Руководство администратора

Программный комплекс электронный замок Витязь

ВЕРСИЯ 2.2

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для администрирования программного комплекса электронный замок «Витязь» версии 2.2 (далее по тексту ПК ЭЗ «Витязь» В2.2), который поставляется в виде системного программного обеспечения материнских плат.

В настоящем документе содержится информация о назначении ПО, функциях ПО с некоторыми ограничениями на его применение, сведения о технических средствах, обеспечивающих выполнение данного ПО, представлены сведения о настройке ПО, работе, приводятся информационные сообщения, сообщения об ошибках ПО и способы их устранения.

Данное руководство ориентировано для персонала системного администрирования.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПО

1.1 Обозначение и наименование ПО

Наименование программного обеспечения – Программный комплекс электронный замок «Витязь» версия 2.2.

Версия программного обеспечения – 2.2.

Обозначение программного обеспечения – 643.18184162.00006-2.2.

Наименование предприятия-изготовителя – АО «Крафтвэй корпорэйшн ПЛС»

Фактический адрес: 3-я Мытищинская, д. 16, корп. 60. Москва, 129626,

тел. +7(495) 969-2400

1.2 Назначение ПО

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

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

1) Для самого средства доверенной загрузки:

– нарушение целостности программного обеспечения средства доверенной загрузки;

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

– несанкционированное изменение конфигурации (параметров) средства доверенной загрузки;

– преодоление или обход функций безопасности средства доверенной загрузки;

– несанкционированное внесение изменений в логику функционирования средства доверенной загрузки, в том числе за счет получения остаточной информации средства

доверенной загрузки из памяти средства вычислительной техники и (или) получение доступа к ресурсам средства доверенной загрузки из программной среды средства вычислительной техники после завершения работы средства доверенной загрузки;

– сбои и ошибки в процессе функционирования средства доверенной загрузки.

2) Для средства вычислительной техники:

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

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

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

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

– блокирование попыток несанкционированной загрузки нештатной операционной системы;

– контроль доступа пользователей к процессу загрузки операционной системы;

– контроль целостности программного обеспечения и среды функционирования.

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

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

– самотестирование средства доверенной загрузки;

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

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

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

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

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

1.3 Функции ПО

ПК ЭЗ «Витязь» В2.2 обеспечивает:

1) Разграничение доступа:

– к управлению СДЗ;

– к управлению работой СДЗ;

– к управлению параметрами СДЗ;

2) Аутентификацию с выбором способа аутентификации:

– аутентифицирующий носитель;

– цифровой сертификат;

3) Контроль целостности:

– электронного замка;

– базы данных ЭЗ при каждом старте ПК;

– компонентов компьютера;

– программной среды;

4) Блокирование загрузки операционной системы ЭЗ;

5) Управление доступом к ресурсам компьютера;

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

7) Управление журналом аудита;

8) Запрет загрузки ОС с внешних USB;

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

– обнаружение зараженных вредоносными компьютерными программами (вирусами) объектов;

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

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

10) Обеспечение безопасности после завершения работы СДЗ.

1.4 Условия применения

ПК ЭЗ «Витязь» В2.2 поставляется исключительно в предустановленном виде, как ПО интегрированное в UEFI BIOS на этапе производства материнских плат.

1.4.1 Требования к среде функционирования ЭЗ:

В среде функционирования средств доверенной загрузки должны быть обеспечены следующие основные условия:

1) Установка и управление средствами доверенной загрузки в соответствии с эксплуатационной документацией;

2) Совместимость компонентов средств доверенной загрузки с компонентами средств вычислительной техники информационной системы;

3) Физическая защита компонентов средств доверенной загрузки

- Обеспечение физической целостности средств вычислительной техники, доступ к которым контролируется с применением СДЗ – ЭЗ;

4) Обеспечение доверенного маршрута

- Обеспечение доверенного маршрута при взаимодействии с уполномоченными субъектами;

5) Обеспечение условий безопасного функционирования

- Обеспечение аутентификации пользователей ЭЗ;
- Обеспечение расширенных возможностей по хранению и анализу информации аудита безопасности;
- Обеспечение меток времени для реализации функции аудита безопасности средства доверенной загрузки;

6) Управление атрибутами безопасности

– Обеспечение возможности управления атрибутами безопасности компонентов ЭЗ;

7) Защита от отключения (обхода)

– Обеспечение невозможности отключения (обхода) компонентов ЭЗ.

