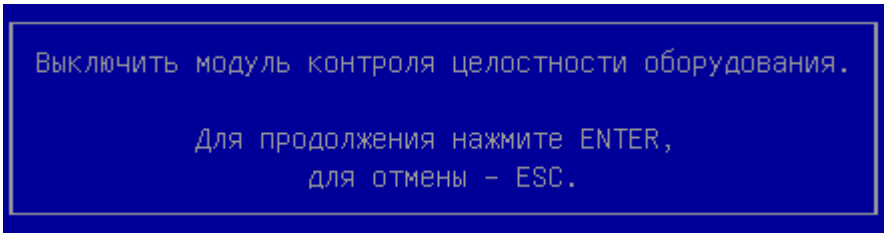

Рис. 103

5) нажать клавишу [Enter], выполняется выключение модуля *Контроль целостности оборудования*, отображение статуса модуля меняется с «Вкл» на «Выкл».

2.6.6. Вывод результата последнего выполнения КЦ оборудования

Для вывода результата последнего выполнения процедуры КЦ оборудования следует:

1) выбрать п. *Контроль целостности оборудования* раздела *Модули безопасности* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности оборудования* (рис. 104, 105);

Страница *Контроль целостности оборудования* (вид 1),

с положительным результатом проверки

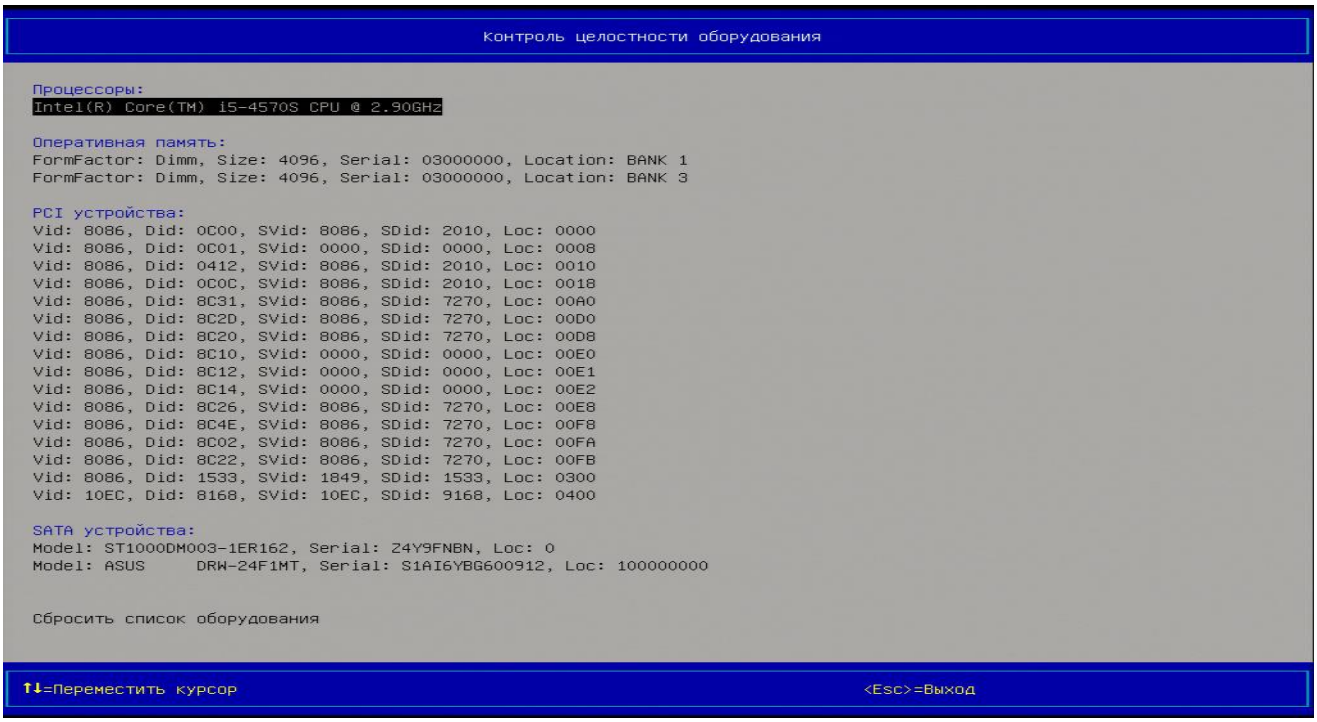

Рис. 104

Страница *Контроль целостности оборудования* (вид 2),

с отрицательным результатом проверки

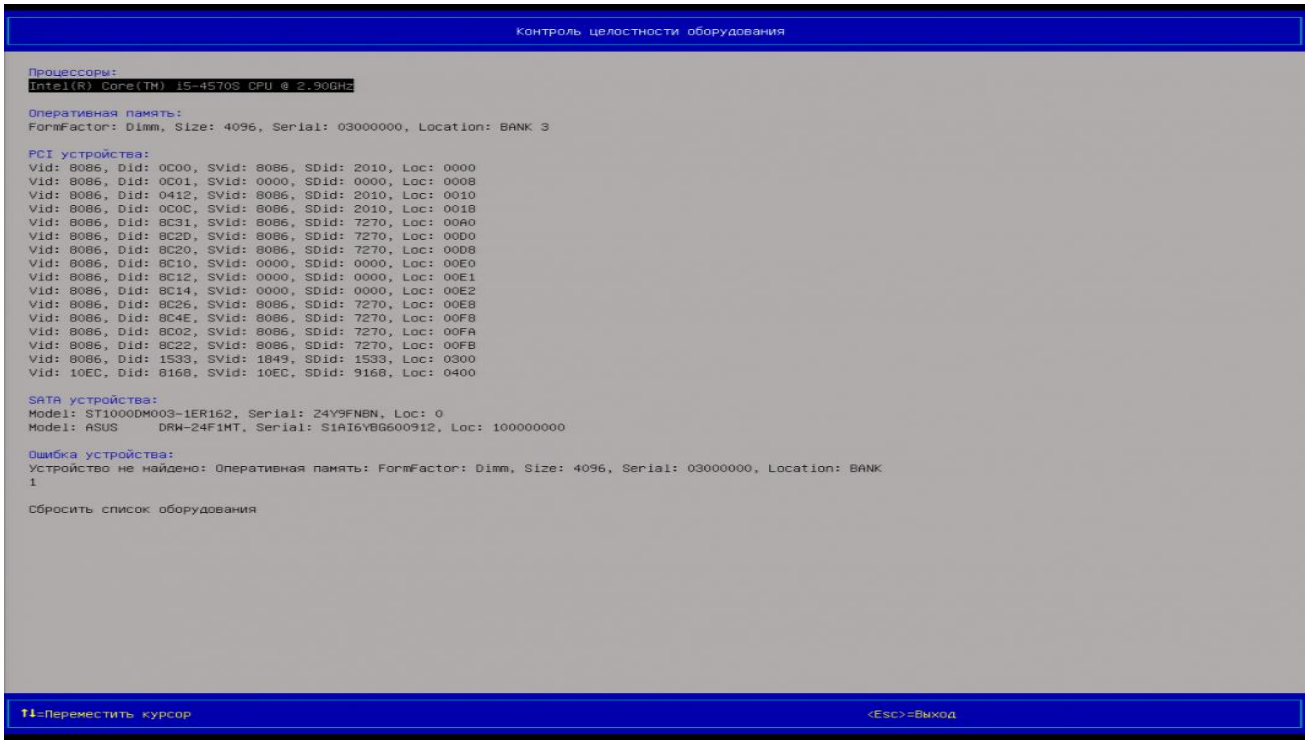

Рис. 105

3) нажать клавишу [Esc], для возврата в главное меню KSS.

Примечания:

1. Вывод результата последней процедуры КЦ оборудования возможен только после включения модуля *Контроль целостности оборудования* (см. п. 2.6.1) и перезагрузки ОС для создания контрольного списка оборудования.

2. При возникновении *Ошибки устройства* и последующем устранении ошибки, путем замены старого устройства на новое, необходимо выбрать п. *Сбросить список оборудования*, для создания нового списка, при следующей перезагрузке для КЦ новой конфигурации оборудования (см. п. 2.6.7).

3. Информация от модуля *Контроль целостности оборудования* сохраняется в журнале событий (см. подраздел 2.9).

4. Если записи о результате последней процедуры КЦ, выводимые на странице *Результат последней проверки*, не умещаются в области № 2 страницы (обозначения областей экранных страниц – см. рис. 3) , то в данной области выводятся стрелки красного цвета: ↑ – дополнительные записи располагаются выше, ↓ – дополнительные записи располагаются ниже.

5. В области № 2 страницы перемещение по записям выполняется клавишами [↑], [↓], а постраничный вывод записей – клавишами [Page Up], [Page Down].

2.6.7. Сброс списка оборудования, подлежащего контролю на целостность

Сброс списка оборудования применяется для обновления данных для КЦ оборудования.

Для сброса списка оборудования, подлежащего КЦ, следует:

1) выбрать п. *Настройки* раздела *Модули безопасности* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности оборудования* (см. рис. 104, 105);

3) выбрать п. *Сбросить список оборудования*;

4) нажать клавишу [Enter], отображается окно (рис. 106), запрашивающее подтверждение на сброс списка оборудования;

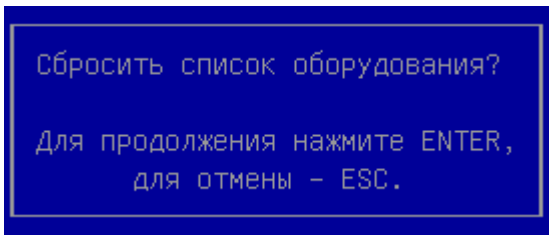

Рис. 106

5) нажать клавишу [Enter], происходит сброс ранее созданного списка оборудования, подлежащего КЦ, и отображается окно (рис. 124), сообщающее о выполненном сбросе списка оборудования;

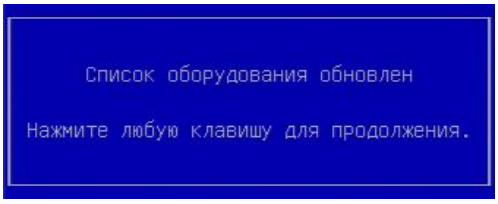

Рис. 107

6) нажать клавишу [Esc] для возврата в главное меню KSS.

Примечание. Сбросить список оборудования, подлежащих КЦ, возможно только после включения модуля *Контроль целостности оборудования* (см. п. 2.6.1).

2.7. Контроль программной среды

2.7.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 37);

3) выбрать п. *Контроль программной среды* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Контроль программной среды: Настройки* с пунктом для включения модуля (рис. 108);

Страница *Контроль программной среды: Настройки*,

пункт для включения модуля

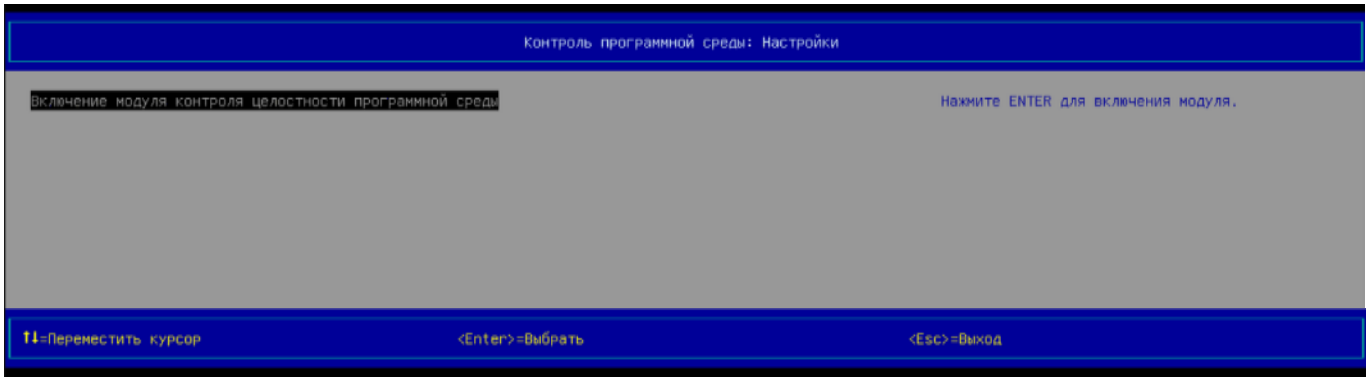

Рис. 108

5) нажать клавишу [Enter], отображается окно (рис. 109) для подтверждения включения модуля;

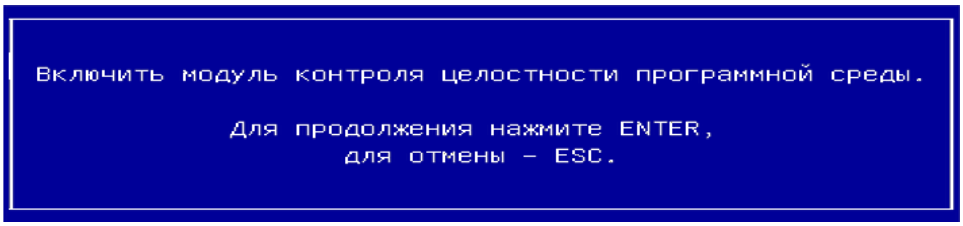

Рис. 109

6) нажать клавишу [Enter], выполняется включение модуля *Контроль программной среды*, откроется страница *Контроль программной среды: Настройки* (рис. 110);

Страница *Контроль программной среды: Настройки* (вид 2),

выбор объектов контроля

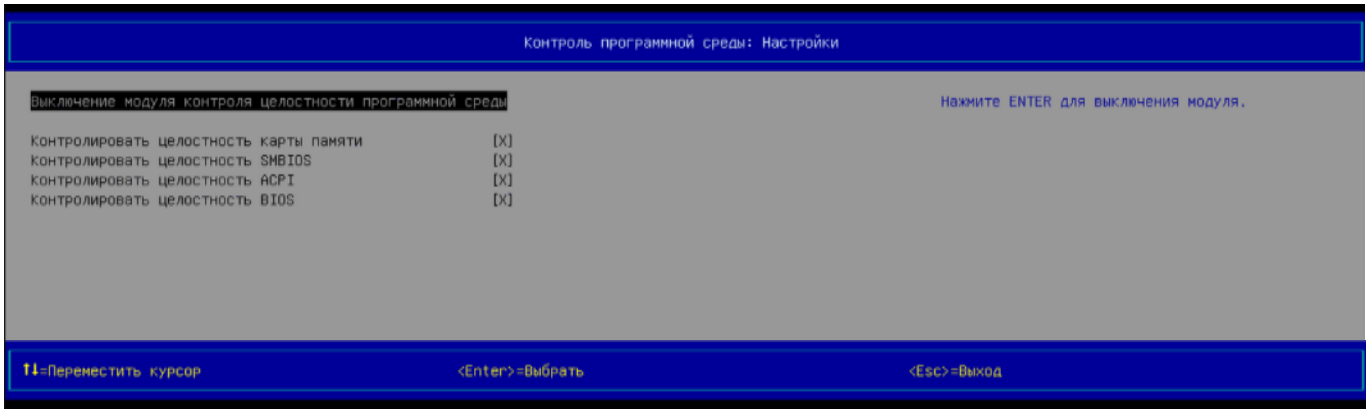

Рис. 110

7) выбрать требуемые объекты контроля из следующего списка:

– *Контролировать целостность карты памяти*;

– *Контролировать целостность SMBIOS*;

– *Контролировать целостность ACPI*;

– *Контролировать целостность BIOS*;

8) чтобы активировать функцию КЦ соответствующего объекта следует выбрать эту функцию и нажать клавишу [Пробел], флажок «X» будет установлен;

9) чтобы деактивировать функцию КЦ соответствующего объекта следует выбрать эту функцию и нажать клавишу [Пробел], флажок «X» будет снят.

2.7.2. Просмотр результата последнего выполнения КЦ программной среды

Для вывода результата последнего выполнения процедуры КЦ программной среды следует:

1) выбрать п. *Контроль программной среды* раздела *Модули безопасности* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль программной среды* (рис. 111);

Страница *Контроль программной среды* с результатом проверки

Рис. 111

3) если необходимо, можно сбросить результаты контроля по отдельным объектам нажатием клавиши [Enter] на соответствующем пункте:

– *Сбросить карту памяти*;

– *Сбросить данные контроля SMBIOS*;

– *Сбросить данные контроля ACPI*;

– *Сбросить данные контроля BIOS*;

4) для закрытия страницы следует нажать клавишу [Esc].

2.7.3. Выключение модуля

Для выключения модуля следует:

1) выбрать п. *Настройки* в главном меню KSS (см. рис. 2);

2) выбрать п. *Контроль программной среды*;

3) нажать клавишу [Enter], отображается страница *Настройки* (рис. 110);

4) выбрать п. *Выключение модуля контроля целостности программной среды*;

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 112), запрашивающее подтверждение на выключение модуля;

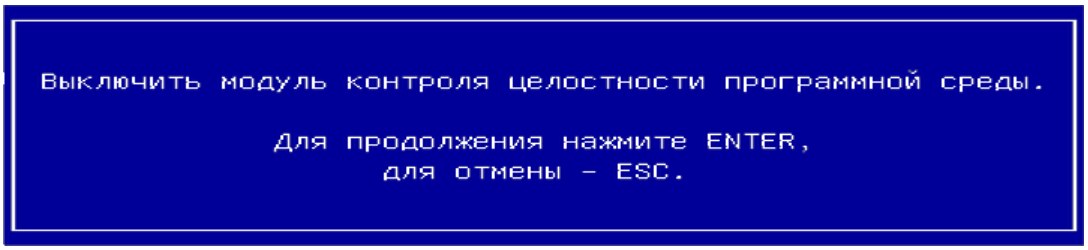

Рис. 112

6) нажать клавишу [Enter], выполняется выключение модуля *Контроль программной среды*, отображение статуса модуля меняется с «Вкл» на «Выкл».

2.8. Контроль целостности реестра Windows

2.8.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Контроль целостности реестра Windows* раздела *Настройки модулей безопасности*, и нажать клавишу [Enter];

4) отображается страница *Контроль целостности реестра Windows: Настройки* с пунктом включения модуля (рис. 113);

Страница *Контроль целостности реестра Windows: Настройки* (вид 1),

пункт для включения модуля

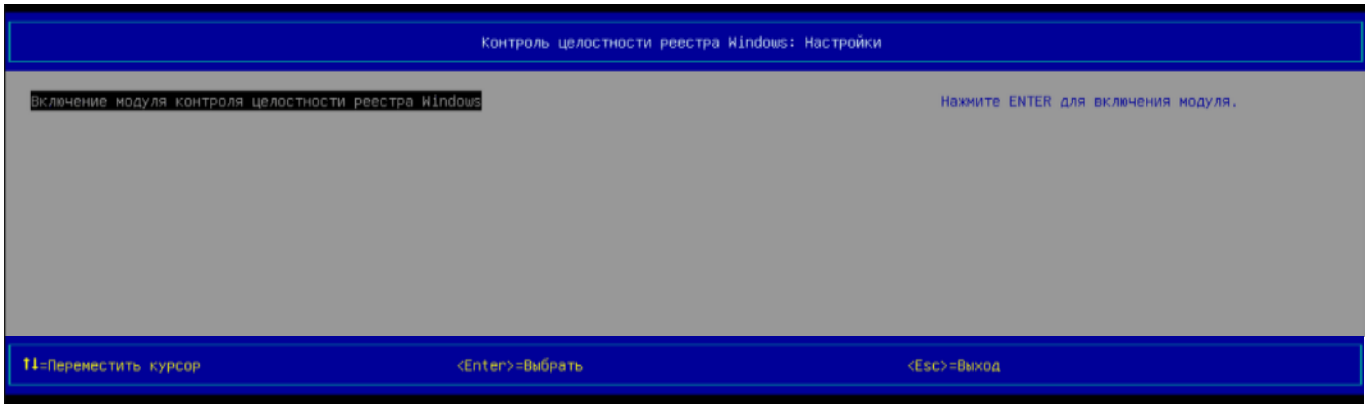

Рис. 113

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 114), запрашивающее подтверждение на включение модуля;

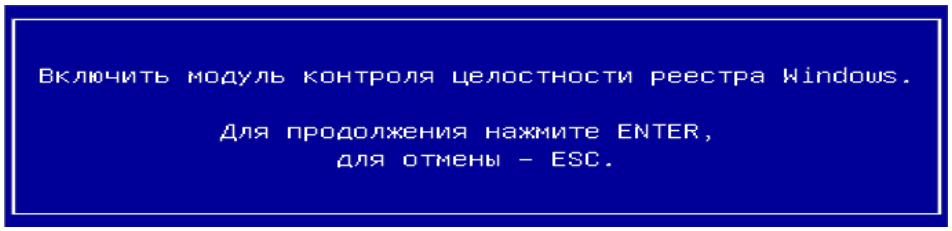

Рис. 114

6) нажать клавишу [Enter], выполняется включение модуля *Контроль целостности реестра Windows*, откроется страница *Контроль целостности реестра Windows: Настройки* (рис. 115);

Страница *Контроль целостности реестра Windows: Настройки*,

выбор хэш-функции

Рис. 115

7) выбрать хеш-функцию, есть возможность использовать следующие функции:

– «CBI»;

– «GOST512»;

– «GOST256».

Примечание. По умолчанию используется хеш-функция CBI.

2.8.2. Выбор параметров реестра Windows для контроля

Чтобы выбрать параметры из некоторого раздела реестра Windows для контроля следует:

1) выбрать п. *Контроль целостности реестра Windows* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности реестра Windows* (рис. 116);

Страница *Контроль целостности реестра Windows*

Рис. 116

3) выбрать п. *Добавить новый раздел*, нажать клавишу [Enter], откроется страница для выбора дисков (рис. 117);

Страница выбора дисков

Рис. 117

4) выбрать дисковое устройство и нажать клавишу [Пробел], далее возможны варианты:

– если на выбранном диске имеется установка Windows, откроется окно для выбора разделов реестра Windows (рис. 118);

Страница выбора разделов реестра Windows

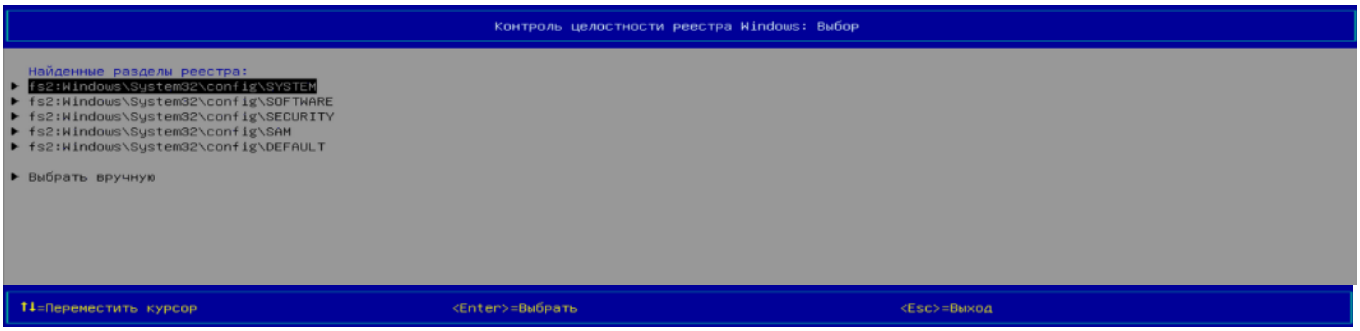

Рис. 118

– если на выбранном диске нет установки Windows, будет сообщено об отсутствии разделов (рис. 119) и можно будет покинуть окно выбора (клавишей [Esc]) или использовать п. *Выбрать вручную* для выбора на диске файла, содержащего раздел реестра (рис. 120);

Разделы реестра Windows автоматически не обнаружены

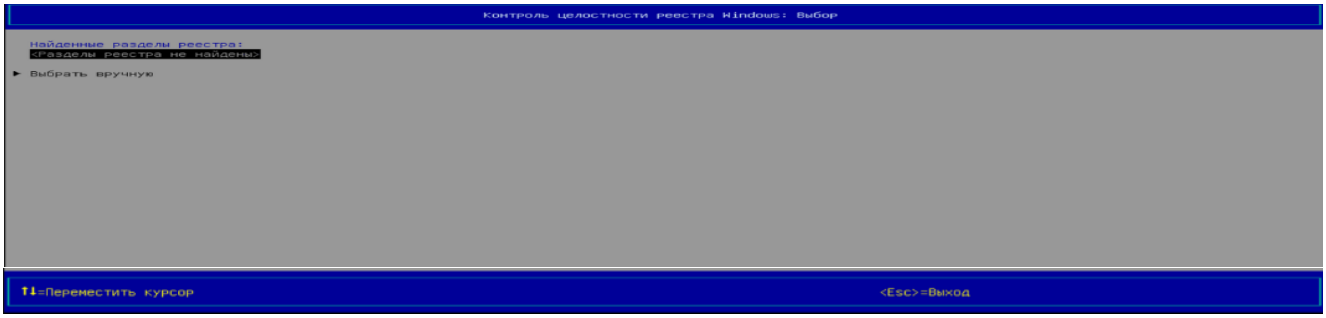

Рис. 119

Ручной выбор файлов, содержащих разделы реестра Windows

Рис. 120

5) чтобы добавить параметр контроля из автоматически обнаруженного раздела, нужно передвинуть на раздел курсор и нажать клавишу [Enter], раздел будет добавлен в список контролируемых (рис. 121), но пока без добавки параметров;

Добавлен один раздел реестра Windows

(пока не добавлено ни одного контролируемого параметра)

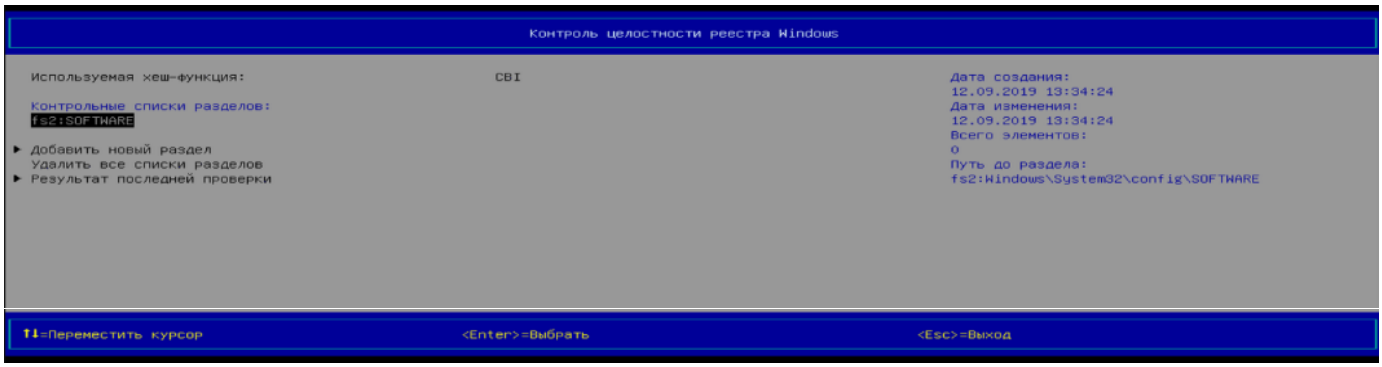

Рис. 121

6) чтобы добавить параметр, нужно передвинуть на раздел курсор и вновь нажать клавишу [Enter], появится контекстное меню (рис. 122);

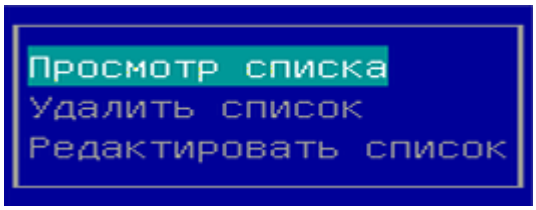

Рис. 122

7) для добавления параметра нужно выбрать п. *Редактировать список* и нажать клавишу [Enter] для входа в «дерево» реестра. Передвижение по уровням «дерева» выполняется клавишами [↑], [↓], [Enter] (Перейти ниже), [Esc] (Перейти выше), а выбор параметра – клавишей [Пробел] (рис. 123). Чтобы выбор параметров был запомнен, нужно нажать клавишу [F2] (Выход с сохранением), перед сохранением будет запрос, на который нужно ответить утвердительно;

Добавление двух параметров для контроля

Рис. 123

8) после сохранения добавленных параметров, их общее количество будет показано на странице *Контроль целостности реестра Windows* (рис. 124);

Добавлено три параметра в одном разделе

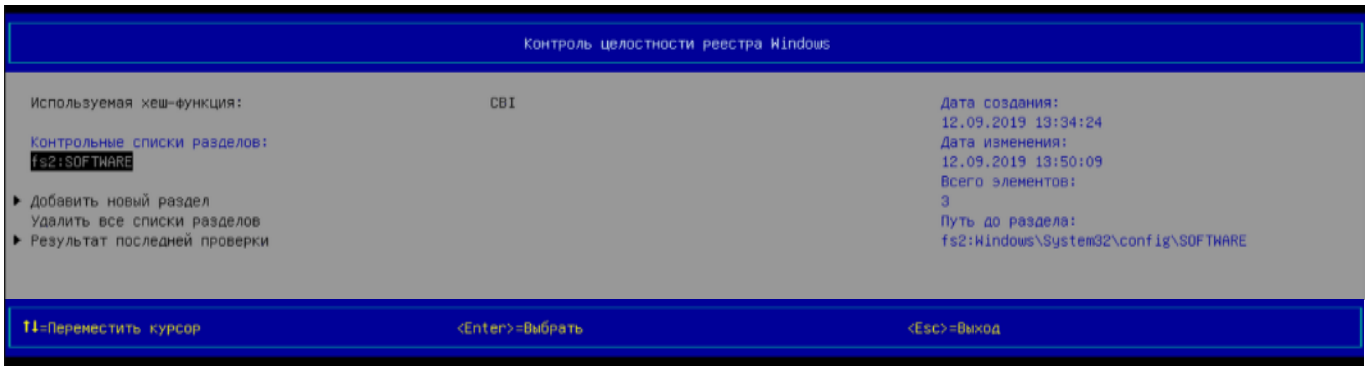

Рис. 124

9) просмотр списка добавленных параметров в разделе (через пункт контекстного меню *Просмотр списка*) имеет такой же интерфейс: передвижение по уровням «дерева» выполняется клавишами [↑], [↓], [Enter] (Перейти ниже), [Esc] (Перейти выше), увидеть значение параметра можно будет только после достижения той «ветви дерева», к которой данный параметр относится;

10) удаление списка добавленных параметров в разделе (через пункт контекстного меню *Удалить список*) удаляет все параметры только одного выбранного раздела, перед удалением будет запрос, на который нужно ответить утвердительно;

11) чтобы добавить параметр из раздела, не определяемого автоматически, нужно использовать п. *Выбрать вручную* (см. рис. 118), откроется окно для ручного выбора файлов реестра Windows (см. рис. 120);

12) п. *Удалить все списки разделов* (см. рис. 116) действует в соответствии со своим названием, перед удалением будет запрос, на который нужно ответить утвердительно.

Примечание. По умолчанию системный реестр Windows хранится в файлах:

1) папка `%Systemroot%\system32\config\`, в которой в файлах находятся разделы:

–файл SAM — раздел HKEY_LOCAL_MACHINE\SAM;

–файл SECURITY — раздел HKEY_LOCAL_MACHINE\Security;

–файл Software — раздел HKEY_LOCAL_MACHINE\Software;

–файл System — раздел HKEY_LOCAL_MACHINE\System и HKEY_CURRENT_CONFIG;

–файл Default — раздел HKEY_USERS\.DEFAULT;

2) папка %SystemRoot%\Users\%username%\ (для версии Windows не младше чем Windows-7) с файлом NTUSER.DAT, в которой находится раздел HKEY_CURRENT_USER. В папке `%Systemroot%\system32\config\` находятся также файлы реестра с расширениями:

–.ALT — содержит архивную копию раздела HKEY_LOCAL_MACHINE\System;

–.LOG — журнал изменений, записывающий модификации ключей и значений реестра;

–.SAV — копия реестра на момент завершения текстовой фазы процесса установки Windows.

ВНИМАНИЕ! ИНТЕРФЕЙС ВЫБОРА ВРУЧНУЮ ФАЙЛА, СОДЕРЖАЩЕГО РАЗДЕЛЫ РЕЕСТРА WINDOWS, НЕ ПОЗВОЛЯЕТ ИСПОЛЬЗОВАТЬ ФАЙЛЫ, ИМЕЮЩИЕ В ФАЙЛОВОЙ СИСТЕМЕ ОС ПРИЗНАКИ «СКРЫТЫЙ» И/ИЛИ «СИСТЕМНЫЙ».

2.8.3. Выключение модуля

Для выключения модуля следует:

1) выбрать п. *Настройки* в главном меню KSS (см. рис. 2);

2) выбрать п. *Контроль целостности реестра Windows*;

3) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 115);

4) выбрать п. *Выключение модуля контроля целостности реестра Windows*;

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 125), запрашивающее подтверждение на выключение модуля;

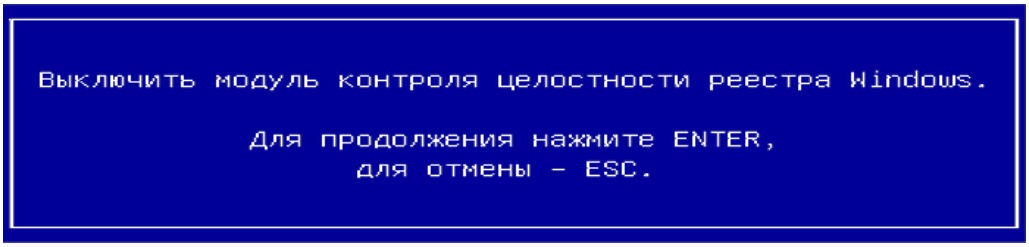

Рис. 125

6) нажать клавишу [Enter], выполняется выключение модуля *Контроль целостности реестра Windows*, отображение статуса модуля меняется с «Вкл» на «Выкл».

2.8.4. Просмотр результата последней процедуры КЦ реестра Windows

Для вывода результата последней процедуры КЦ реестра Windows следует:

1) выбрать п. *Контроль целостности реестра Windows* раздела *Модули безопасности* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Контроль целостности реестра Windows* (рис. 126);

Страница *Контроль целостности реестра Windows*

Рис. 126

3) выбрать п. *Результат последней проверки*, нажать клавишу [Enter], отображается страница *Контроль целостности реестра* Windows: *Результаты проверки* (рис. 127);

Страница *Контроль целостности реестра Windows* с результатами проверки

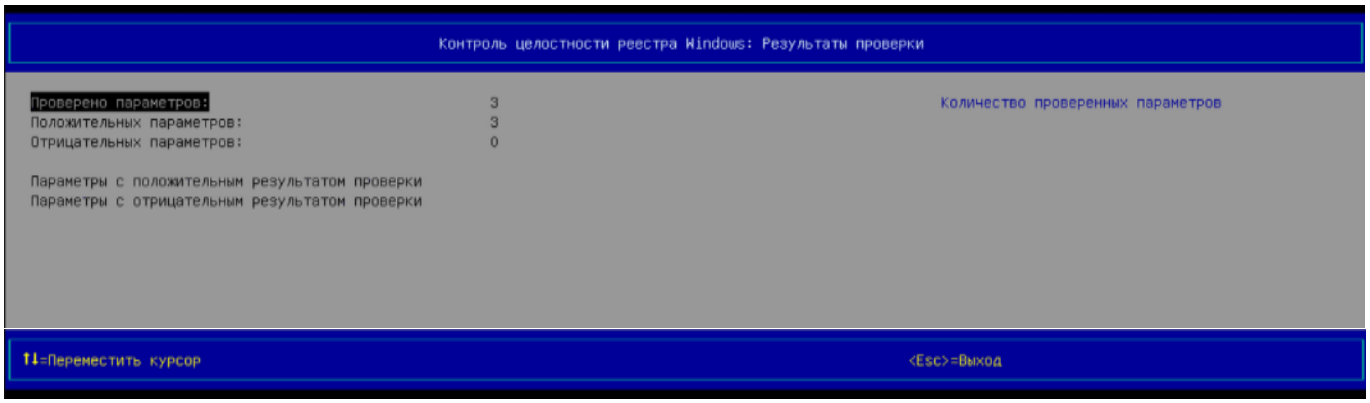

Рис. 127

4) для просмотра КС конкретных параметров следует использовать пункты *Параметры с положительным результатом проверки* и *Параметры с отрицательным результатом проверки*, просмотр выполняется в отдельном окне (рис. 128), передвижение по уровням «дерева» выполняется клавишами [↑], [↓], [Enter] (Перейти ниже), [Esc] (Перейти выше), увидеть КС параметра можно будет только после достижения той «ветви дерева», к которой данный параметр относится.

Страница *Результаты контроля целостности* реестра с КС конкретных параметров

Рис. 128

2.9. Журнал событий

Записи о событиях всех модулей безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2 заносятся в общий журнал событий.

2.9.1. Включение модуля

Для включения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (рис. 129) с п. *Включение модуля управления журналом событий*;

Страница *Управление журналом событий: Настройки* (вид 1),

п. *Включение модуля управления журналом событий*

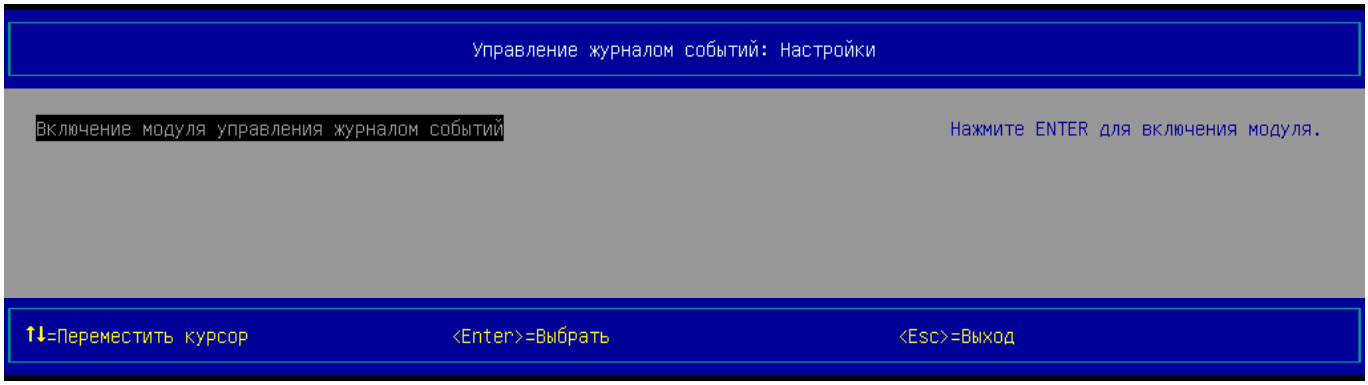

Рис. 129

5) нажать клавишу [Enter], отображается окно (рис. 130), запрашивающее подтверждение на включение модуля;

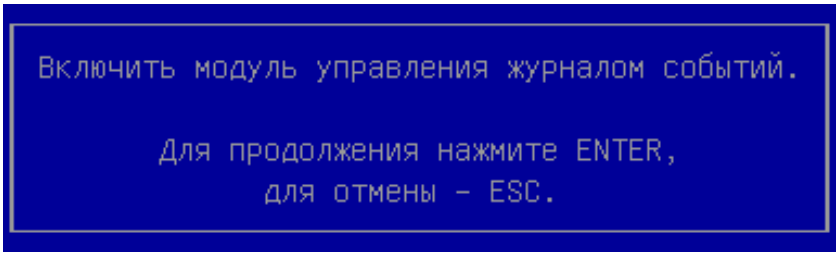

Рис. 130

6) нажать клавишу [Enter], выполняется включение модуля *Журнал событий*, на странице *Настройки*, отображение статуса модуля меняется с «Выкл» на «Вкл».

2.9.2. Выключение модуля *Журнал событий*

Для выключения модуля следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (рис. 131) с п. *Выключение модуля управления журналом событий*;

Страница *Управление журналом событий: Настройки* (вид 2),

п. *Выключение модуля управления журналом событий*

Рис. 131

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 132), запрашивающее подтверждение на выключение модуля;

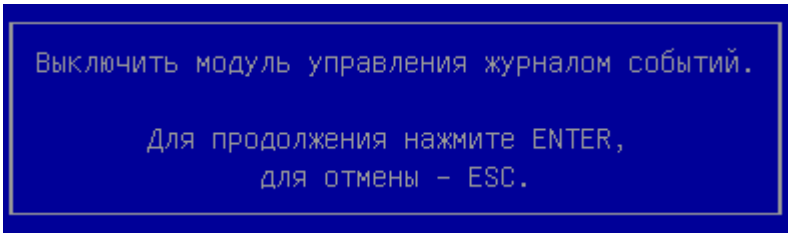

Рис. 132

6) нажать клавишу [Enter], выполняется выключение модуля *Журнал событий*, отображается страница *Настройки*, отображение статуса модуля меняется с «Вкл» на «Выкл».

2.9.3. Защита от перезаписи

Журнал событий организован как кольцевой буфер, в котором самые старые (по времени наступления события) записи постепенно затираются самыми новыми (по времени наступления события). Если недопустима потеря информации о событиях, можно использовать возможность защищать журнал событий от перезаписи, для чего следует:

1) на странице *Управление журналом событий: Настройки* выбрать п. *Защита от перезаписи*;

2) нажать клавишу [Пробел], отображается еще одна строка с дополнительным п. *Блокирование загрузки при переполнении*, который может быть активирован клавишей [Пробел] (рис. 133).

Страница *Управление журналом событий: Настройки:*,

пп. *Защита от перезаписи*, *Блокирование загрузки при переполнении*

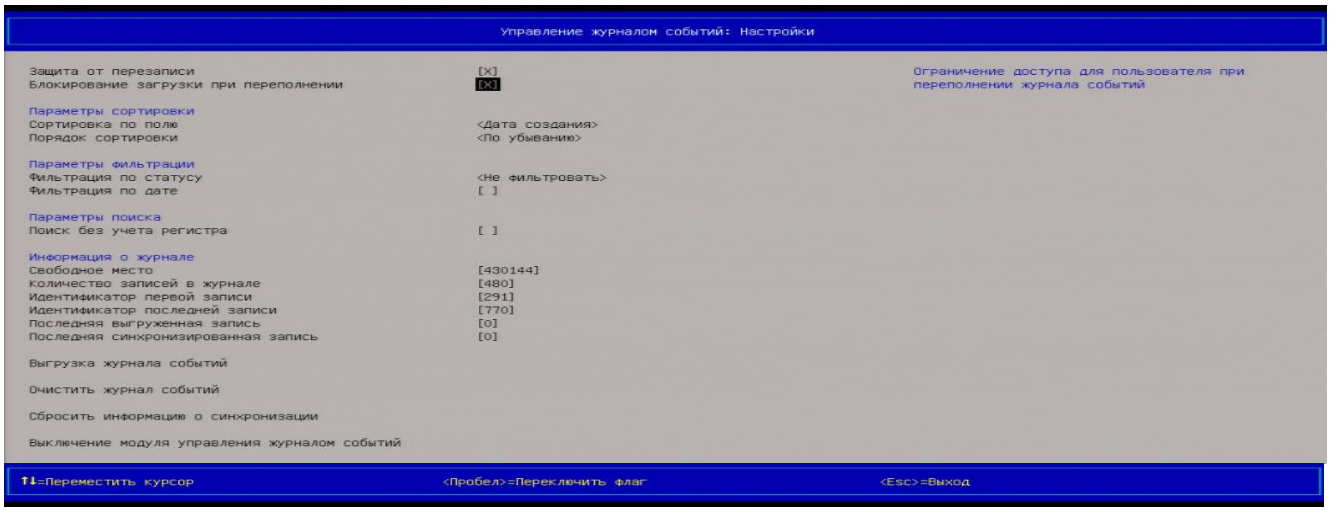

Рис. 133

Примечания:

1. Защита от перезаписи возможна только после включения модуля *Журнал событий* (см. п. 2.9.1).

2. Если задана защита от перезаписи, и обнаружено переполнение журнала, но параметр *Блокирование загрузки при переполнении* НЕ активирован, новые события не будут записываться в журнал (будут теряться), но ни одно ранее произошедшее событие не будет перезаписано и утеряно.

3. Если задана защита от перезаписи, обнаружено переполнение журнала, и параметр *Блокирование загрузки при переполнении* активирован, загрузка ОС блокируется и вход возможен только администратору, который может очистить журнал (и) или разрешить перезапись.

2.9.4. Просмотр журнала событий

Для просмотра журнала событий следует:

1) выбрать п. *Журнал событий* раздела *Модули безопасности* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Журнал событий* (рис. 134).

Страница *Журнал событий*

Рис. 134

Формат записи журнала событий:

/Дата события//Время события//Субъект, вызвавший событие//Описание события/

Общее количество записей в журнале событий зависит от свободного объема памяти в микросхеме SPI Flash. Когда журнал событий полностью заполнен, данные о новых событиях записываются поверх самых старых данных, то есть, новые записи «затирают» самые старые.

Примечания:

1. Просмотр журнала событий ПК «ЭЗ «ВИТЯЗЬ» 2.2 возможен только после включения модуля *Журнал событий* (см. п. 2.9.1).

2. Перемещение по строкам записей журнала событий выполняется клавишами [↑], [↓].