1.4.2 Требования к аппаратному обеспечению

Для обеспечения двухфакторной аутентификации при взаимодействии ПК ЭЗ «Витязь» с АН должны применяться USB-ключи (типа Рутокен S, Рутокен ЭЦП, eToken PRO, eToken ГОСТ) и смарт-карты (типа Микрон, eToken PRO, eToken ГОСТ), сертифицирован-

ные на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по соответствующему конфиденциальности обрабатываемой информации уровню контроля отсутствия недекларированных возможностей. Для работы с USB-ключом АН требуется минимум один свободный порт USB. Для использования смарт-карт необходимо наличие установленного считывателя смарт-карт.

ПК ЭЗ «Витязь» В2.2 поставляется исключительно в предустановленном на материнскую плату виде.

Для работы ЭЗ необходима материнская плата с поддержкой UEFI 2.3.1 или с поддержкой UEFI более поздней версии. Обязательным параметром материнской платы является наличие микросхемы SPI Flash с объемом свободной памяти не менее 6 Мб, которая требуется для работы ЭЗ.

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

В зависимости от количества объектов, целостность которых будет контролироваться ЭЗ, для хранения списка объектов требуется хранилище размером не менее 325 Кбайт.

1.4.3 Требования к программному обеспечению

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

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

– наличие программного кода, пользовательского интерфейса и интерфейсов взаимодействия с ЭЗ (оболочка Kraftway Secure Shell - KSS), которые обеспечивают его интерфейс включения/отключения, очистки содержимого хранилища учетных записей пользователей и журналов ЭЗ, получения после аутентификации информации о роли авторизованного пользователя из ЭЗ с целью обеспечения доступа администратора к настройкам ЭЗ и блокирования такого доступа для пользователя.

ЭЗ может применяться со следующими файловыми системами:

- FAT16;
- FAT32;

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

1.5 Основные характеристики

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

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

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

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

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

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

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

1.6 Ролевая модель пользователей ЭЗ

Доступ к настройкам ЭЗ зависит от роли получаемой пользователем при аутентификации в ЭЗ.

ЭЗ обеспечивает разделение пользователей на следующие роли:

– *Администратор*;

– *Пользователь*.

Администраторы ЭЗ, в свою очередь, различаются между собой правами доступа. Назначение прав доступа администраторам выполняется при создании или изменении профилей пользователей с ролью *Администратор* (см. п. 3.5.1 - п. 3.6.4). Из-за различий прав доступа администраторов можно разбить по типам (см. Таблица 1.1):

– Тип1 – администратор, которому разрешено: доступ к программе настройки UEFI материнской платы, доступ к оболочке KSS для последующей настройки ЭЗ, загрузка ОС компьютера;

– Тип 2 – администратор, которому разрешено: доступ к программе настройки UEFI материнской платы, загрузка ОС компьютера;

– Тип 3 – администратор, которому разрешено: доступ к оболочке KSS для последующей настройки ЭЗ, загрузка ОС компьютера;

– Тип 4 – администратор, которому разрешена возможность только загрузки ОС компьютера, например, в случае нештатных ситуаций.

Примечание. Администратор, профиль которого был создан первым после включения ЭЗ, всегда Тип 1 и защищен от изменений.

Таблица 1.1 – Права доступа пользователей

Тип пользователя	Доступ к настройкам		
	UEFI	KSS / ЭЗ	ОС
Администратор			
- Тип 1	X	X	X
- Тип 2	X		X
- Тип 3		X	X
- Тип 4			X
Пользователь			X

1.7 Организационно-технические меры

Должны быть приняты организационные (организационно-технические) меры, исключающие неконтролируемый доступ посторонних лиц к компьютерам пользователей в нерабочее время, а также в рабочее время при отсутствии пользователей.

1.7.1 Правила поведения администратора

Администратор должен работать в соответствии с документом «Программный комплекс электронный замок «Витязь» версия 2.2. Руководство администратора» и, прежде всего, ознакомиться с ним.

Администратор обязан соблюдать следующие правила работы с АН:

1) после получения АН заменить установленный в нем PIN-код для защиты доступа к компьютеру;
2) своевременно заменять PIN-код к АН в соответствии с политикой безопасности организации;
3) при вводе PIN-кода к АН исключать возможность визуального просмотра его набора другими лицами;
4) не передавать АН, находящийся в распоряжении администратора, другим лицам, а также не оставлять его без присмотра. Попадание АН в чужие руки несет опасность его компрометации;
5) не сообщать PIN-код к АН другим лицам, хранить записанные PIN-коды в недоступном для других лиц месте. Разглашение PIN-кода к АН означает его компрометацию;
6) при утере АН следует немедленно присвоить новое АН, учётной записи администратора, АН которой был утерян;
7) беречь АН от механических повреждений;
8) не отсоединять АН от рабочей станции во время работы с использующими его приложениями. Перед отсоединением АН от рабочей станции следует завершить работу всех приложений, использующих АН.