3. Для журнала событий перемещение курсора на первую и последнюю строки записей выполняется клавишами [Page Up], [Page Down], а постраничный вывод записей – клавишей [Enter], при перемещении курсора на строку <Следующая страница>.

4. В ПК «ЭЗ «ВИТЯЗЬ» 2.2 применяется цветовая индикация событий. Цвет записи события в журнале зависит от типов событий. Каждое событие журнала может быть одного цвета и принадлежать к одному из следующих типов:

–Зеленый – сведения. Событие, которое обозначает успешное выполнение какой-либо задачи. Например, событие с типом «Сведения» будет записано при успешном создании профиля первого администратора.

–Желтый – предупреждение. Событие может не быть важным, но может указывать на возможность возникновения отрицательных последствий в дальнейшем. Например, предупреждение будет записано в журнал, когда будет отключен модуль *Контроль целостности оборудования*.

–Красный – ошибка. Событие обозначает нарушение КЦ системы. Например, когда нарушена целостность оборудования системы.

2.9.5. Сортировка журнала событий

Представление журнала событий на экране можно отсортировать (упорядочить по возрастанию или убыванию какого-либо параметра).

Для выбора параметра сортировки журнала событий следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (рис. 135);

Страница *Управление журналом событий: Настройки*

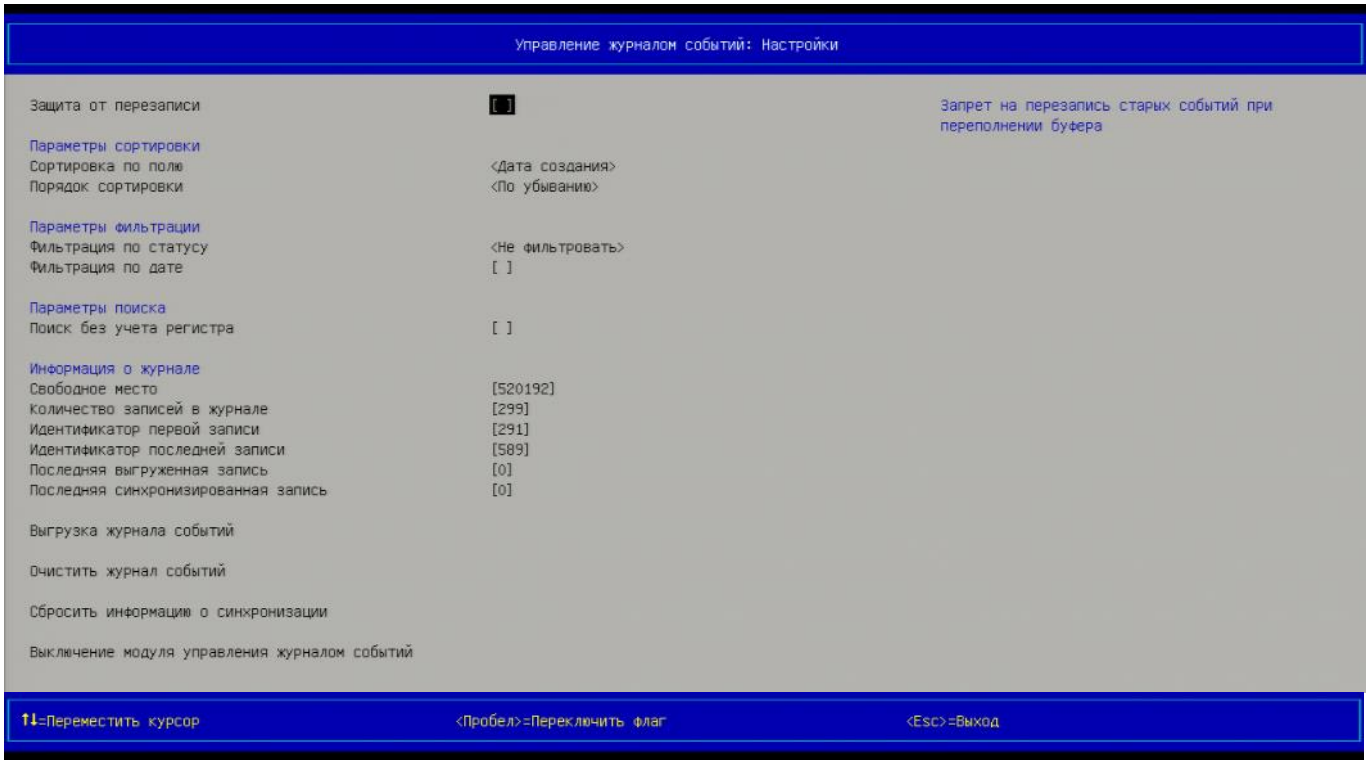

Рис. 135

5) выбрать п. *Сортировка по полю*;

6) нажать клавишу [Enter], отображается окно (рис. 136) для выбора поля, по которому нужно выполнять сортировку;

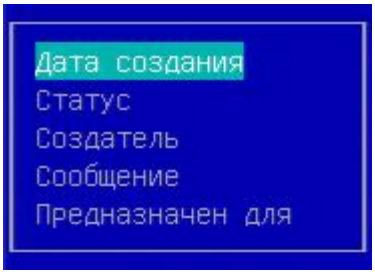

Рис. 136

7) выбрать нужное поле и нажать клавишу [Enter], для возврата на страницу;

8) выбрать п. *Порядок сортировки* и нажать клавишу [Enter];

9) выбрать нужное направление упорядочивания (*По убыванию* или *По возрастанию*);

10) нажать клавишу [Enter];

11) нажать клавишу [Esc] для возврата на страницу.

2.9.6. Фильтрация журнала событий

При просмотре, журнал событий можно отфильтровать, таким образом, чтобы показывать только интересующие строки.

Для фильтрации журнала событий следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (см. рис. 135);

5) выбрать п. *Фильтрация по статусу*;

6) нажать клавишу [Enter], отображается окно (рис. 137) для типа событий, которые нужно показывать при просмотре журнала событий;

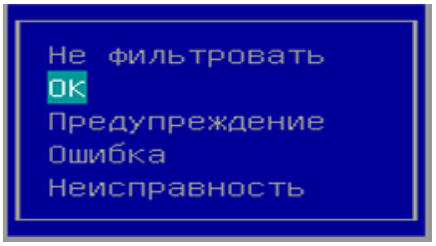

Рис. 137

7) выбрать нужное поле;

8) нажать клавишу [Enter], для возврата на страницу;

9) при необходимости просмотра событий только за конкретную дату, выбрать п. *Фильтрация по дате* и нажать клавишу [Пробел], на экране будет показано поле выбора даты (рис. 138);

Выбор даты, за которую нужно показать события при просмотре журнала

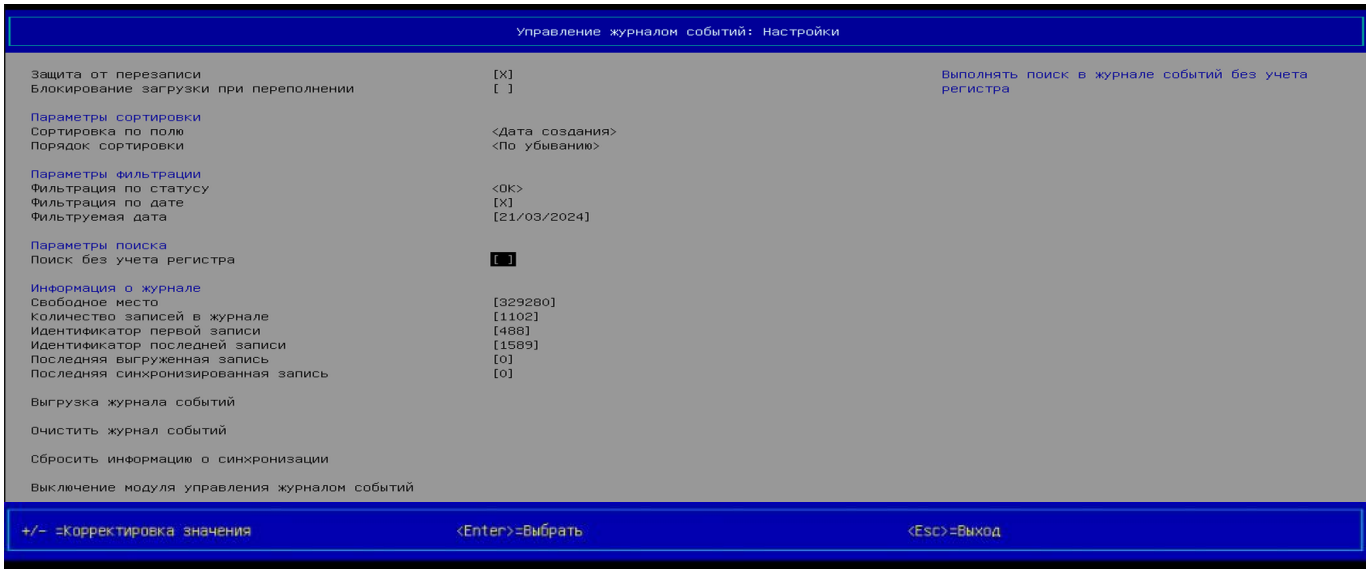

Рис. 138

10) выбрать дату;

11) нажать клавишу [Esc], для возврата на страницу.

Примечания:

1. Перемещение между составляющими даты (число/месяц/год) осуществляется при помощи клавиш [←], [→].

2. Изменение значений каждой отдельной составляющей даты осуществляется при помощи клавиш [**-**] (уменьшение) и [**+**] (увеличение). Подсказка по клавишам уменьшения/увеличения значений показана в нижней строке экрана.

2.9.7. Поиск в журнале событий

При просмотре журнала событий, в верхней строке экрана имеется поле *Поиск в журнале*. Чтобы им воспользоваться, нужно установить на него курсор и нажать клавишу [Enter] для ввода *Строки для поиска*. После ввода значения и нажатия клавиши [Enter] на экране останутся только те строки, в которых имеется заданное для поиска значение (то есть, произойдет фильтрация содержимого журнала). Если заданное значение не будет найдено во всем журнале, вместо содержимого журнала выдается сообщение: *«Нет элементов для отображения»*.

Примечания:

1. По умолчанию при поиске имеет значение регистр символов (заглавные и строчные буквы считаются различными). Этот режим можно отключить с помощью параметра *Поиск без учета регистра* (см. рис. 135).

2. Вернуться к просмотру полного журнала (не отфильтрованного по результатам поиска) можно нажатием клавиши [Esc] (произойдет выход из журнала) и затем клавиши [Enter] для повторного входа в журнал.

3. Для изменения ранее введенной *Строки для поиска* нужно установить в нее курсор, нажать клавишу [Enter] и начать ввод нового значения. Пока не начат ввод, нельзя изменить старое значение, после начала ввода можно использовать для редактирования клавиши [←], [→] и [BackSpace] (клавиша [Delete] не работает в этом окне), режим ввода символов – «вставка».

2.9.8. Сохранение журнала событий в файл

Для сохранения журнала событий ПК «ЭЗ «ВИТЯЗЬ» 2.2 в файл следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (рис. 139) с п. *Выгрузка журнала событий*;

Управление журналом событий: Настройки,

п. *Выгрузка журнала событий*

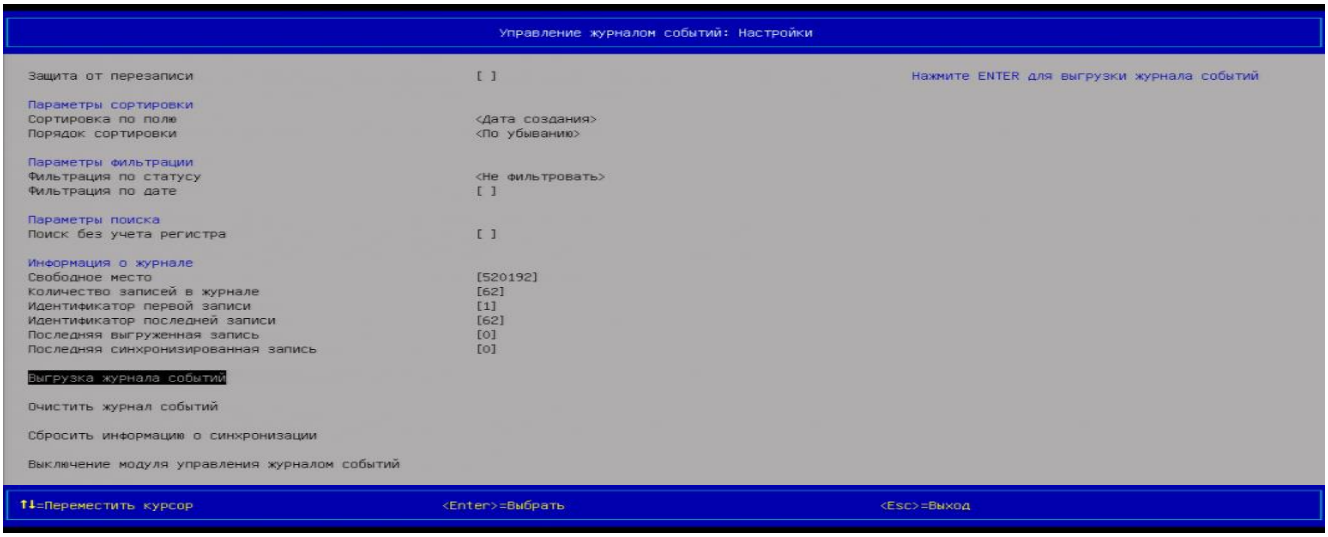

Рис. 139

5) подключить USB-диск к USB-порту;

6) выбрать п. *Выгрузка журнала событий*;

7) нажать клавишу [Enter], в корне USB-диска сохраняется текстовый файл *EventLog-dd-mm-hh-mm-ss.json* с данными журнала событий, где *dd* – день, *mm* – месяц, *hh* – часы, *mm* – минуты, *ss* – секунды, и отображается окно (рис. 140), информирующее администратора об успешном сохранении журнала;

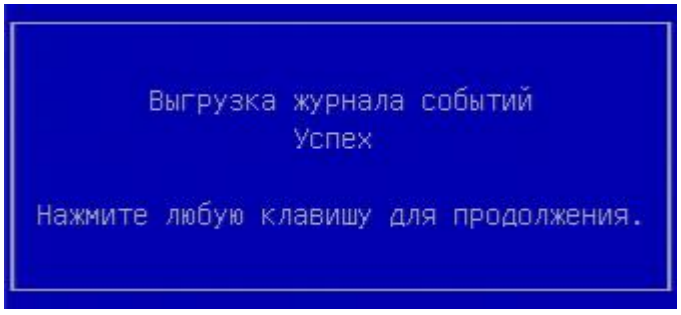

Рис. 140

8) нажать любую клавишу на клавиатуре.

Примечания:

1. Перемещение между строками меню осуществляется клавишами [↑], [↓].

2. EventLog-dd-mm-hh-mm-ss.json – это текстовый файл (JavaScript Object Notation), который содержит определенные данные в структурированной форме. Для ознакомления с данными отчета следует открыть данный файл в соответствующем текстовом редакторе.

3. При отсутствии подключенного USB-диска, после нажатия на клавишу [F10] отображается окно (рис. 141), информирующее об отсутствии устройства памяти.

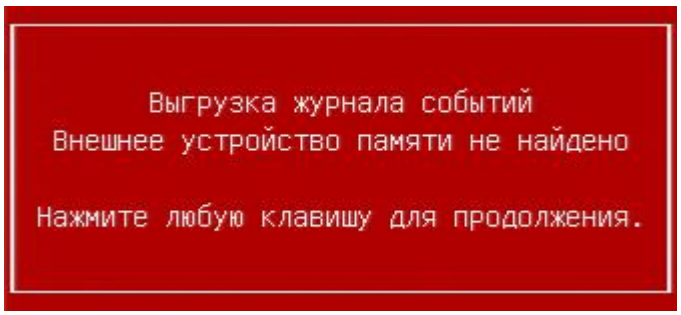

Рис. 141

4. Если сохранить журнал событий в файл невозможно (например, нет места на диске), то отображается окно (рис. 142).

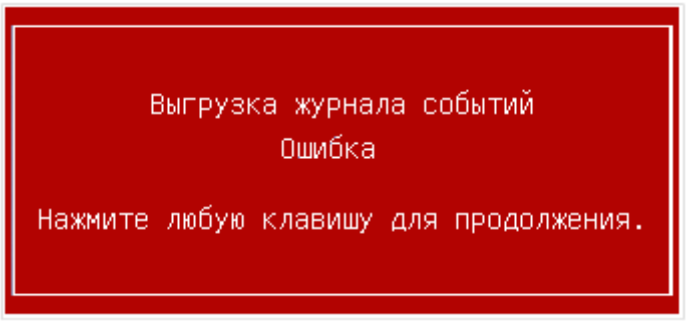

Рис. 142

2.9.9. Очистка журнала событий

Для очистки журнала событий следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 37);

3) выбрать п. *Журнал событий* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Управление журналом событий: Настройки* (рис. 143) с п. *Очистить журнал событий*;

Управление журналом событий: Настройки,

п. *Очистить журнал событий*

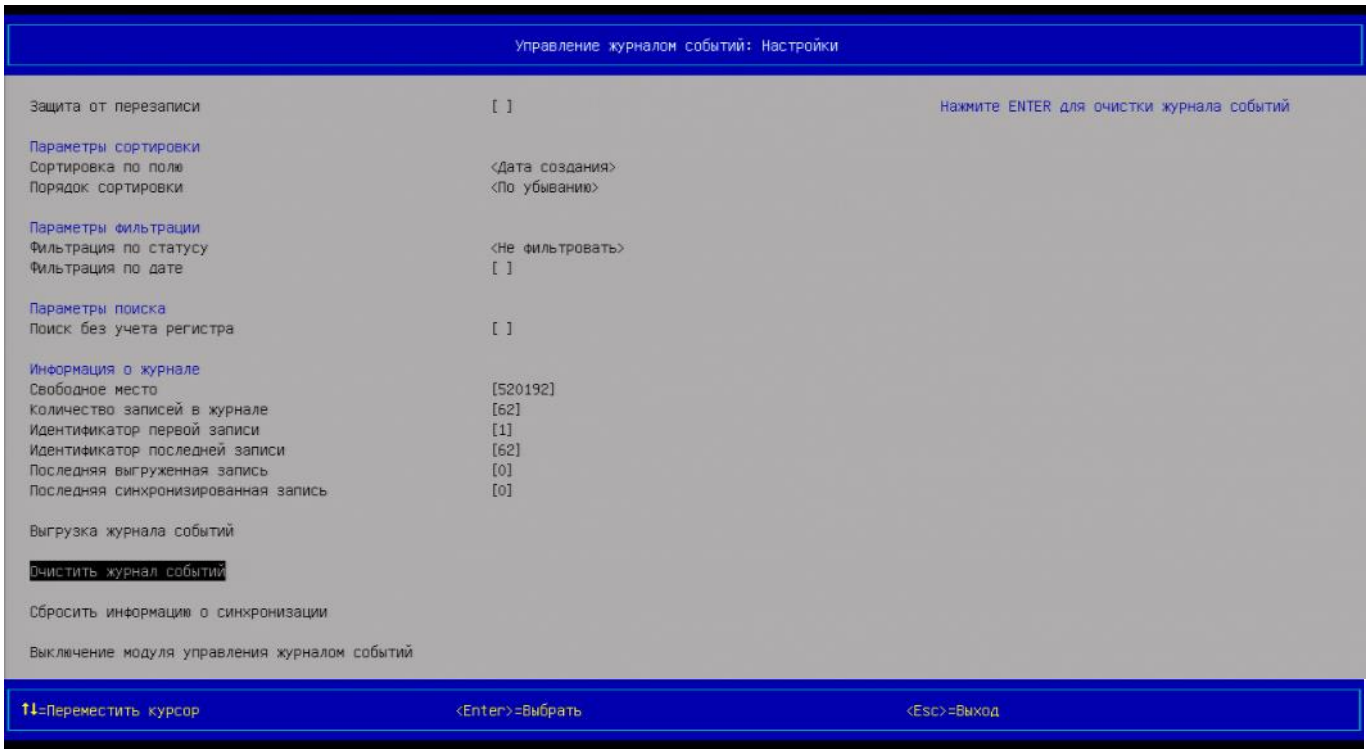

Рис. 143

5) выбрать п. *Очистить журнал событий*;

6) нажать клавишу [Enter], отображается окно (рис. 144), запрашивающее подтверждение на очистку журнала событий;

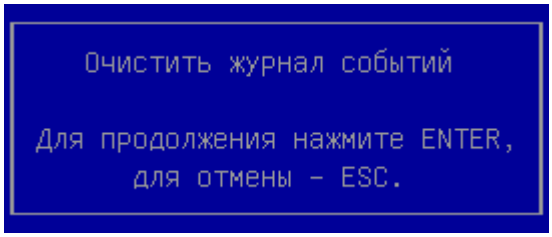

Рис. 144

7) нажать клавишу [Enter], происходит очистка ранее сформированного журнала событий;

8) нажать клавишу [Esc], для возврата на страницу.

2.10. Антивирус Касперского для UEFI

Модуль *Антивируса Касперского для UEFI* выполняет антивирусную проверку сразу после прохождения пользователем аутентификации.

2.10.1. Включение и выключение антивирусной проверки

Чтобы включить или выключить антивирусную проверку, следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) выбрать п. *Антивирус Касперского для UEFI* и нажать клавишу [Enter];

3) откроется страница *Антивирус Касперского для UEFI* (рис. 145);

Страница *Антивирус Касперского для UEFI*

Рис. 145

4) выбрать п. *Включить антивирусную проверку* и нажать клавишу [Enter];

5) отображается окно с текстом *Лицензионного соглашения*, приведенного в сокращенном виде (полный текст приведен на официальном сайте АО «Лаборатория Касперского» по адресу: http://support.kaspersky.ru/kuefi/eula).

6) далее выполнить одно из следующих действий:

– если вы согласны с условиями лицензионного соглашения, нажать кнопку [Принять]. Для параметра *Включить Антивирус Касперского для UEFI* будет установлено значение [X]. Если соглашение принято, подсистема проверки модуля выполняет антивирусную проверку критически важных областей ОС и папок, используемых ОС, перед ее загрузкой.

– если вы не согласны с условиями лицензионного соглашения, нажать кнопку [Отказаться]. Значение параметра *Включить Антивирус Касперского для UEFI* не изменится. Если соглашение не принято, подсистема проверки модуля не выполняет антивирусную проверку критически важных областей ОС и папок, используемых ОС, перед ее загрузкой.

При повторном включении или выключении антивирусной проверки окно с текстом лицензионного соглашения не отображается.

Примечания:

1. Параметр будет применен после выхода из оболочки KSS и перезагрузки ОС.

2. По умолчанию антивирусная проверка выключена.

2.10.2. Включение и выключение загрузки антивирусных баз

Для включения/выключения загрузки антивирусных баз из пользовательской папки следует:

1) выбрать п. Настройки раздела Конфигурация главного меню KSS;

2) выбрать п. Антивирус Касперского для UEFI и нажать клавишу [Enter];

3) в разделе Параметры хранилища выбрать п. Настройка путей к хранилищу;

4) ввести значения путей по ФС загрузочного диска – один или несколько (до трех) вариантов в полях Путь 1, Путь 2, Путь 3;

5) выйти из пункта по клавише [Esc];

6) в разделе Параметры хранилища выбрать п. Расположение хранилища;

7) клавишей [Enter] выбрать одно из следующих значений параметра:

– «По умолчанию» – антивирусные базы загружаются из папки, заданной по умолчанию;

– «Пользовательские папки» – антивирусные базы загружаются из пользовательских папок, заданных в полях *Путь 1*, *Путь 2*, *Путь 3*.

Примечания:

1. Параметр будет применен после выхода из оболочки KSS и перезагрузки ОС.

2. Хранилище антивируса Касперского – хранилище файлов, необходимых для антивирусной проверки и устранения угроз модулем. По умолчанию хранилище расположено в папках:

–для поддерживаемых ОС Windows -
- AllUsersProfile%\Kaspersky Lab\Kaspersky Antivirus for UEFI;

–для поддерживаемых ОС семейства Linux - /var/opt/kaspersky/kav_uefi.

В хранилище модуля расположены следующие папки:

–*bases* – папка для хранения антивирусных баз;

–*quarantine* – хранилище файлов, помещенных на карантин. *Карантин* – это специальное изолированное хранилище, в котором файлы хранятся в упакованном виде. Перед выполнением действий над зараженными файлами модуль создает резервные копии файлов и помещает их на карантин. Карантин предоставляет возможность удалить, восстановить или повторно проверить файлы, помещенные в хранилище. Файлы, помещенные на карантин, не могут нанести вред компьютеру;

–*backup* – резервное хранилище копий критически важных для работы ОС файлов (System Critical Objects). Резервные копии критически важных файлов создаются при первой антивирусной проверке, которая длится дольше, чем последующие. При обнаружении угрозы в критически важном файле вы можете восстановить файл из резервного хранилища.

2.10.3. Задания путей проверки файлов

Чтобы добавить папки к антивирусной проверке, следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) выбрать п. *Антивирус Касперского для UEFI* и нажать клавишу [Enter];

3) в списке *Параметры проверки* выбрать п. *Настройка дополнительной проверки* и нажать клавишу [Enter];

4) ввести значения путей по ФС загрузочного диска – один или несколько (до трех) вариантов в полях *Путь 1*, *Путь 2*, *Путь 3*;

5) в поле ввода указать канонические пути к файлам и папкам, которые требуется добавить в область проверки (например, */startup/prog/*);

6) выйти из пункта по клавише [Esc].

Примечания:

1. Параметр будет применен после выхода из оболочки KSS и перезагрузки ОС.
2. По умолчанию в параметрах дополнительной проверки выбран вариант Путь 1, которому соответствует область проверки: /bin; /sbin; /usr/bin; /usr/sbin; /tmp.
3. Вы можете не указывать имя локального диска – в этом случае подсистема проверки выполнит поиск указанных файлов на всех дисках.
4. Если вы хотите добавить в область проверки файлы, которые находятся в папке, и исключить файлы во вложенных папках, используйте знак «*» (например, /startup/prog/*).
5. При вводе пути к папкам и файлам, которые требуется добавить в область проверки, соблюдайте следующие правила:

–в качестве разделительного символа можно использовать «;» или «,»;

–при вводе пути к файлу или папке для всех ФС следует соблюдать регистр;

–не следует использовать маски или переменные окружения. Исключение составляет символ «*», который может быть использован только в конце пути и после символов «/» или «\» (например, /startup/prog/*). Запрещено использовать символ «*» в имени файла или папки для выбора нескольких объектов (например, file*.exe);

–не следует использовать пути, которые содержат точку монтирования. Следует указывайть путь к папкам или файлам от корня тома, на котором они находятся;

–не следует использовать символы: «?», «|», «:» (их разрешается использовать только после буквы диска), а также символы «<», «>» (везде);

–максимальное количество символов в строке – 255.

6. Если по указанному к папке пути подсистема проверки модуля не находит антивирусные базы во время антивирусной проверки, то загрузка ОС блокируется (рис. 146).

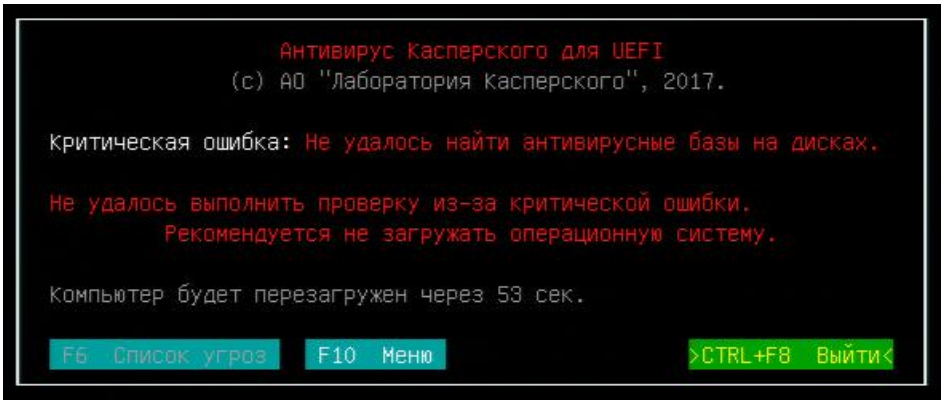

Рис. 146

2.10.4. Исключение файлов из проверки

Чтобы исключить файлы из антивирусной проверки, следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) выбрать п. *Антивирус Касперского для UEFI* и нажать клавишу [Enter];

3) в списке *Параметры проверки* выбрать п. *Исключения из проверки*, нажать клавишу [Enter];

4) указать в поле ввода имена файлов, маски имен файлов или пути к файлам, которые требуется исключить из антивирусной проверки.

Примечания:

1. По умолчанию список файлов, исключенных из антивирусной проверки, пуст.
2. Во время проверки критически важных областей ОС и папок, используемых ОС при загрузке, подсистема проверки будет пропускать указанные файлы.
3. Не следует использовать имя диска при указании пути к файлам. Подсистема проверки модуля выполняет поиск указанных файлов, масок имен файлов и путей к файлам на всех дисках.
4. Можно использовать знак «*» после имени папки, чтобы исключить из антивирусной проверки все файлы, расположенные в ней, например, \kav\logs*.
5. Имена файлов следует записывать в одну строку. В качестве разделителя можно использовать запятую или точку с запятой. Максимальное количество символов в строке – 255.
6. Для всех ФС учитывается регистр при задании имени файла и маски файла.
7. Параметр будет применен после выхода из оболочки KSS и перезагрузки ОС.

2.10.5. Обновление антивирусной базы

Обновление антивирусной базы проводится администратором «локально» без применения средств автоматизации в следующей последовательности:

1) скачивание файлов антивирусной базы из доверенного источника (сайта производителя). Скачивание выполняется автоматически на отдельном компьютере, имеющем доступ в интернет с помощью программы «агента», работающего под управлением одной из поддерживаемых ОС.

2) копирование файлов антивирусной базы на автономный носитель (переносной диск, Flash-диск, CD/DVD-диск и т.п.).

3) копирование файлов антивирусной базы с автономного носителя на раздел ФС компьютера с ПК «ЭЗ «ВИТЯЗЬ» 2.2 в одну из папок, путь к которой был ранее задан в настройках (см. п. 2.10.2).

Примечания:

1. Выполнение операции по обновлению антивирусной базы производится после завершения работы ПК «ЭЗ «ВИТЯЗЬ» 2.2.
2. Файлы антивирусной базы содержат только информацию о вредоносном коде и не являются исполняемыми, поэтому обновление антивирусной базы нельзя рассматривать как обновление самого ПК «ЭЗ «ВИТЯЗЬ» 2.2.
3. Адреса доверенных источников для антивирусных БД (настраиваются в программе «агент») указаны в формуляре на ПК «ЭЗ «ВИТЯЗЬ» 2.2.
4. Периодичность проверки обновлений антивирусных БД рекомендуется установить не реже одного раза в сутки.

2.10.6. Настройка действий при обнаружении угрозы

Администратор может разрешить или запретить некоторые действия при обнаружении ПКПВ. Эти параметры устанавливаются простановкой соответствующих флажков в разделе *Действия при обнаружении угрозы* на странице *Настройки* (см. рис. 145).

Примечание. Не рекомендуется устанавливать флажок *Разрешить пользователю выбирать действие*, который позволит обычному пользователю проводить лечение или восстановление или удаление зараженных файлов, так как, это может нарушить организационные правила безопасности в организации.

2.10.7. Работа с «грязными» дисками

Среди параметров модуля имеется параметр *Разрешить лечение на "грязных" дисках* (см. рис. 145). «Грязный диск» – это диск, помеченный для проверки на загрузке. ОС помечает диск для проверки перед загрузкой «грязным», если работа была завершена не штатно, например, если выдернуть кабель питания компьютера из розетки во время работы. Это приводит к тому, что ФС может находиться в не консистентном состоянии (с нарушенными внутренними связями).

Так как модуль запускается раньше автоматической проверки диска, ему приходится в таком случае работать с ФС, которая может содержать ошибки. Если включено лечение, то при лечении происходит перезапись данных в ФС, и есть риск повредить данные, не относящиеся к данным, подлежащим лечению. Например, возможно записать данные в сектор, помеченный как пустой, хотя на самом деле содержащий критически важные данные. Если администратор не готов к такому риску, то рекомендуется отключить эту опцию.

2.10.8. Работа с дампами и журналами подсистемы проверки

Сохранение дампов и журналов подсистемы проверки необходимо для выявления и устранения ошибок в работе программы. Сохранение данных может быть выполнено на любой диск, в том числе на подключенный съемный диск (например, флэш-накопитель).

Файл журнала сохраняется в формате *txt*. Файл может содержать имена файлов или папок пользователя. Имя файла формируется автоматически и включает дату и время создания файла. Имя файла имеет вид *kl_log.YYYY_MM_DD.hh_mm_ss.txt*, где *DD* – день, *MM* – месяц, *YYYY* – год, *hh* – час, *mm* – минута, *ss* – секунда. Файл сохраняется в кодировке UTF-8.

Файл дампа сохраняется в формате *bin*. Файл содержит информацию о физической памяти, загруженных драйверах, компонентах антивирусных баз и копию фрагментов физической памяти, необходимых для идентификации места в программе, повлекшего сбой. Имя файла формируется автоматически и включает дату и время создания файла. Имя файла имеет вид *kl_dump.YYYY_MM_DD.hh_mm_ss.bin*, где *DD* – день, *MM* – месяц, *YYYY* – год, *hh* – час, *mm* – минута, *ss* – секунда.

Примечания:

1. По умолчанию сохранение дампов и журналов отключено, включить сохранение можно на странице настройки модуля *Антивируса Касперского для UEFI* (см. рис. 162).
2. Значение параметра будет применено после выхода из оболочки KSS и перезагрузки ОС.

3. Если вы активировали сохранение дампов и журналов после включения или перезагрузки ОС, модуль предложит выбрать диск для сохранения данных. Если вы отмените сохранение дампов и журналов на диск, антивирусная проверка будет продолжена без сохранения данных.

4. Если выполнить сохранение дампов и журналов подсистемы проверки не удалось, модуль отобразит сообщение об ошибке.

5. Если сохранение дампов и журналов подсистемы включено, то при возникновении сбоя или ошибки после перезагрузки модуль отобразит окно выбора устройства для сохранения данных.

6. Если сохранение дампов и журналов подсистемы проверки выключено, то при возникновении сбоя в работе модуля данные сохранены не будут. Для просмотра журнала следует:

– запустить компьютер под учетной записью *Администратора*;

– по окончании антивирусной проверки нажать [F10], откроется меню *Администратора*;

– выбрать п. *Журнал Подсистемы проверки,* откроется журнал подсистемы проверки.

Для просмотра журнала вы также можете открыть файл журнала подсистемы проверки, находящийся в ФС одного из дисков (если сохранение журналов подсистемы проверки включено).

2.11. Сообщения администратору

Сообщения – это текстовая информация (записи), выводимые на страницах или в окнах в процессе работы с ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Основная часть сообщений, выводимых на экран, представлена в соответствующих разделах данного руководства. В данном разделе приводятся дополнительные сообщения ПК «ЭЗ «ВИТЯЗЬ» 2.2, которые не были описаны и требуют отдельного рассмотрения. Также приводятся действия администратора, которые ему следует выполнить, при выводе сообщений. Дополнительные сообщения приводятся ниже по тексту при описании различного рода ситуаций, с которыми администратор может столкнуться при работе с ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2.11.1. Отображение информации о нарушении целостности оборудования

Пример ситуации: выход из строя планки оперативной памяти системного блока.

Отображение информации, сгенерированной модулем *Контроль целостности оборудования* на различных страницах и окнах KSS при наступлении одного и того же события – нарушении целостности оборудования. Отчет модуля *Контроль целостности оборудования* приведен на рис. 147.

Ошибка устройства: Устройство не найдено: Оперативная память

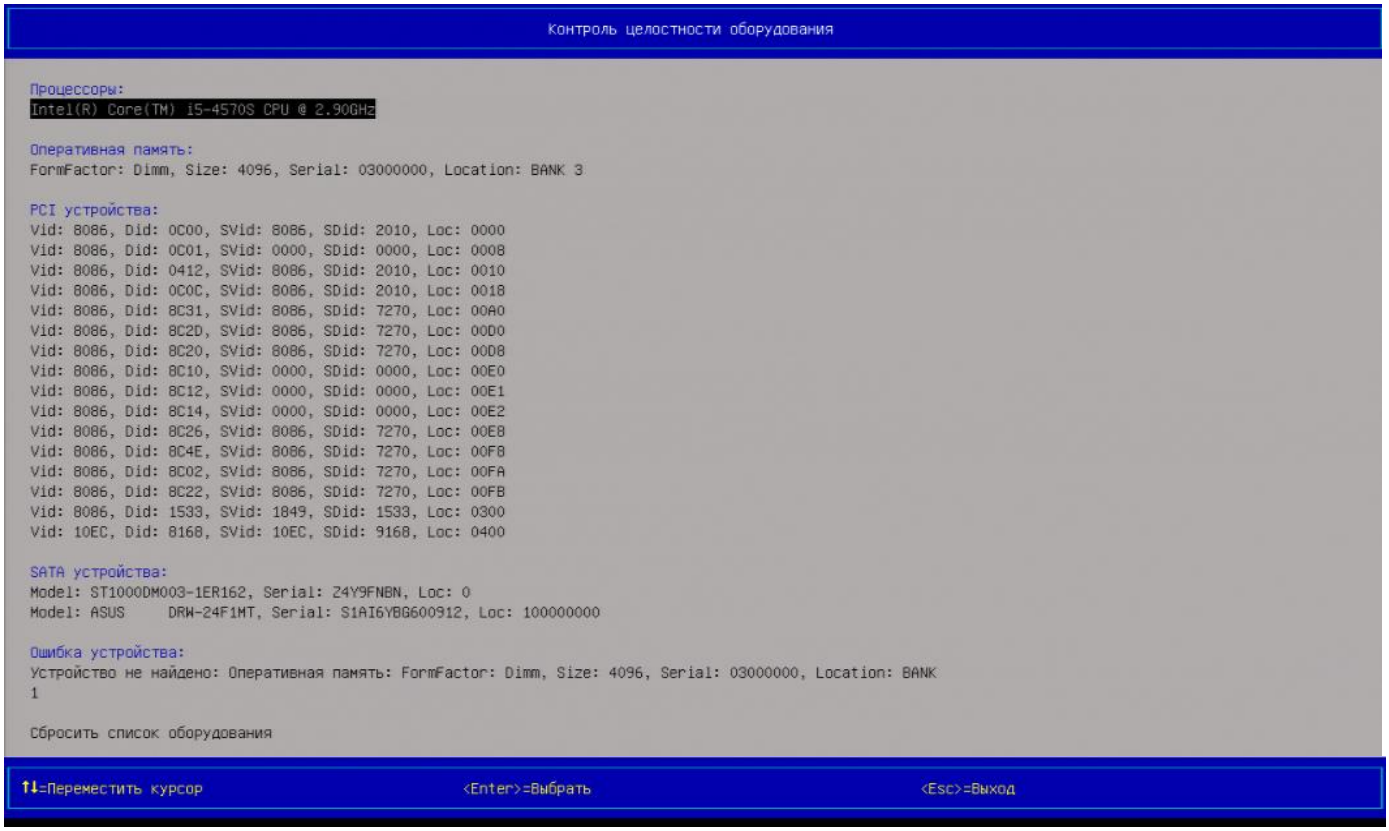

Рис. 147

Содержание журнала событий для примера нарушения целостности ФС приведено на рис. 148.

Нарушена целостность ФС

Рис. 148

2.11.2. Сообщения о различных ситуациях

Ситуация № 1. При отрицательном результате процедуры КЦ, на экран выводятся записи (рис. 149).

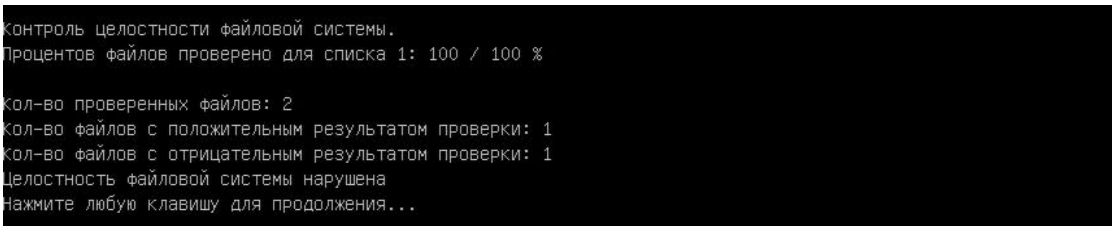

Рис. 149

Решение:

1) либо обновить КС файлов, которые прошли процедуру КЦ с отрицательным результатом;

2) либо удалить эти файлы из списка файлов (данное действие выполняется в том случае, если отрицательный результат КЦ определенных файлов не является критичным).

Также администратору следует просмотреть журнал событий ПК «ЭЗ «ВИТЯЗЬ» 2.2 и проанализировать данные, хранящиеся в нем, для нахождения причины нарушения целостности файлов.

Ситуация № 2. При отрицательном результате процедуры КЦ, и когда ПК «ЭЗ «ВИТЯЗЬ» 2.2 включен, на экран выводятся записи следующего вида:

```
Ограничение доступа:
Нарушена целостность файловой системы.
Доступ разрешен только администратору

Поиск электронного ключа
Подключите электронный ключ
```

Решение: пройти процедуру аутентификации, далее выполнить действия, приведенные для ситуации № 1.

Ситуация № 3. Если текущий пароль пользователя был введен неправильно во время его аутентификации, то отображается окно (рис. 150), информирующее о том, что был введен неверный пароль.

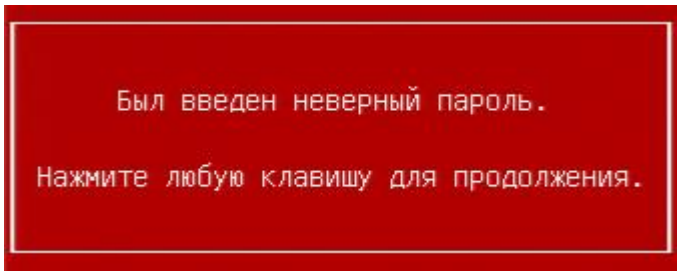

Рис. 150

Решение: нажать любую клавишу на клавиатуре и 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 ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Ситуация № 4. Если количество неправильно введенного пароля пользователя во время его аутентификации равно значению параметра *Максимальное количество попыток ввода пароля* (см. п. 2.2.2), то после нажатия на клавишу [Enter] отображается окно (рис. 151), сообщающее о превышении количества попыток ввода пароля. После повторного нажатия на клавишу [Enter] отображается окно (см. рис. 150), сообщающее о том, что был введен неверный пароль, а после третьего нажатия на клавишу [Enter] – окно (рис. 152), сообщающее о попытке входа заблокированного пользователя.

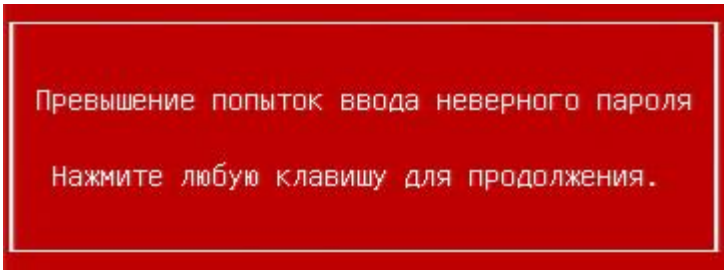

Рис. 151

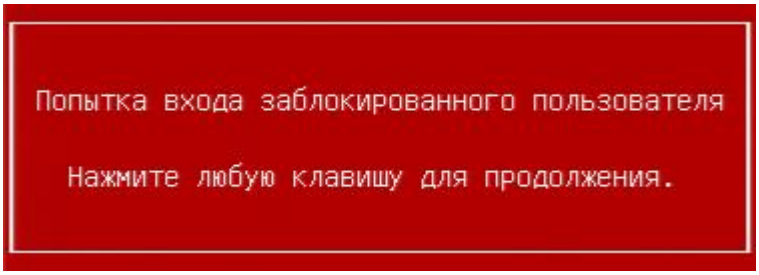

Рис. 152

Решение:

1) отключить от USB-порта АН пользователя, профиль которого был заблокирован;

2) пройти процедуру аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 с помощью АН администратора;

3) войти в оболочку KSS и разблокировать профиль пользователя, профиль которого был заблокирован.

Ситуация № 5. Если после включения компьютера, во время процедуры аутентификации, подключить АН пользователя, профиль которого ранее был заблокирован ПК «ЭЗ «ВИТЯЗЬ» 2.2, то на экран будет выведено окно (рис. 152), информирующее о попытке входа заблокированного пользователя.

Решение:

1) отключить АН пользователя от USB-порта, профиль которого был заблокирован;

2) пройти процедуру аутентификации в ПК «ЭЗ «ВИТЯЗЬ» 2.2 с помощью АН администратора;

3) войти в оболочку KSS и разблокировать профиль пользователя, профиль которого был заблокирован.

Ситуация № 6. На экран выводится запись вида:

ОШИБКА! Превышено количество попыток входа.
Нажмите любую клавишу для перезагрузки

При следующих условиях:

1) если во время прохождения пользователем процедуры аутентификации было превышено максимальное количество попыток аутентификации, т.е. количество подключений АН пользователя к USB-порту, заданное администратором ранее в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. документ 643.18184162.00006-02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2);

2) если во время прохождения пользователем процедуры аутентификации количество попыток ввода пароля превысило максимальное количество попыток аутентификации, которое было задано администратором ранее в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2, т.е. если после вывода окна (рис. 203) пользователем было выполнено последовательное нажатие на клавишу [Enter] такое количество раз, которое привело к превышению максимального количества попыток аутентификации.