1.7.2 Правила поведения пользователя

Администратор должен ознакомить с данными правилами пользователей, работающих за компьютерами, на которых установлен ПК ЭЗ «Витязь» В2.2.

Пользователь обязан соблюдать следующие правила работы с АН:

1) после получения АН заменить установленный в нем PIN-код к АН для защиты доступа к компьютеру;
2) своевременно заменять PIN-код к АН в соответствии с политикой безопасности организации;
3) при вводе PIN-кода к АН исключать возможность визуального просмотра его набора другими лицами;
4) не передавать АН, находящийся в распоряжении пользователя, другим лицам, а также не оставлять его без присмотра. Попадание АН в чужие руки несет опасность его компрометации;

5) не сообщать PIN-код к АН другим лицам, хранить записанные PIN-коды в недоступном для других лиц месте. Разглашение PIN-кода означает его компрометацию;
6) при утере АН немедленно сообщить об этом администратору;
7) беречь АН от механических повреждений;
8) не отсоединять АН от рабочей станции во время работы с использующими его приложениями. Перед отсоединением АН от рабочей станции следует завершить работу всех приложений, использующих АН.

2 ЛОГИЧЕСКАЯ СТРУКТУРА ПК ЭЗ «ВИТЯЗЬ» В2.2

2.1 Описание логической структуры ПК ЭЗ «Витязь» В2.2

Структура интерфейсных функций, составных частей и связи между ними. Логическая структура интерфейсных функций приведена на рисунке 2.1:

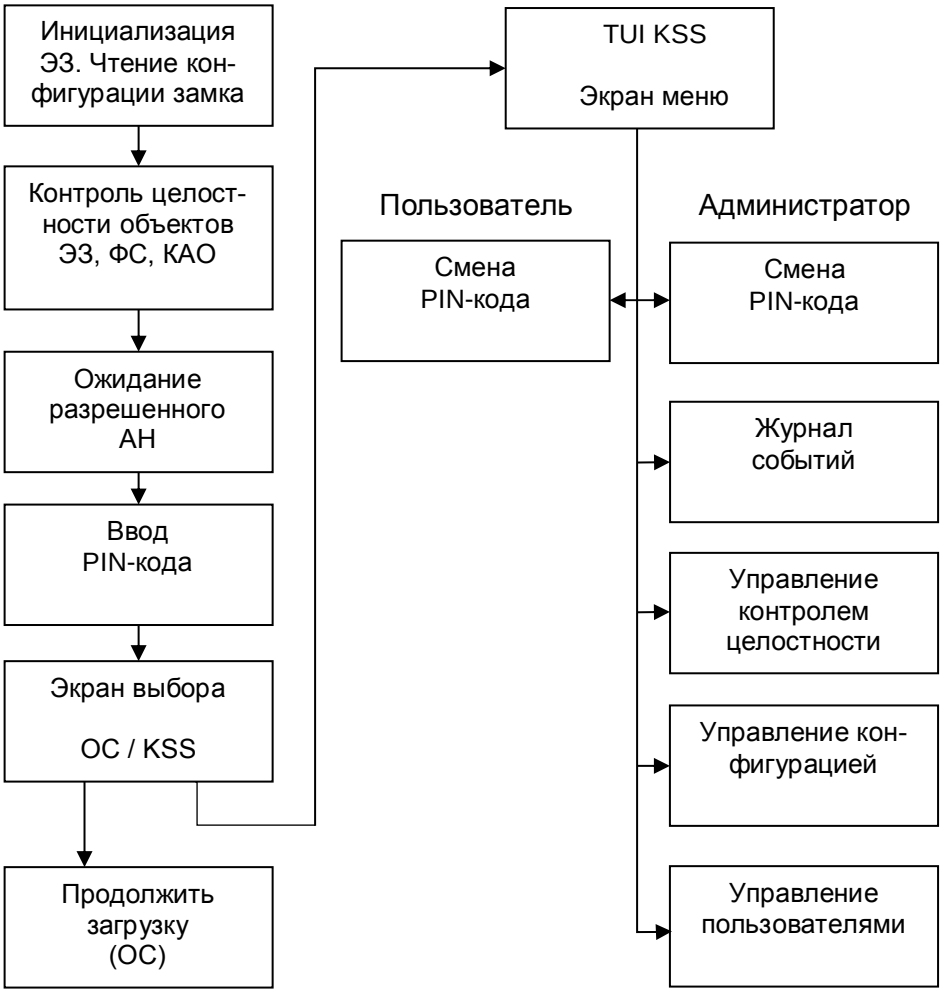


Рисунок 2.1 – Логическая структура интерфейсных функций

ПК ЭЗ «Витязь» В2.2 состоит из следующих логических блоков:

– блок обеспечения базового функционала ЭЗ (инициализация ЭЗ, чтение конфигурации замка, аутентификация пользователя, управление пользователями, управление конфигурацией ЭЗ, запись событий в журнал событий);

– блок проверки целостности объектов ЭЗ, ФС, Оборудования (проверка целостности объектов ЭЗ, ФС, Оборудования управление контролем целостности, выгрузка журнала событий).

2.2 Используемые методы

При написании программы ЭЗ применялось низкоуровневое, процедурное программирование.