Решение:

1) отключить от USB-порта АН пользователя, профиль которого был заблокирован,

2) нажать любую клавишу клавиатуры,

3) пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 с помощью АН администратора,

4) войти в оболочку KSS и разблокировать профиль пользователя, который был заблокирован.

Ситуация № 7. Если при прохождении процедуры аутентификации подключить АН пользователя, незарегистрированный в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2, к USB-порту, то на экран будет выведено окно (рис. 153), информирующее о попытке использования незарегистрированного ключа.

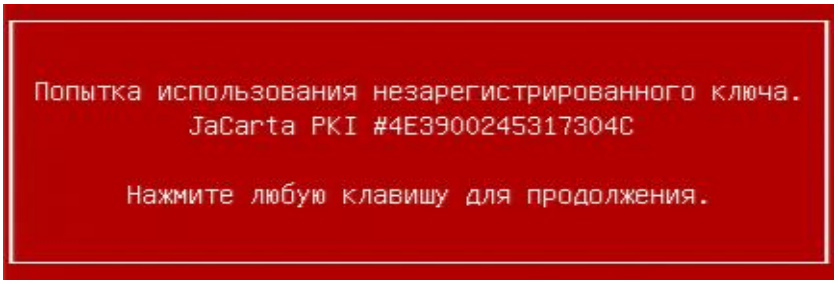

Рис. 153

Примечание. Окно (см. рис. 153) выводится на экран только, если пользователь проходит процедуру аутентификации при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Возможные решения:

1) отключить от USB-порта АН пользователя, который не был ранее зарегистрирован в ПК «ЭЗ «ВИТЯЗЬ» 2.2, и подключить АН пользователя, зарегистрированный в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2;

2) отключить от USB-порта АН пользователя, который не был ранее зарегистрирован в ПК «ЭЗ «ВИТЯЗЬ» 2.2, подключить АН администратора к USB-порту, пройти процедуру аутентификации, войти в оболочку KSS, создать профиль нового пользователя с применением АН, с помощью которого аутентификация пользователя ранее была невозможна.

Ситуация № 8. Если во время прохождения процедуры аутентификации пользователем было выбрано значение ключевого поля на странице *Локальная аутентификация* (см. п. 2.1.3), которое отсутствует в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2, то после нажатия на клавишу [Enter] на экран будет выведено окно (рис. 154), информирующее о том, что пользователь, проходящий в данный момент процедуру аутентификации, не зарегистрирован для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

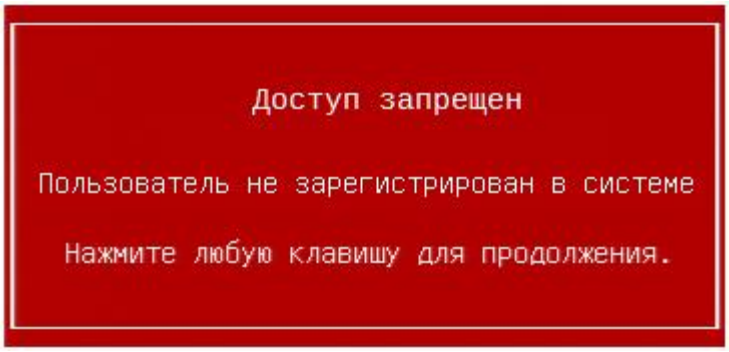

Рис. 154

Примечание. Окно (см. рис. 154) выводится на экран только, если пользователь проходит процедуру аутентификации при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», «Электронный ключ и Цифровой сертификат».

Решение:

1) нажать любую клавишу клавиатуры,

2) отключить АН пользователя от USB-порта,

3) подключить АН администратора к USB-порту,

4) пройти процедуру аутентификации и войти в оболочку KSS,

5) создать профиль нового пользователя с применением АН, с помощью которого ранее была невозможна аутентификация пользователя.

Примечание. Так как в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2 параметру Способ аутентификации было присвоено значение «Цифровой сертификат», то перед созданием профиля нового пользователя администратору следует проверить наличие сертификата пользователя в АН.

Ситуация № 9. Если во время прохождения процедуры аутентификации не были найдены сертификаты пользователя на АН, на странице *Локальная аутентификация* выводится запись следующего вида (рис. 155).

Рис. 155

Примечание. Окно (рис. 155) выводится на экран только, если пользователь проходит процедуру аутентификации при следующих настройках: Электронный замок «Витязь» – «Вкл», Способ аутентификации – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: записать сертификат пользователя на АН.

Ситуация № 10. Если во время прохождения пользователем процедуры аутентификации результат проверки сертификата пользователя на подлинность отрицательный (см. п. 3.1.4), то отображается окно (рис. 156), информирующее об ошибке идентификации.

Рис. 156

Примечание. Окно (см. рис. 156) выводится на экран только, если пользователь проходит процедуру аутентификации при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Возможные решения:

1) записать сертификат пользователя на АН, который был подписан с помощью сертификата УЦ, добавленного ранее в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2) администратору следует пройти процедуру аутентификации, войти в оболочку KSS, добавить к имеющемуся списку сертификатов УЦ новый сертификат УЦ, с помощью которого был подписан сертификат пользователя.

3) обратиться в АО «Крафтвэй корпорэйшн ПЛС, т.к. дальнейшая аутентификация для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 невозможна (см. предупреждение в п. 2.4.3).

Ситуация № 11. Если модуль *Электронный замок «Витязь»* выключен, то операции, выполняемые в нем, недоступны для администратора, т.е. после выбора п. *Электронный замок «Витязь»* раздела *Модули безопасности* главного меню KSS (рис. 2) и нажатия клавиши [Enter] отображается страница *Электронный замок «Витязь»* с записью (рис. 157).

Страница *Электронный замок «Витязь»*,

пункты для выполнения операций отсутствуют

Рис. 157

Решение: включить модуль *Электронный замок «Витязь»* (см. документ 643.18184162.00006- 02 90 «Руководство администратора», раздел 5. Рекомендации по безопасной установке и настройке ПК «ЭЗ «ВИТЯЗЬ» 2.2).

Ситуация № 12. Если модуль *Контроль целостности файловой системы* выключен, то операции, выполняемые в нем, недоступны для администратора, т.е. после выбора п. *Контроль целостности файловой системы* раздела *Модули безопасности* главного меню KSS (рис. 2) и нажатия клавиши [Enter] отображается страница *Контроль целостности файловой системы* с записью (рис. 158).

Страница Контроль целостности файловой системы (вид 3),

пункты для выполнения операций отсутствуют

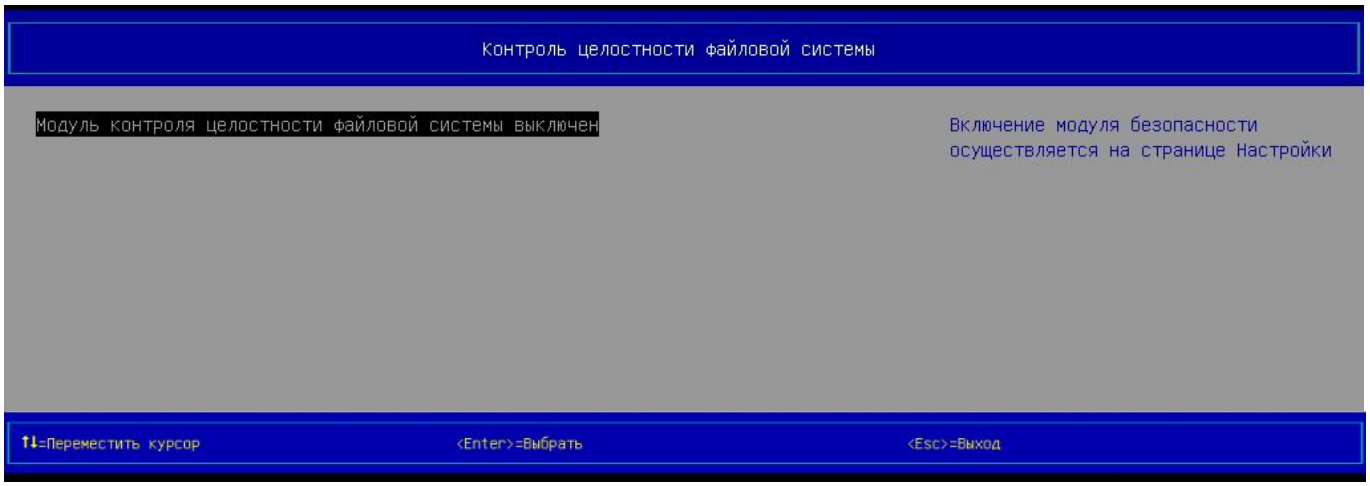

Рис. 158

Решение: включить модуль *Контроль целостности файловой системы* (см. подраздел 2.5).

Ситуация № 13. Если модуль безопасности *Управление сертификатами* выключен, то операции, выполняемые в нем, недоступны для администратора, т.е. после выбора п. *Управление сертификатами* раздела *Модули безопасности* главного меню KSS (рис. 2) и нажатия клавиши [Enter] отображается страница *Управление сертификатами* с записью (рис. 159).

Страница *Управление сертификатами*,

пункты для выполнения операций отсутствуют

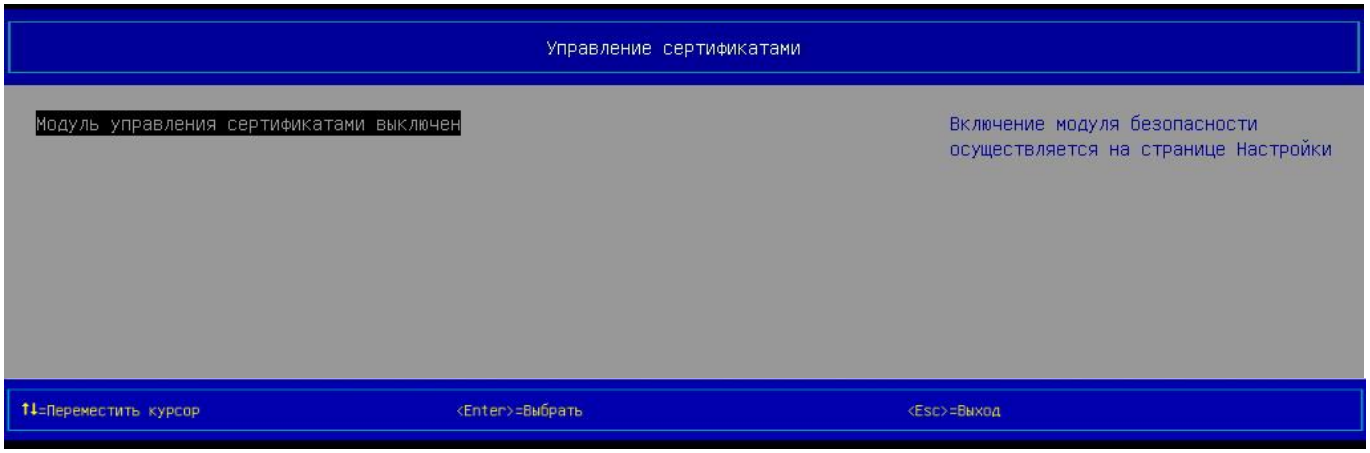

Рис. 159

Решение: включить модуль *Управление сертификатами* (см. подраздел 2.4).

Ситуация № 14. Если при создании профиля нового пользователя с применением его АН попытаться создать данный профиль, не подключив АН пользователя и нажав на клавишу [Enter] после соответствующего запроса (рис. 7), то отображается окно (рис. 160), информирующее о том, что АН не найден.

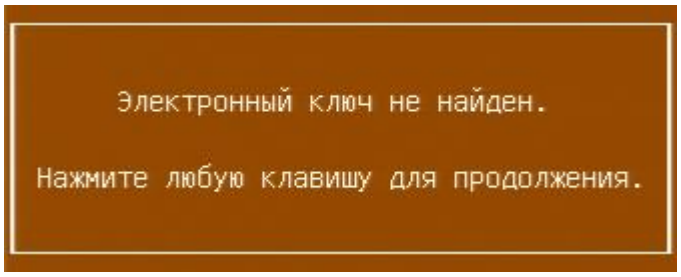

Рис. 160

Решение:

1) нажать любую клавишу на клавиатуре,

2) повторить процедуру создания профиля нового пользователя,

3) подключить АН пользователя при соответствующем запросе (рис. 7),

4) закончить создание профиля нового пользователя.

Ситуация № 15. Если при создании профиля нового пользователя с применением его АН поле окна для ввода пароля (рис. 9) оставить пустым или ввести пароль неправильно, то после нажатия клавиши [Enter] на экран будет выведено окно (рис. 161), информирующее о том, что был введен неверный пароль.

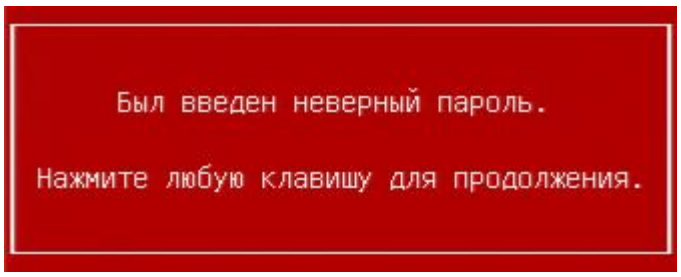

Рис. 161

Решение: нажать любую клавишу на клавиатуре, и повторить процедуру создания профиля нового пользователя.

Ситуация № 16. Если при создании профиля нового пользователя с применением его АН после вывода на экран окна для ввода пароля пользователя (рис. 9) нажать клавишу [Esc], то на экран будет выведено окно (рис. 162), информирующее о том, что операция прервана.

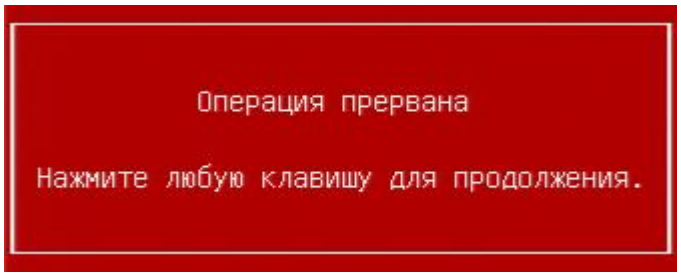

Рис. 162

Решение: нажать любую клавишу на клавиатуре, и повторить процедуру создания профиля нового пользователя при необходимости.

Ситуация № 17. Если при создании профиля нового пользователя с применением АН попытаться создать данный профиль, подключив АН, которое ранее использовалось при создании профиля другого пользователя, и нажав на клавишу [Enter] после соответствующего запроса (рис. 9), то в этом случае отображается окно (рис. 163), информирующее о том, что АН был зарегистрирован ранее в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

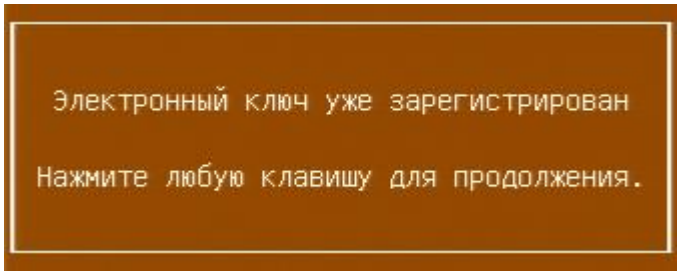

Рис. 163

Примечание. Окно (см. рис. 163) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Решение: нажать любую клавишу на клавиатуре и повторить создание профиля нового пользователя с применением АН, которое было инициализировано (отформатировано) специально для данного пользователя.

Ситуация № 18. Если при создании профиля нового пользователя с применением АН попытаться создать профиль, подключив АН, на котором отсутствует сертификат пользователя, то после выполнения поиска сертификатов на АН отображается окно (рис. 164), сообщающее о том, что сертификат недоступен.

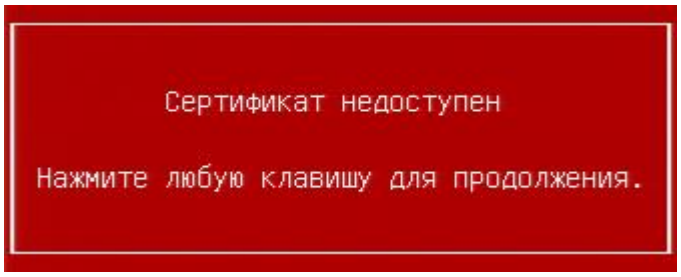

Рис. 164

Примечание. Окно (см. рис. 164) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках: *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Возможные решения:

1) нажать любую клавишу на клавиатуре, и повторить создание профиля нового пользователя с применением АН, на котором размещен сертификат пользователя, специально созданный для данного пользователя;

2) нажать любую клавишу на клавиатуре. Сгенерировать сертификат для пользователя, для которого ранее нельзя было создать профиль пользователя в ПК «ЭЗ «ВИТЯЗЬ» 2.2, сохранить этот сертификат пользователя на АН пользователя, повторить создание профиля нового пользователя с применением данного АН.

Ситуация № 19. 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 (рис. 208), информирующее о том, что АН не был подключен, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (рис. 209), информирующее о том, что произошла ошибка при смене пароля.

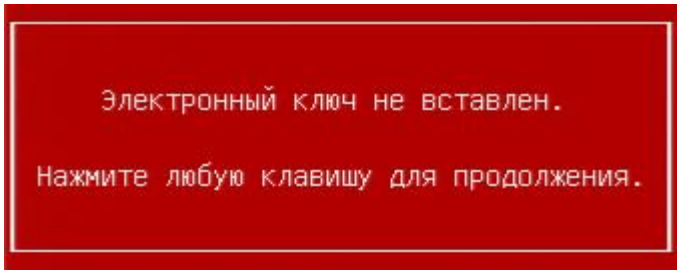

Рис. 165

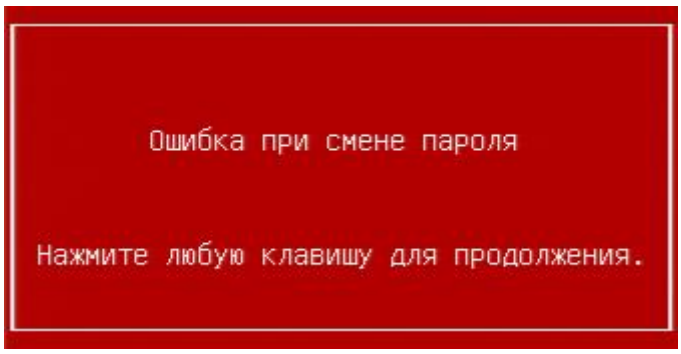

Рис. 166

Решение: нажать любую клавишу клавиатуры, далее подключить АН пользователя, пароль которого подлежит изменению, повторить процедуру изменения пароля.

Ситуация № 20. Если текущий пароль пользователя был введен неправильно во время изменения пароля пользователя, то отображается окно (рис. 167), информирующее о том, что пароль был введен неправильно, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рис. 209), информирующее о том, что произошла ошибка при смене пароля.

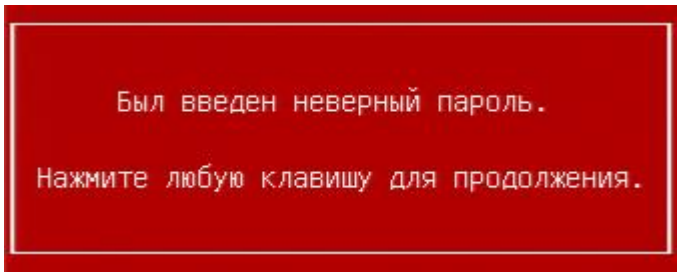

Рис. 167

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

Ситуация № 21. Если новый пароль пользователя был введен неправильно во время изменения пароля, то отображается окно (рис. 211), информирующее о несовпадении паролей, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рис. 209), информирующее о том, что произошла ошибка при смене пароля.

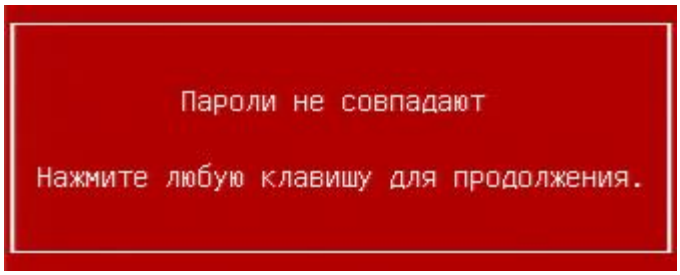

Рис. 168

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

Ситуация № 22. Если при добавлении списка файлов, подлежащих КЦ, поле в окне для ввода названия списка файлов (рис. 87) оставить пустым и нажать клавишу [Enter], на экран будет выведено окно (рис. 169), информирующее о том, что были введены неверные данные.

Рис. 169

Решение: ввести верные данные в поле ввода названия списка файлов.

Ситуация № 23. Если при добавлении списка файлов, подлежащих КЦ, ввести название списка файлов с использованием специальных символов в соответствующем окне (рис. 87) и нажать клавишу [Enter], то на экран будет выведено окно (рис. 170), информирующее о том, что название списка файлов содержит недопустимые символы.

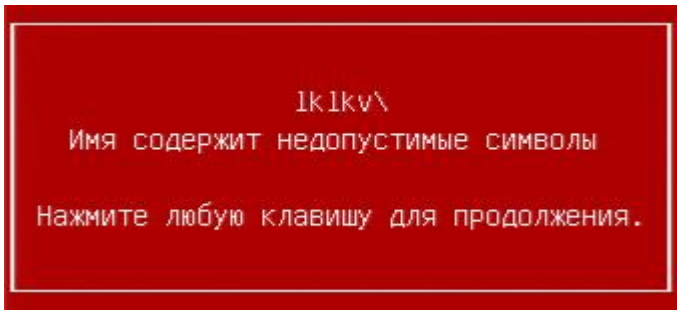

Рис. 170

Решение: повторно выполнить добавление списка файлов, подлежащих КЦ.

Примечание. Выполняя данную операцию, при присвоении названия списку файлов, администратору разрешено использовать только строчные или прописные буквы латинского алфавита (a-z, A-Z) и любые цифры (0-9).

Ситуация № 24. Если при добавлении нового списка файлов, подлежащих КЦ, ввести название, которое было присвоено ранее уже добавленному списку файлов в соответствующем окне (рис. 87) и нажать клавишу [Enter], то на экран будет выведено окно (рис. 171), состоящее из записей (рис. 171), сообщающее о том, что введенное название списка файлов уже присвоено добавленному списку.

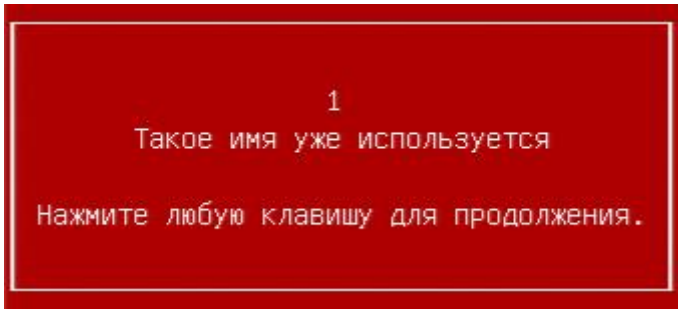

Рис. 171

Решение: повторно выполнить добавление нового списка файлов, подлежащих КЦ.

Примечание. Выполняя данную операцию, при присвоении названия новому списку файлов, администратору следует ввести название, отличное от названий списков файлов, которые ранее были добавлены в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Ситуация № 25. При попытке сохранить список файлов, подлежащих КЦ, которому не было присвоено название, отображается окно (рис. 172), информирующее о том, что список файлов невозможно сохранить по причине отсутствия названия у сохраняемого списка файлов.

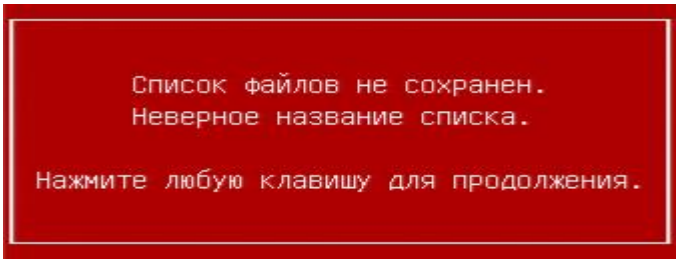

Рис. 172

Решение: для сохранения списка файлов, подлежащих КЦ, присвоить название добавляемому списку файлов.

Ситуация № 26. При попытке добавления сертификата УЦ, который ранее был добавлен в ПК «ЭЗ «ВИТЯЗЬ» 2.2, отображается окно (рис. 173), информирующее о наличии данного сертификата УЦ в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

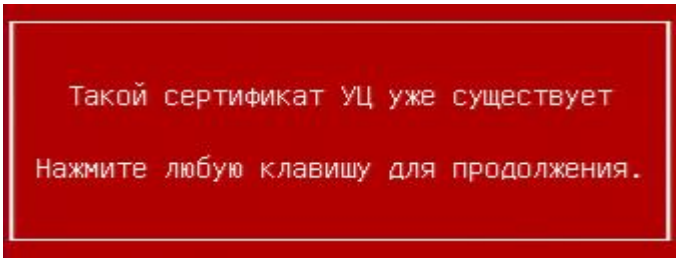

Рис. 173

Решение: добавить другой сертификат УЦ при необходимости.

Ситуация № 27. Если во время добавления сертификата компьютера в ПК «ЭЗ «ВИТЯЗЬ» 2.2 на странице *Файловый менеджер* (п. 2.4.6) ввести неправильно пароль для сертификата компьютера в соответствующем окне (см. рис. 20), то после нажатия на клавишу [Enter] отображается окно (рис. 174), информирующее о том, что не удалось импортировать сертификат компьютера.

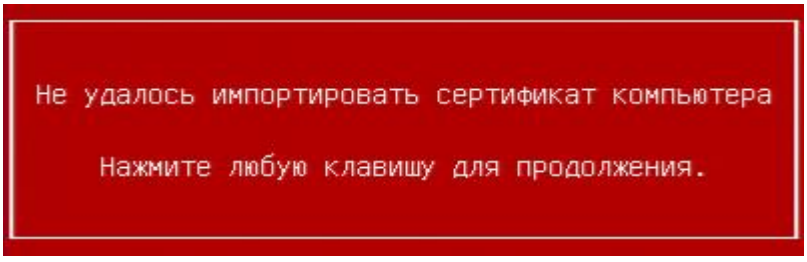

Рис. 174

Решение: повторно выполнить добавление сертификата компьютера.

2.11.3. Отображение информации о событии обнаружения вируса

Если во время проверки компьютера на наличие вирусов антивирусным модулем будет обнаружено заражение, то отображается сообщение (рис. 175).

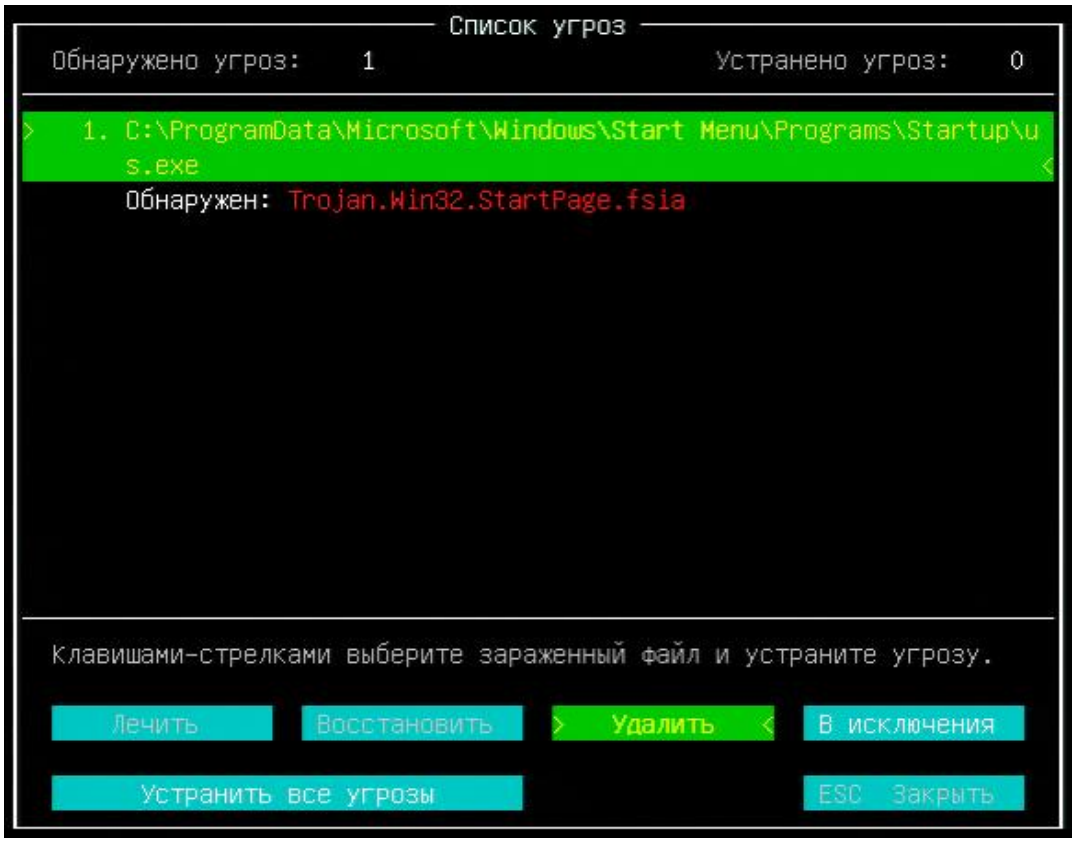

Рис. 175

Решение: При получении пользователем сигнала тревоги об обнаружении вируса администратором должны быть выполнены следующие мероприятия:

1) изолировать компьютер от локальной сети и доступа в Интернет;

2) выполнить вход на компьютер с правами администратора;

3) отменить запрет загрузки ОС с внешних носителей;

4) загрузить ОС с доверенного внешнего носителя в режиме «только чтение»;

5) выполнить процедуру удаления, лечения или восстановления зараженных файлов;

6) установить запрет загрузки компьютера с внешних носителей;

7) подключить компьютер к локальной сети.

3. РАБОТА ПОЛЬЗОВАТЕЛЯ С РОЛЬЮ «ПОЛЬЗОВАТЕЛЬ» С ПК «ЭЗ «ВИТЯЗЬ» 2.2

3.1. Аутентификация пользователя в ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для загрузки ОС необходимо пройти аутентификацию в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

В ПК «ЭЗ «ВИТЯЗЬ» 2.2 реализовано три способа аутентификации:

1) по электронному ключу;

2) по цифровому сертификату;

3) по цифровому сертификату и электронному ключу.

Аутентификация пользователя проводится путем предъявления АН на этапе загрузки ОС.

Одному пользователю соответствует один АН.

При выборе одного из следующих способов аутентификации – по электронному ключу, а также по цифровому сертификату и электронному ключу – выполняется проверка наличия серийного номера АН в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся серийные номера АН, зарегистрированные ранее. Занесение серийного номера АН в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2 выполняется администратором на этапе создания профиля нового пользователя.

При выборе способа аутентификации только по цифровому сертификату данная проверка не выполняется.

Для всех способов имеется три варианта:

1) по PIN-коду к АН;

2) по ключевому полю цифрового сертификата пользователя;

3) по PIN-коду к АН и ключевому полю цифрового сертификата пользователя.

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.

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 ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы администратором профили пользователей в ПК «ЭЗ «ВИТЯЗЬ» 2.2. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

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 ПК «ЭЗ «ВИТЯЗЬ» 2.2, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых

ранее были созданы администратором профили пользователей в ПК «ЭЗ «ВИТЯЗЬ» 2.2. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

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

3.1.1. Аутентификация пользователя, вариант 1

Аутентификация пользователя при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2:

1) модуль *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ»,

2) модуль *Контроль целостности файловой системы* – «Вкл», создан контрольный список файлов для КЦ.

Для прохождения аутентификации:

1) включить компьютер, на экране отображаются Logo-изображение материнской платы (рис. 18) и далее процедура КЦ списка файлов соответствующим модулем (рис. 176);

Процедура КЦ списка файлов

```
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
```

Рис. 176

Примечания:

1. Процесс КЦ выполняется, если администратором предварительно включены следующие модули безопасности – *Контроль целостности файловой системы* и *Контроль целостности оборудования*.

2. Во время выполнения процедуры КЦ отображается информация о ходе проверки и итоговая информация с результатами проверки.

3. Результат может быть, как с положительным, так и с отрицательным результатом. В случае отрицательного результата дальнейшие действия пользователя будут заблокированы. При появлении любой информации о нарушении КЦ следует обратиться к администратору.

2) по окончании КЦ объектов пользователю предлагается подключить АН к USB-порту (рис. 8);

3) подключить АН к USB-порту;

4) после аутентификации пользователя по АН появится окно для ввода пароля (рис. 177);

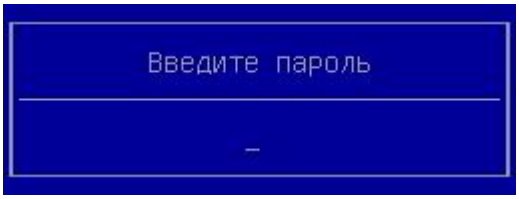

Рис. 177

5) ввести пароль (время на ввод пароля ограничено настройками ПК «ЭЗ «ВИТЯЗЬ» 2.2);

6) нажать клавишу [Enter];

7) в случае успешной аутентификации откроется окно для выбора дальнейших действий пользователя, предлагающее (рис. 178) дождаться загрузки ОС или нажать клавишу [F1] для входа в оболочку KSS.

Окно выбора загрузки ОС / входа в оболочку KSS

Рис. 178

Примечание. Время задержки по входу в оболочку KSS задано в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2.

3.1.2. Аутентификация пользователя, вариант 2

Аутентификация пользователя при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2:

1) модуль *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Цифровой сертификат»;

2) *Ключевое поле* – «Общее имя (CN)», модуль *Контроль целостности файловой системы* – «Вкл»;

3) создан контрольный список файлов, подлежащих КЦ.

Для прохождения аутентификации:

1) включить компьютер, на экране отображаются Logo-изображение материнской платы (см. рис. 18) и далее процедура КЦ списка файлов соответствующим модулем (см. рис. 176);

2) после окончания КЦ объектов предлагается подключить АН к USB-порту (см. рис. 8);

3) подключить АН к USB-порту;

4) после аутентификации пользователя по АН предлагается ввести пароль (см. рис. 177);

5) ввести пароль;

6) нажать клавишу [Enter], осуществляется поиск сертификатов пользователей, расположенных на АН, во время которого отображается окно (рис. 179);

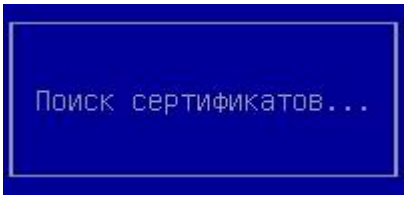

Рис. 179

7) после завершения поиска сертификатов пользователю предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов на странице *Локальная аутентификация* (рис. 180);

Страница *Локальная аутентификация* (вид 2),

выбор значения ключевого поля *Общее имя (CN)* сертификатов пользователя

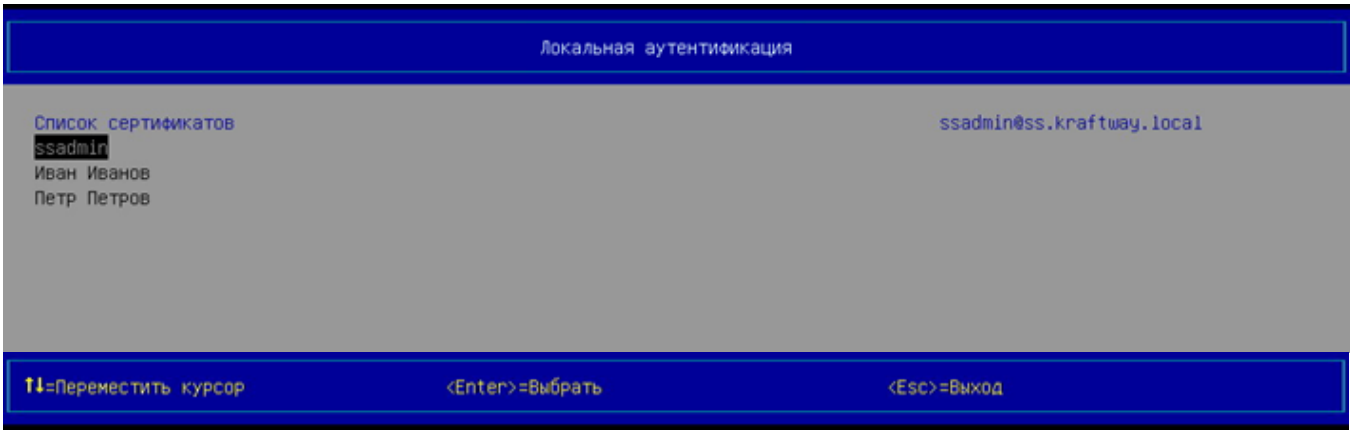

Рис. 180

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

9) нажать клавишу [Enter], после успешной аутентификации предлагается дождаться загрузки ОС или войти в оболочку KSS (рис. 178).

Примечания:

1. Если для пользователя задан *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)» – после завершения поиска сертификатов пользователю предлагается выбрать универсальное имя из списка (рис. 24).

2. Если для пользователя задан *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата» – после завершения поиска сертификатов пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (рис. 181).

Страница *Локальная аутентификация* (вид 4),

выбор серийного номера сертификата

Рис. 181

3.1.3. Аутентификация пользователя, вариант 3

Аутентификация пользователя при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2:

1) модуль *Электронный замок «Витязь»* – «Вкл»;

2) *Способ аутентификации* – «Цифровой сертификат и электронный ключ»;

3) *Ключевое поле* – «Общее имя (CN)»;

4) модуль *Контроль целостности файловой системы* – «Вкл»;

5) создан контрольный список файлов для КЦ.

Для прохождения аутентификации выполните действия, описанные в п. 3.1.2.

Примечания:

1. Если для пользователя задан *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Универсальное имя (UPN)» – после завершения поиска сертификатов пользователю предлагается выбрать универсальное имя из списка (см. рис. 24).

2. Если для пользователя задан *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Серийный номер сертификата» – после завершения поиска сертификатов пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. рис. 17).

3.1.4. Дополнительные сведения о процедуре аутентификации

Если ранее аутентификация пользователя выполнялась 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, пользователь не сможет пройти процедуру аутентификации с положительным результатом. Если результат проверки на подлинность положительный, пользователю предлагается дождаться загрузки ОС или войти в оболочку KSS (см. рис. 178).

3.2. Действия пользователя

Пользователь имеет возможность выполнить следующие действия:

1) изменение пароля пользователя;

2) вывод детальной информации о пользователе (профиль);

3) загрузку штатной ОС компьютера.

Для выбора действий пользователя:

1) пройти процедуру аутентификации (см. подраздел 3.1);

2) нажать клавишу [F1], отображается страница *Kraftway Secure Shell* (рис. 2).

3.2.1. Изменение пароля пользователя

Для изменения пароля пользователя:

1) выбрать п. *Электронный замок «Витязь»* раздела *Модули безопасности* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (рис. 182);

Страница *Электронный замок «Витязь»* (вид 1)

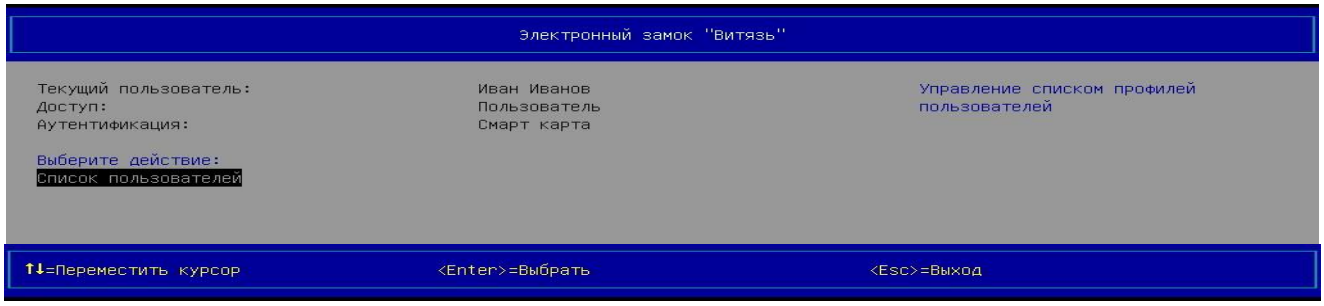

Рис. 182

3) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: список пользователей* (рис. 183 - 186), на которой представлен единственный профиль пользователя, который только что прошел процедуру аутентификации и выполнил вход в оболочку KSS;

Страница *Электронный замок «Витязь»: список пользователей* (вид 1),

профиль пользователя, *Способ аутентификации* – «Электронный ключ»

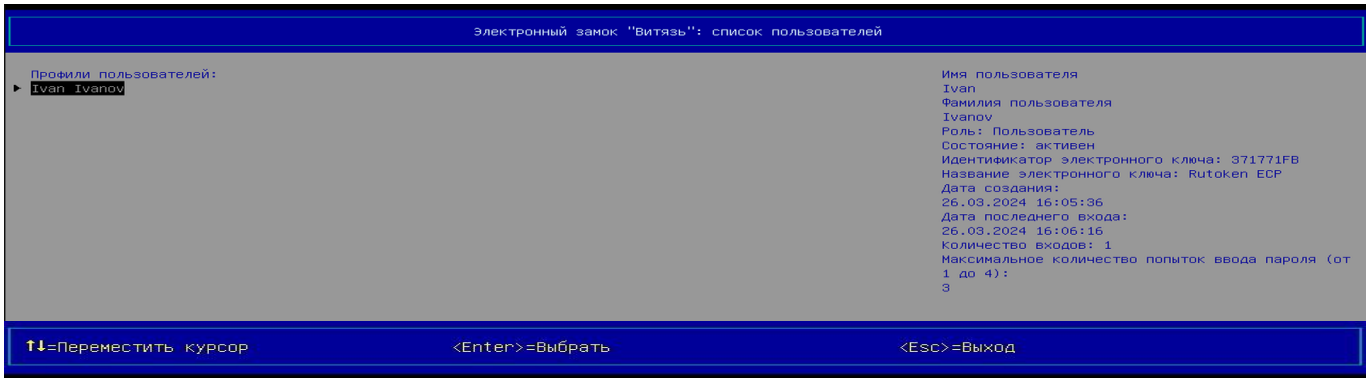

Рис. 183

Страница *Электронный замок «Витязь»: список пользователей* (вид 2),

профиль пользователя, *Способ аутентификации* – «Цифровой сертификат»,

Ключевое поле – «Общее имя (CN)»

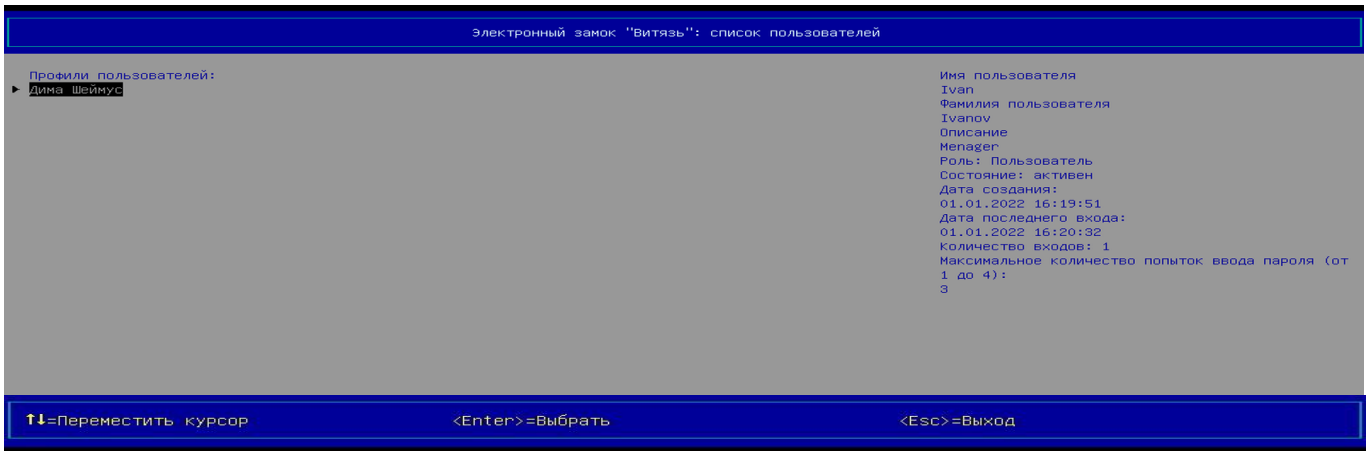

Рис. 184

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

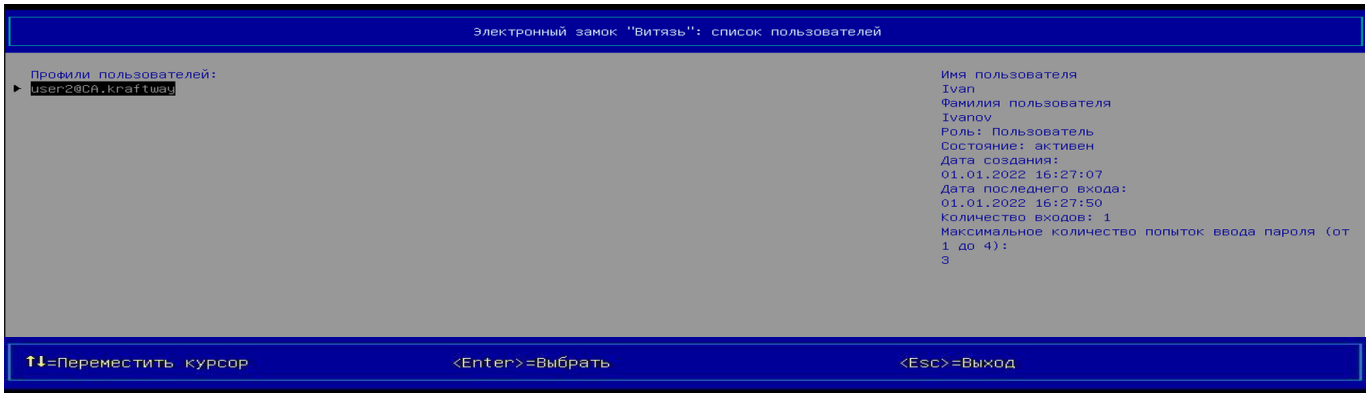

Рис. 185

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

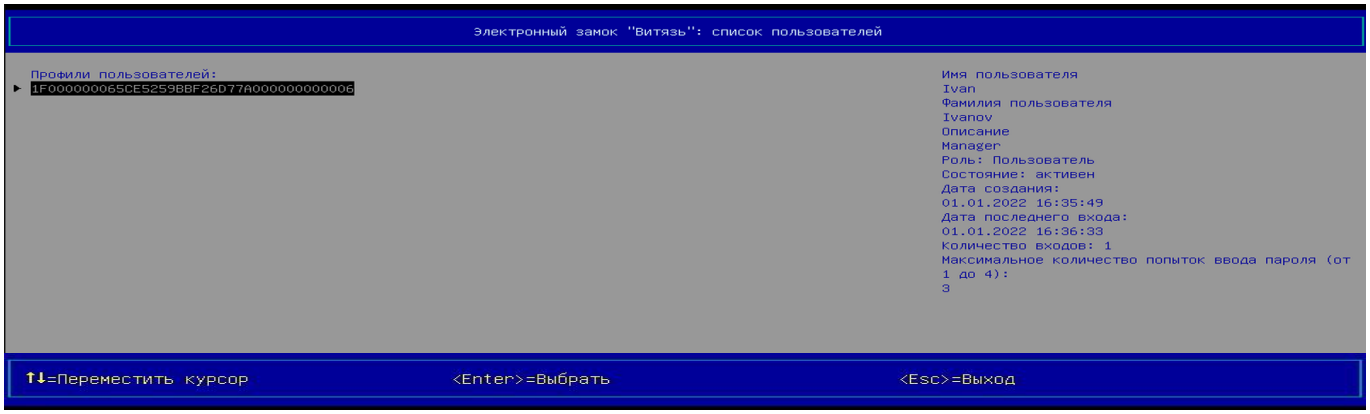

Рис. 186

4) нажать клавишу [Enter], отображается окно (рис. 187) для выбора действия, которое необходимо выполнить над профилем пользователя;

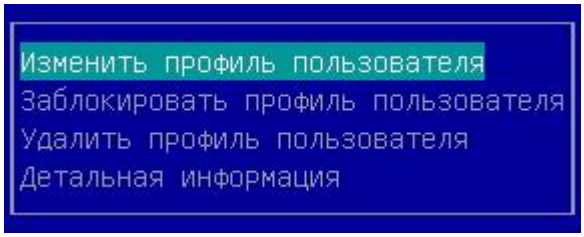

Рис. 187

5) выбрать п. *Изменить профиль пользователя* в окне (см. рис. 187);

6) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: изменение профиля пользователя* (рис. 188 - 190);

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

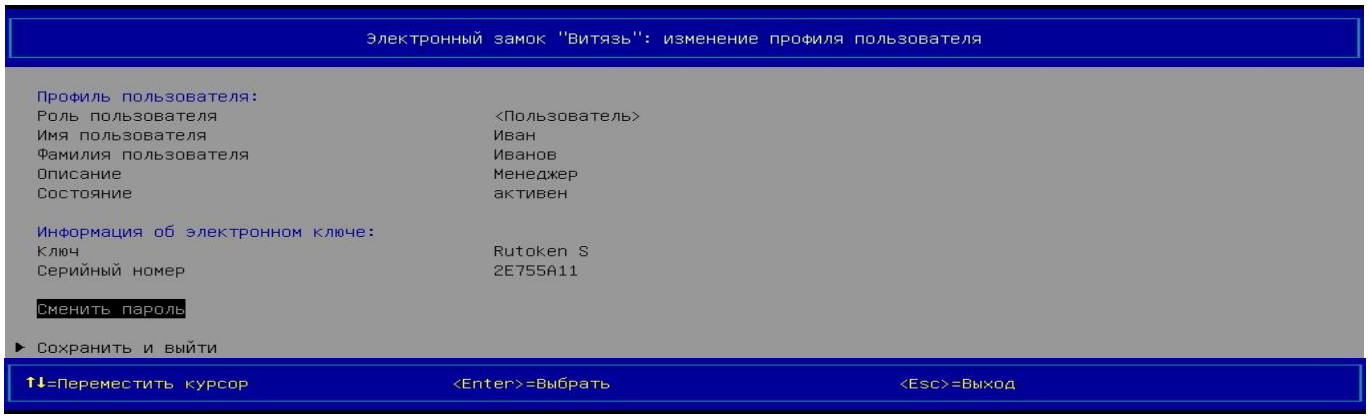

Рис. 188

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»

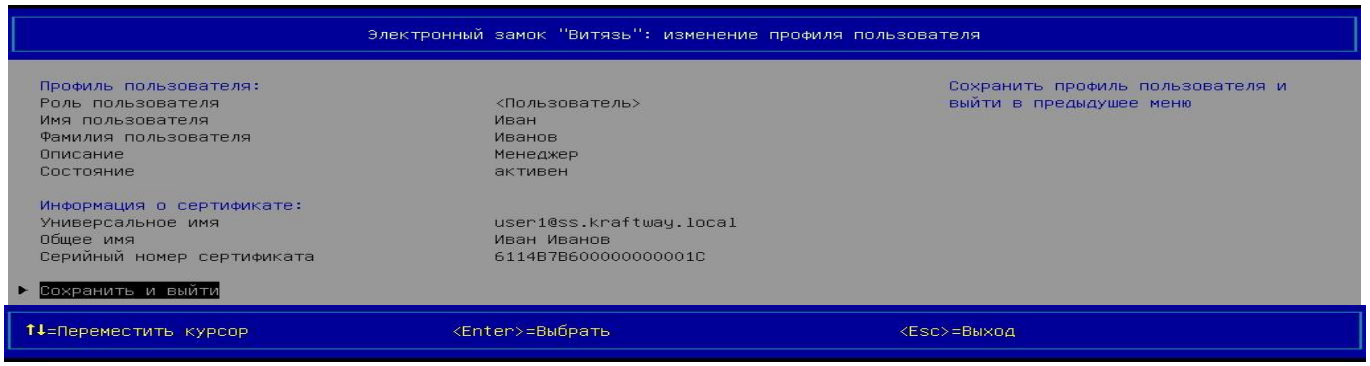

Рис. 189

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»

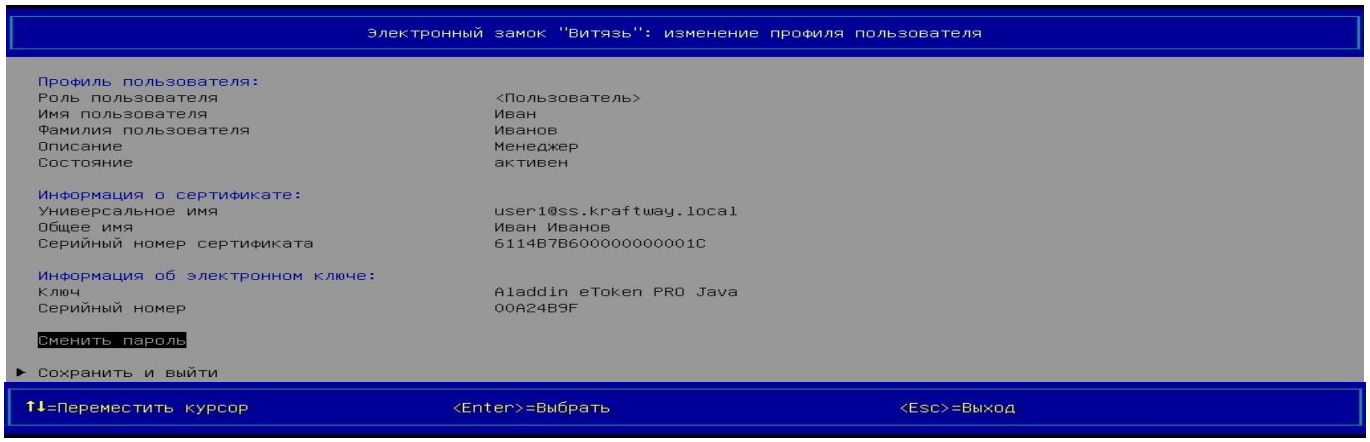

Рис. 190

7) выбрать п. *Сменить пароль*;

8) подключить АН к USB-порту, PIN-код которого подлежит изменению;

9) нажать клавишу [Enter], отображается окно для ввода старого пароля пользователя (рис. 191);

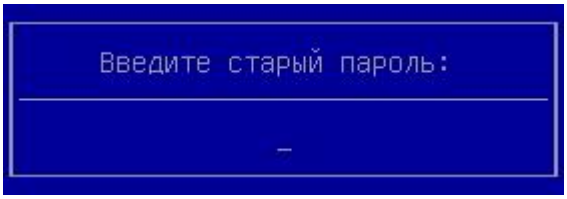

Рис. 191

10) ввести старый пароль в окно;

11) нажать клавишу [Enter], отображается окно для ввода нового пароля пользователя (рис. 192);

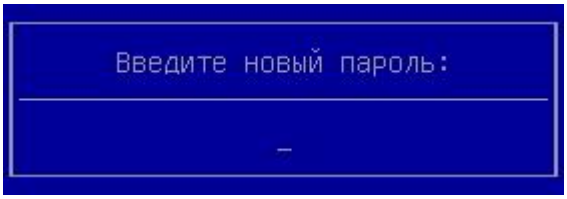

Рис. 192

12) ввести новый пароль;

13) нажать клавишу [Enter], отображается окно для подтверждения нового пароля пользователя (рис. 193);

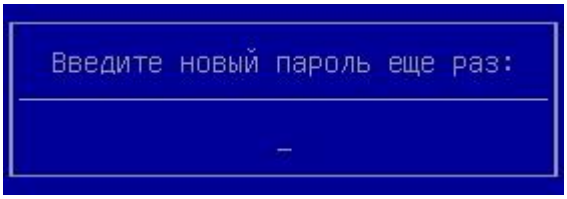

Рис. 193

14) ввести новый пароль;

15) нажать клавишу [Enter], отображается окно (рис. 194), информирующее об успешном изменении пароля;

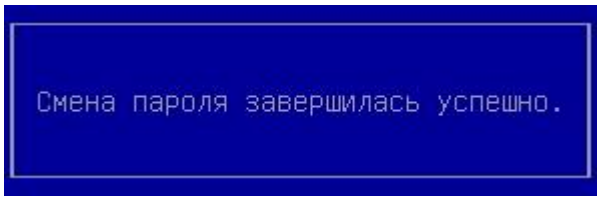

Рис. 194

16) нажать любую клавишу на клавиатуре.

Примечания:

1. При выбранном профиле пользователя в разделе *Профили пользователей* (см. рис. 183 - 186) 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, определенное для пользователя администратором). Объем выводимой дополнительной информации о профиле пользователя зависит от способа аутентификации и роли пользователя.

2. Если для пользователя задан *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 аналогична тем страницам, что представлены на рис. 184 - 186, когда параметру *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* идентично представлению дополнительной информации при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: модуль *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – «Электронный ключ» (см. рис. 183).

3. Пользователю предоставляется возможность изменения пароля при следующих настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2: модуль *Электронный замок «Витязь»* – «Вкл», *Способ аутентификации* – или «Электронный ключ», или «Цифровой сертификат и электронный ключ».

4. Если для пользователя задан *Способ аутентификации* – «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок «Витязь»: изменения профиля пользователя* (см. рис. 189). При данном способе аутентификации изменить пароль пользователя нельзя.

3.2.2. Вывод детальной информации о пользователе

Для вывода детальной информации о пользователе:

1) выполнить действия перечисления 1) – 4) п 3.2.1;

2) выбрать п. *Детальная информация* в диалоговом окне (см. рис. 187);

3) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: детальная информация о пользователе* (рис. 196 - 197).

Страница *Электронный замок «Витязь»: детальная информация о пользователе* (вид 1),

профиль пользователя, *Способ аутентификации* – «Электронный ключ»

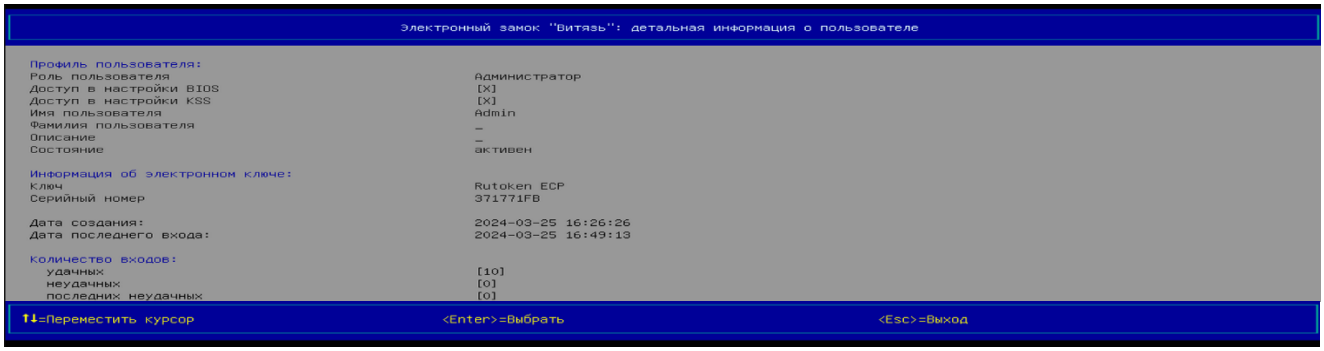

Рис. 195

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

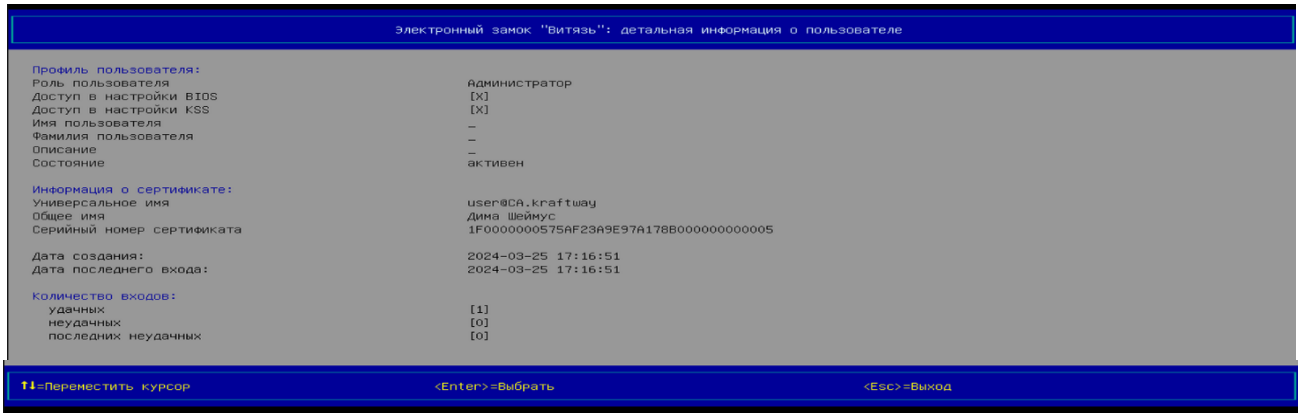

Рис. 196

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

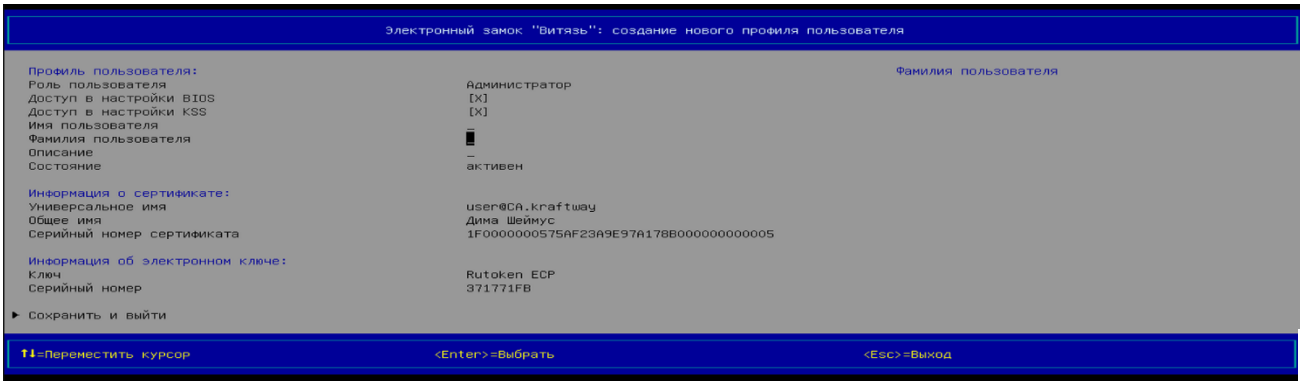

Рис. 197

Примечание. Количество параметров и их значений, выводимых на странице *Электронный замок «Витязь»: детальная информация о пользователе* (см. рис. 196 - 197), зависит от роли пользователя, которая была установлена администратором в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2, 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 и серийный номер;

8) дата создания профиля пользователя;

9) дата последнего входа пользователя;

10) количество входов: удачных, неудачных и последних неудачных;

11) максимальное количество попыток ввода пароля.

Примечание. Количество последних неудачных входов – это количество попыток аутентификации, результаты которых были отрицательными. Если хотя бы один раз, после нескольких неудачных попыток аутентификации, пользователь прошел процедуру аутентификации с положительным результатом, то количество последних неудачных входов обнуляется.

3.2.3. Загрузка штатной ОС компьютера

Для выполнения загрузки ОС при включенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 пользователю следует пройти процедуру аутентификации, а после успешного ее прохождения – дождаться загрузки ОС (см. подраздел 3.1).

3.3. Сообщения пользователю

Сообщения пользователю – это тексты, выводимые на страницах или в окнах в процессе работы с ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Основная часть сообщений, выводимых на экран, представлена в соответствующих подразделах. В разделе приводятся дополнительные сообщения ПК «ЭЗ «ВИТЯЗЬ» 2.2, которые не были описаны и требуют отдельного рассмотрения.

Ситуация № 1. Во время выполнения процедуры КЦ для каждого файла, прошедшего проверку, отображается результат данной проверки в виде записи (рис. 198):

```
<Результат проверки>: <путь к файлу, прошедшего проверку>.
```

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:

1) количество проверенных файлов;

2) количество файлов, которые прошли процедуру КЦ с положительным результатом;

3) количество файлов, которые прошли процедуру КЦ с отрицательным результатом.

При отрицательном результате процедуры КЦ, на экран выводятся сообщения (рис. 198).

Целостность файловой системы нарушена

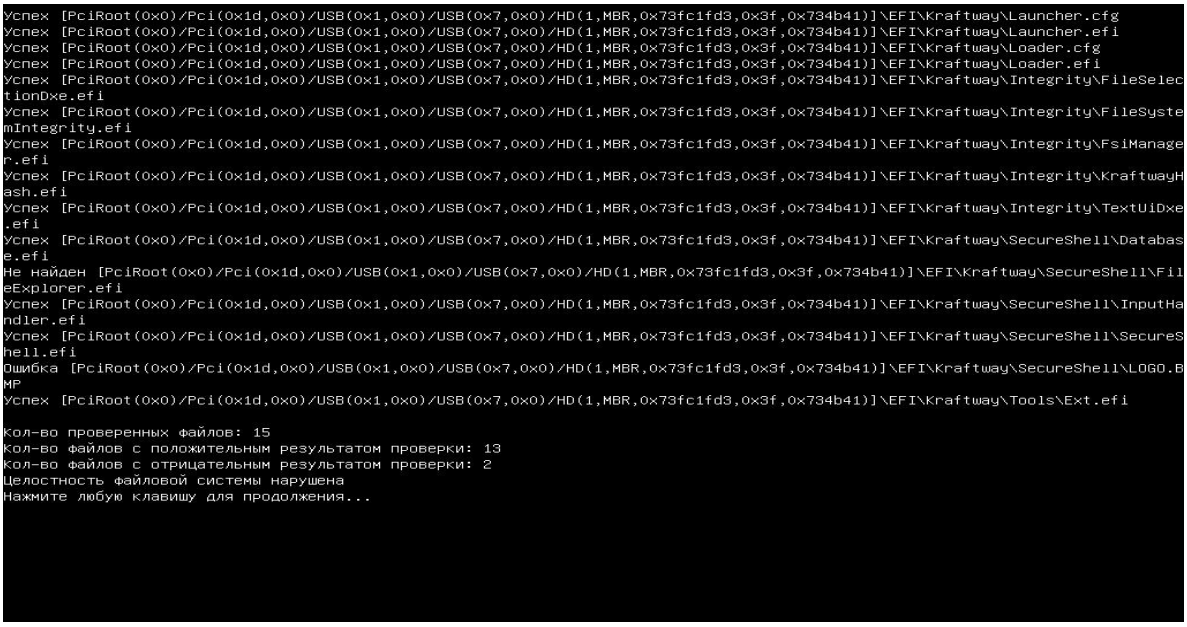

Рис. 198

Решение: обратиться к администратору.

Ситуация № 2. При отрицательном результате процедуры КЦ, и когда ПК «ЭЗ «ВИТЯЗЬ» 2.2 включен, после вывода записей, описанных в ситуации № 1 (рис. 198), и нажатия на любую клавишу клавиатуры, на экран выводятся сообщения (рис. 199).

Страница *Локальная аутентификация* (вид 5),

ПК «ЭЗ «ВИТЯЗЬ» 2.2 заблокировал компьютер

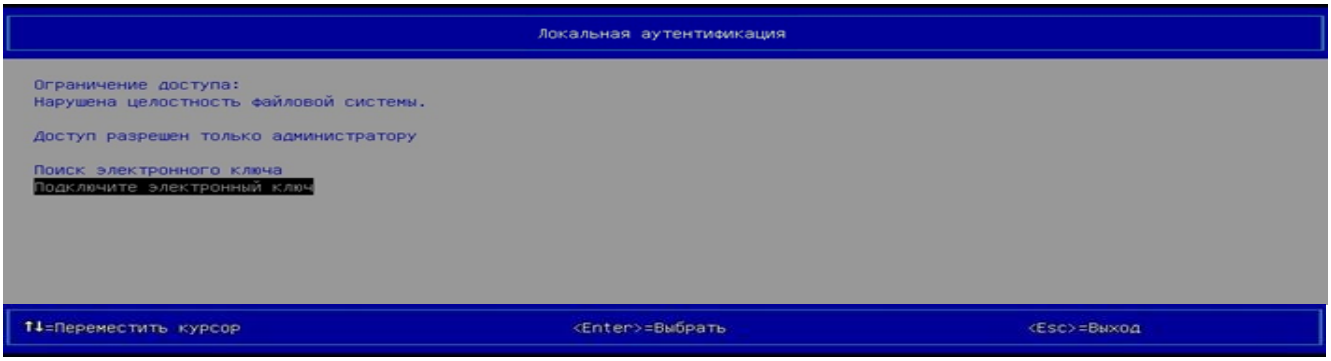

Рис. 199

Решение: обратиться к администратору.

Ситуация № 3. Если после вывода страницы *Локальная аутентификация* (рис. 199) пользователь подключит свой АН к USB-порту, введет пароль пользователя в соответствующем окне (рис. 177) и нажмет клавишу [Enter], на экран будет выведено окно (рис. 200).

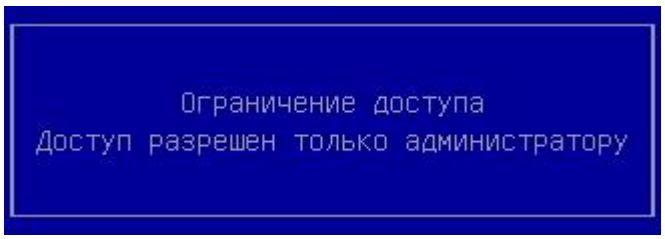

Рис. 200

Ситуация № 4. Если текущий пароль пользователя был введен неправильно во время его аутентификации, отображается окно (рис. 201), информирующее о вводе неверного пароля.

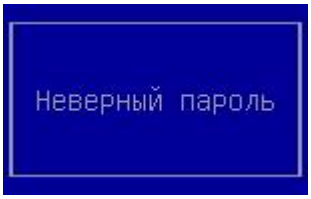

Рис. 201

Решение: нажать любую клавишу на клавиатуре и 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 ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Ситуация № 5. Если количество неправильно введенного пароля пользователя во время его аутентификации равно максимальному количеству попыток ввода пароля, которое устанавливается администратором для пользователя, то после нажатия на клавишу [Enter]:

1) отображается окно (рис. 202), информирующее о превышении количества попыток ввода пароля;

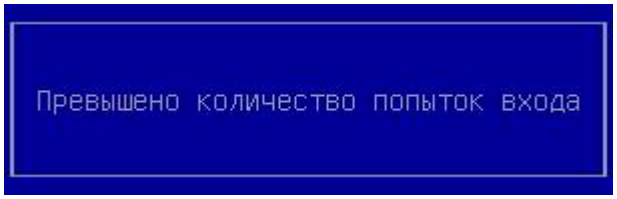

Рис. 202

2) после повторного нажатия на клавишу [Enter] отображается окно (см. рис. 4.4), информирующее о том, что был введен неверный пароль;

3) после третьего нажатия на клавишу [Enter] отображается окно (рис. 4.6), информирующее о попытке входа заблокированного пользователя.

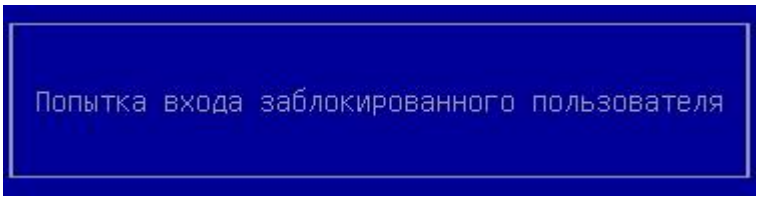

Рис. 203

Решение: обратиться к администратору для разблокировки профиля пользователя.

Ситуация № 6. Если после включения компьютера, во время процедуры аутентификации, подключить АН пользователя, профиль которого ранее был заблокирован ПК «ЭЗ «ВИТЯЗЬ» 2.2, то на экран будет выведено окно (рис. 203), информирующее о попытке входа заблокированного пользователя.

Решение: обратиться к администратору для разблокировки профиля пользователя.

Ситуация № 7. Отображается запись вида:

«ОШИБКА! Превышено количество попыток аутентификации.
Нажмите любую клавишу для перезагрузки…»

при следующих условиях:

1) если во время прохождения пользователем процедуры аутентификации было превышено максимальное количество попыток аутентификации, т.е. количество подключений АН пользователя к USB-порту, которое было задано администратором ранее в настройках ПК «ЭЗ «ВИТЯЗЬ» 2.2;

2) если во время прохождения пользователем процедуры аутентификации количество попыток ввода пароля пользователя превысило максимальное количество попыток аутентификации, которое было задано администратором ранее в настройках, т.е. если после вывода окна (см. рис. 203) пользователем было выполнено последовательное нажатие на клавишу [Enter] такое количество раз, которое привело к превышению максимального количества попыток аутентификации.

Решение: обратиться к администратору для разблокировки профиля пользователя.

Ситуация № 8. Если при прохождении процедуры аутентификации подключить к USB-порту АН пользователя, незарегистрированный в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2, то на экран будет выведено окно (рис. 204), информирующее о попытке использования незарегистрированного ключа.

Рис. 204

Примечание. Окно (рис. 204) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при если для пользователя установлен *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Варианты возможных решений:

1) отключить АН от USB-порта, который не был ранее зарегистрирован в ПК «ЭЗ «ВИТЯЗЬ» 2.2 и обратиться к администратору для получения АН, который применялся

при создании в ПК «ЭЗ «ВИТЯЗЬ» 2.2 профиля пользователя и был зарегистрирован в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2. Повторить процедуру аутентификации с применением нового АН;

2) отключить АН от USB-порта, который не был ранее зарегистрирован в ПК «ЭЗ «ВИТЯЗЬ» 2.2 и обратиться к администратору для создания профиля пользователя с применением имеющегося АН. Повторить процедуру аутентификации с применением этого же АН.

Ситуация № 9. Если во время прохождения процедуры аутентификации пользователем было выбрано значение ключевого поля на странице *Локальная аутентификация* (см. рис. 180 - 17), которое отсутствует в БД ПК «ЭЗ «ВИТЯЗЬ» 2.2, то после нажатия на клавишу [Enter] на экран будет выведено окно (рис. 205), информирующее о том, что пользователь, проходящий в данный момент процедуру аутентификации, не зарегистрирован для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2.

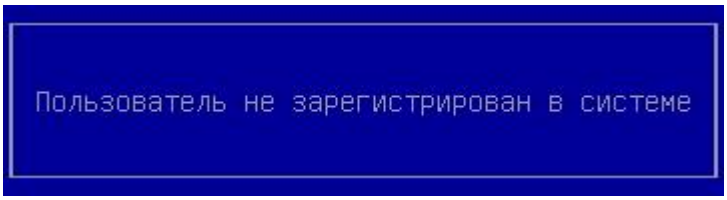

Рис. 205

Примечание. Окно (см. рис. 205) выводится на экран только если для пользователя установлен *Способ аутентификации* – «Цифровой сертификат».

Решение: обратиться к администратору.

Ситуация № 10. Если во время прохождения процедуры аутентификации не были найдены сертификаты пользователей на АН, то на странице *Локальная аутентификация* выводится сообщение (рис. 206).

Страница *Локальная аутентификация* (вид 6),

сертификаты не были найдены на АН

Рис. 206

Примечание. Запись, представленная на странице *Локальная аутентификация* (рис. 206), может быть выведена, если для пользователя установлен *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: обратиться к администратору 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. 3.1.4), то отображается окно (рис. 207), информирующее об ошибке аутентификации.

Рис. 207

Примечание. Окно (рис. 207) выводится на экран если для пользователя установлен *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: обратиться к администратору.

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 (рис. 208), информирующее о том, что АН не был подключен, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (рис. 209), информирующее о том, что произошла ошибка при смене пароля.

Рис. 208

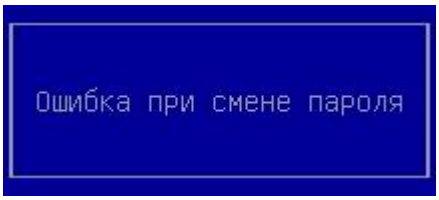

Рис. 209

Решение: обратиться к администратору.

Ситуация № 13. Если текущий пароль пользователя был введен неправильно во время изменения пароля пользователя, то отображается окно (рис. 210), информирующее о том, что пароль был введен неправильно, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рис. 209), информирующее о том, что произошла ошибка при смене пароля.

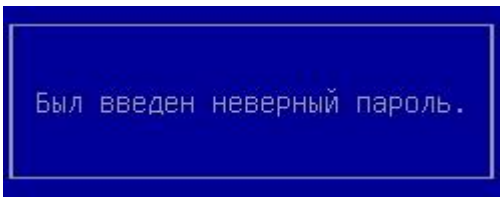

Рис. 210

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

Ситуация № 14. Если новый пароль пользователя был введен неправильно во время изменения пароля, то отображается окно (рис. 211), информирующее о несовпадении паролей, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рис. 209), информирующее о том, что произошла ошибка при смене пароля.

Рис. 211

Решение: 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, то отображается окно (рис. 212), информирующее о превышении отведенного времени на ввод пароля.

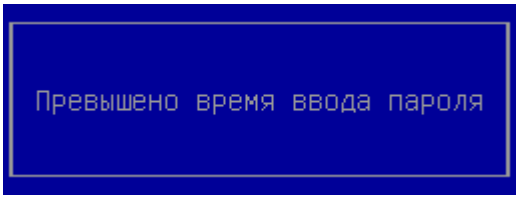

Рис. 212

Решение: пройдите процедуру ввода пароля еще раз.

Ситуация № 16. Пользователь при загрузке ОС может получить сообщение о том, что в системе обнаружен вирус. Возможны два варианта:

1) в случае, если администратор системы предоставил пользователю права выбирать действия при обнаружении вируса (лечить/восстанавливать/удалять), появится сообщение в соответствии с рис. 213, тогда можно клавишами-стрелками выбрать действие и активировать его клавишей [Enter];

Обнаружено заражение, разрешены действия

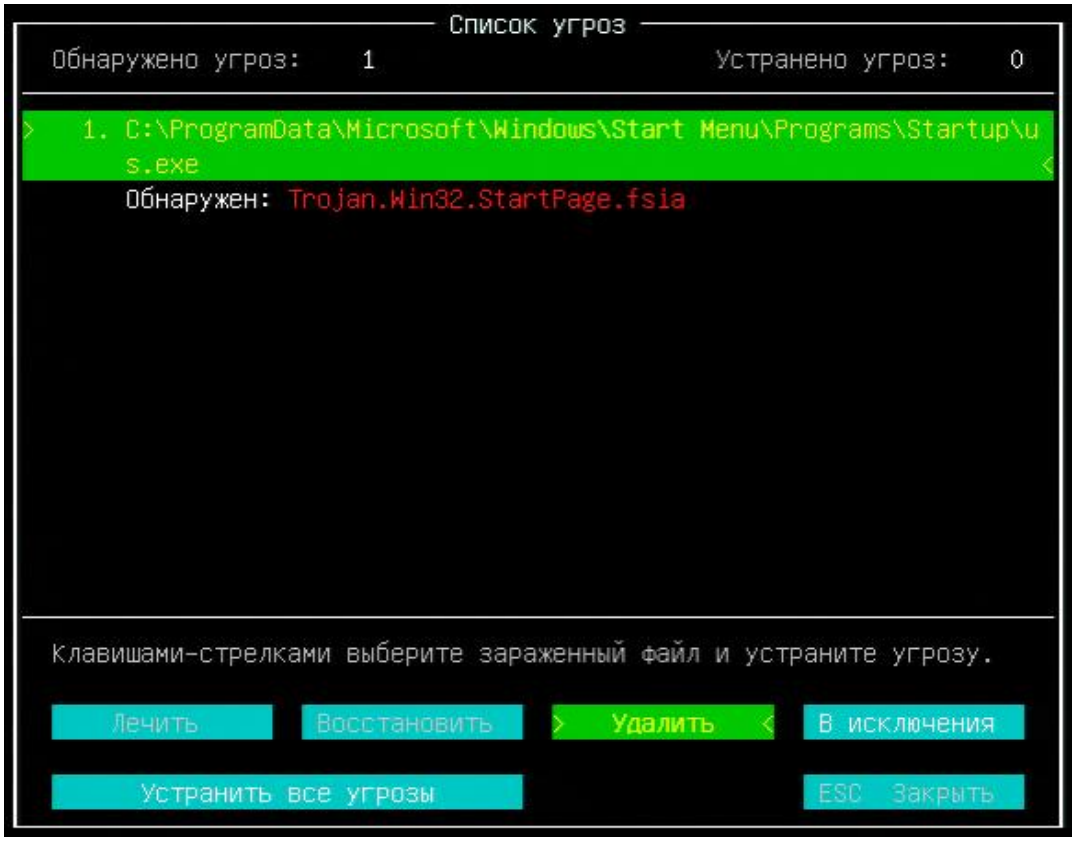

Рис. 213

2) если прав на выполнение действий пользователь не имеет, сообщение будет в соответствии с рисунком 214, в этом случае следует обратиться к администратору.

Обнаружено заражение, действия не разрешены

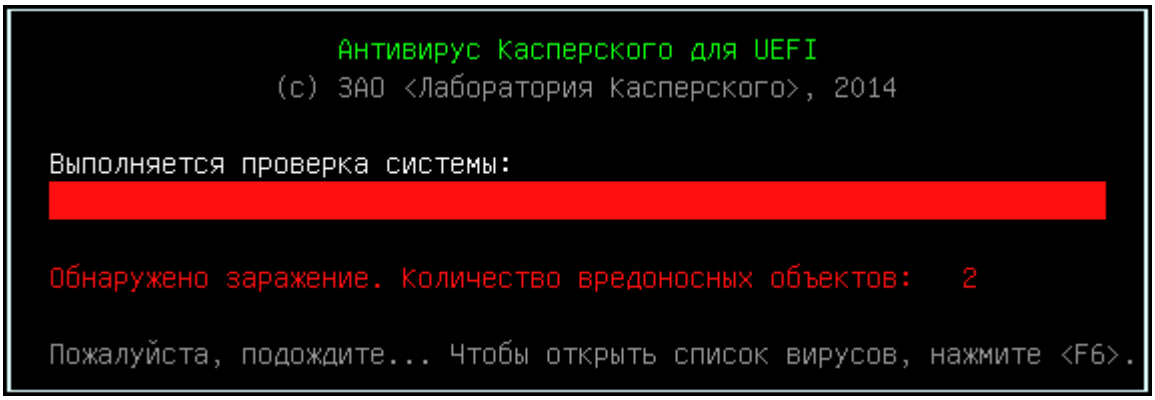

Рис. 214

4. РАБОТА ПОЛЬЗОВАТЕЛЯ С ГОСТЕВЫМ ВХОДОМ

Гостевой вход предназначен для обеспечения пользователю без АН доступа к компьютеру. Активировать гостевой доступ имеет право только пользователь с правами администратора. Для активации гостевого доступа:

1) выбрать п. *Электронный замок «Витязь»* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (см. рис. 5);

3) выбрать п. *Конфигурация* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Конфигурация* (рис. 215);

5) выбрать п. *Гостевой вход* и нажать клавишу [Enter]

Страница Электронный замок «Витязь»: конфигурация,

п. Гостевой вход

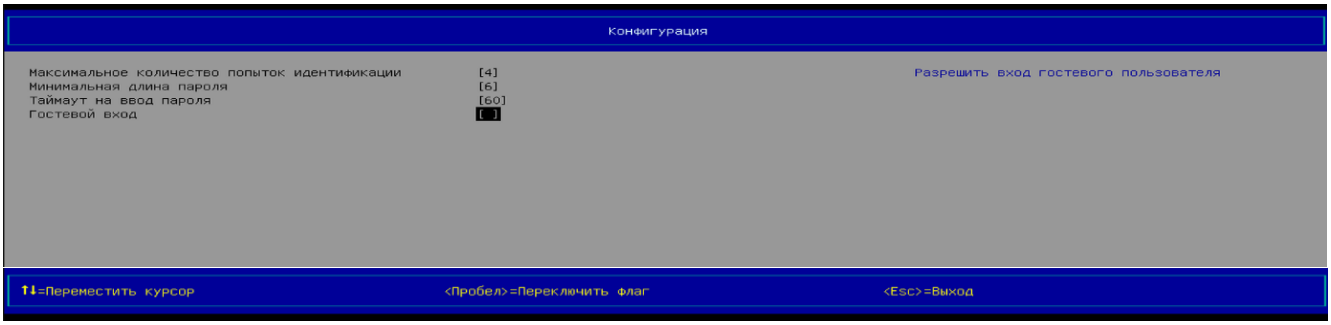

Рис. 215

6) выбрать п. Таймаут на гостевой вход (рис. 216) и нажать клавишу [Enter];

Страница Электронный замок «Витязь»: конфигурация,

п. Таймаут на гостевой вход

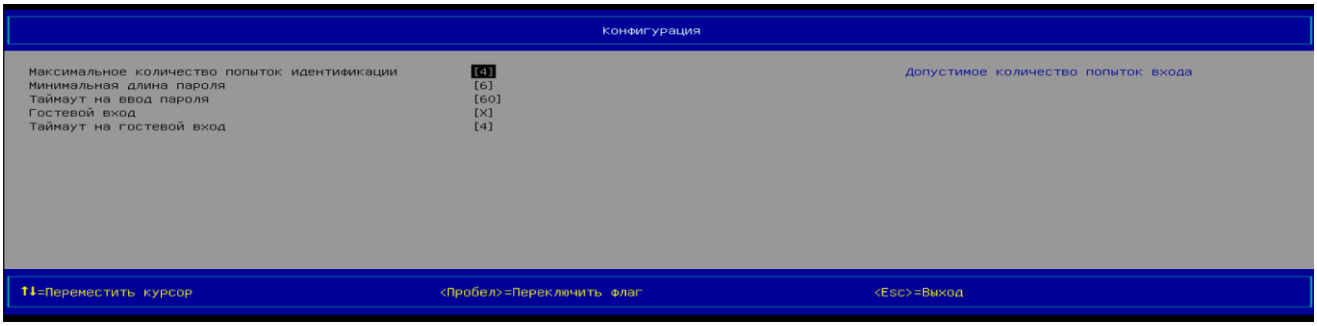

Рис. 216

7) нажать клавишу [Enter] и установить требуемое значение таймаута на гостевой вход клавишами на цифровом блоке клавиатуры;

8) нажать клавишу [Esc] для выхода.

Для входа пользователя по гостевому входу, отключить от компьютера АН и включить питание.

На экране отобразится обратный отсчет таймера гостевого входа (рис. 217) на странице *Локальная аутентификация*.

Страница Электронный замок «Витязь»: Локальная аутентификация, Гостевой вход

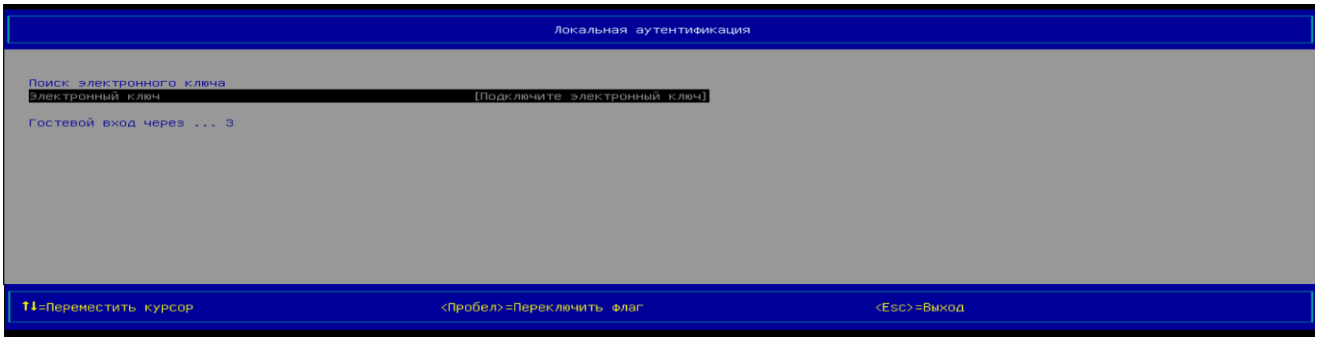

Рис. 217

По окончании отсчета таймаута начнется загрузка ОС произойдет загрузка штатной ОС. Пользователю не будут доступны настройки СДЗ.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение	Термин
АН	Аутентифицирующий носитель (носители)
БД	База данных
КС	Контрольная сумма
КЦ	Контроль целостности
ОС	Операционная система
ПО	Программное обеспечение
СДЗ	Средство доверенной загрузки
УЦ	Удостоверяющий центр
ФС	Файловая система
BIOS	англ. Basic Input/Output System – базовая система ввода/вывода
CN	англ. Common Name – общее имя
EXT	англ. Extended File System – расширенная файловая система в ОС Linux
FAT	англ. File Allocation Table – файловая система ОС MS-DOS, Windows 9x
KSS	англ. Kraftway Secure Shell – оболочка для управления модулями безопасности
MBR	англ. Master Boot Record – главная загрузочная запись: код и данные, необходимые для загрузки ОС и расположенные в первых физических секторах (чаще
NTFS	англ. New Technology File System – файловая система новой технологии, основная файловая система в ОС Windows
PIN-код	англ. Personal Identification Number – персональный идентификационный номер, аналог пароля
Smart Card	англ. ICC (Integrated Circuit Card) – смарт-карта, пластиковая карта с интегрированными электронными цепями
SPI	англ. Serial Peripheral Interface – синхронный последовательный интерфейс связи
SPI Flash	англ. Serial Peripheral Interface Flash - Микросхема памяти для хранения внутреннего ПО материнской платы
UEFI	англ. Unified Extensible Firmware Interface – интерфейс между ОС и микропрограммами, управляющими низкоуровневыми функциями оборудования
UPN	англ. Universal Program Name – универсальное программное имя
USB	англ. Universal Serial Bus – универсальная последовательная шина

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					