2.3 Алгоритм работы программы

Алгоритм работы ЭЗ на этапе загрузки компьютера приведен на рисунке 2.2

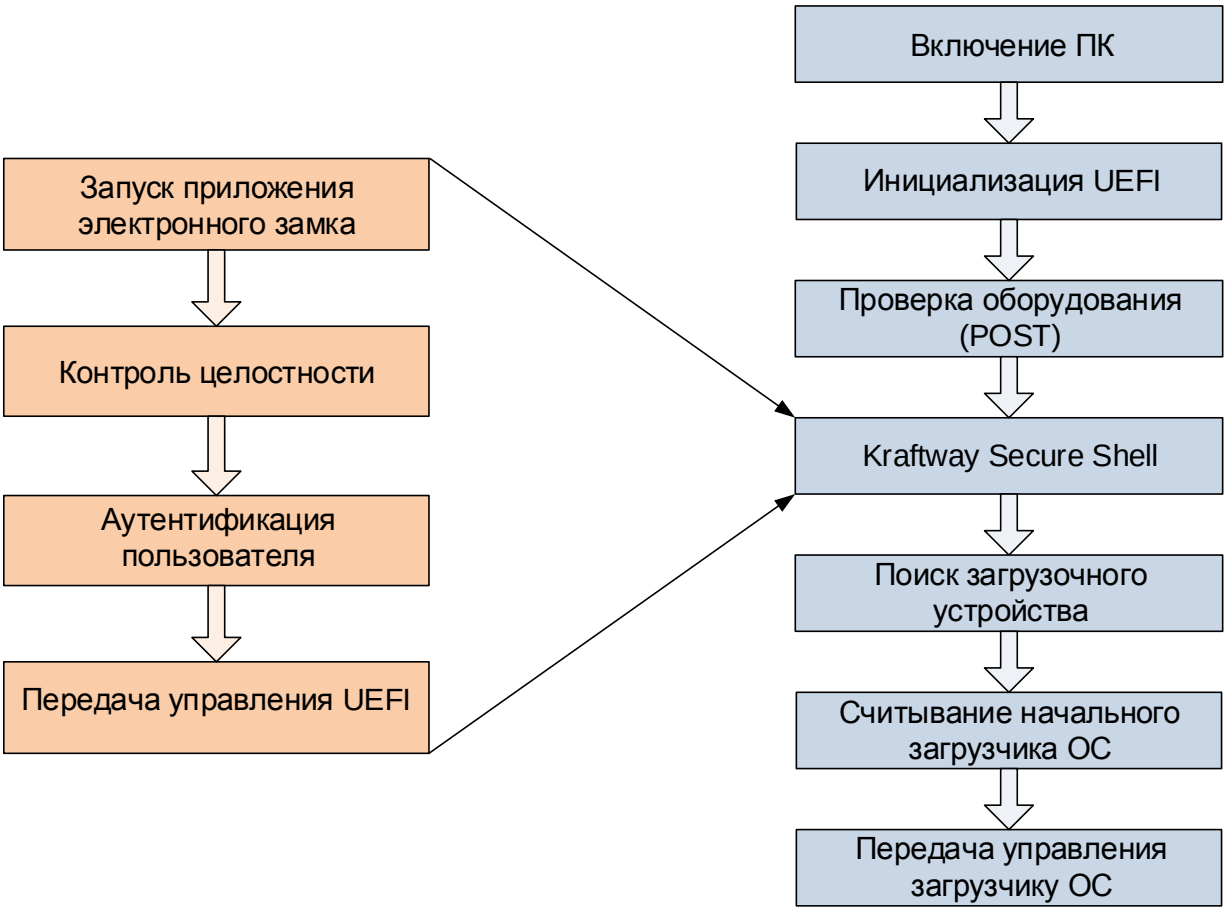


Рисунок 2.2 – Алгоритм работы ЭЗ на этапе загрузки компьютера

После включения компьютера производится инициализация UEFI и самотестирование оборудования, после чего управление компьютером перехватывается ЭЗ.

Описание алгоритма работы ЭЗ на этапе загрузки компьютера:

1) инициализация ЭЗ. Чтение конфигурации замка;
2) проверка целостности объектов ЭЗ, ФС, Оборудования. КЦ имеет два режима: «Жёсткий» и «Мягкий» (см. Таблица 2.1). Для администратора всегда установлен «Мягкий» режим, для пользователя всегда установлен «Жёсткий» режим;
3) ожидание АН, серийный номер которого находится в базе (т.е. для которого зарегистрирован пользователь) и пользователь которого не заблокирован;
4) экран ввода PIN-кода. Пользователь вводит PIN-код, который сравнивается с PIN-кодом, сохраненном в АН. Аутентификация проводится путем проверки наличия АН у пользователя ЭЗ, знания PIN-кода АН и наличия в его памяти дополнительного аутентификатора, который записывается на этапе регистрации в ЭЗ и располагается в защищенной области памяти АН. При способе аутентификации с помощью цифрового сертификата пользователя с применением корневого сертификата УЦ обязательными факторами аутентификации должны являться наличие сертификата пользователя и знание PIN-кода для получения доступа к устройству его хранения. При вводе определенного количества неверных PIN-кодов пользователь блокируется и войти может только администратор, вставив своё АН;
5) экран меню. Для пользователя и администратора количество пунктов разное:

– Администратору доступны все пункты – «Электронный замок “Витязь”», «Управление сертификатами», «Контроль целостности файловой системы», «Контроль модулей безопасности», «Настройки»;
– Пользователю доступны только один пункт меню – «Электронный замок “Витязь”» => «Сменить пароль»;

6) при нажатии клавиши [Esc] ЭЗ завершает работу и управление передается в систему.

После завершения работы ЭЗ и выхода из KSS управление передается UEFI. Далее производится поиск загрузочного устройства, считывание начального загрузчика ОС и передача ему управления, после чего производится загрузка ОС в обычном режиме.

Режимы работы Контроля целостности (КЦ) приведены в Таблица 2.1:

Таблица 2.1 – Режимы работы КЦ

Режим	Описание
Жёсткий	При обнаружении нарушения целостности объектов файловой системы выво-

Режим	Описание
	дится соответствующее сообщение, добавляется запись в журнал регистрации событий, дальнейшая загрузка компьютера блокируется - только для пользователя.
Мягкий	При обнаружении нарушения целостности выводится соответствующее сообщение, добавляется запись в журнал регистрации событий, но дальнейшая загрузка компьютера не блокируется - только для администратора.

2.4 Связи программы с другими программами

Выгрузка отчета о состоянии ЭЗ и журнала событий производится при помощи утилиты ЭЗ, после аутентификации пользователя в ЭЗ с ролью *администратора*. Выгрузка отчета и журнала из ЭЗ, а также генерация сводной информации представляют собой считывание данных из определенных секций памяти SPI Flash, их интерпретацию и вывод в формате JSON (англ. Java Script Object Notation) – текстовый формат обмена данными – для удобного просмотра, архивирования и мониторинга.

3 РАБОТА С ПО

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

3.1 Оболочка Kraftway Secure Shell

3.1.1 Вход в оболочку Kraftway Secure Shell

Оболочка Kraftway Secure Shell (далее по тексту: «оболочка KSS», «KSS») предназначена для создания безопасной среды функционирования и вызова модулей безопасности средства доверенной загрузки. Для входа в оболочку KSS следует:

Вариант 1. При первом запуске компьютера или при выключенном ЭЗ

1) в процессе загрузки компьютера, при появлении окна *Приглашение на вход в KSS* (см. Рисунок 3.1). Нажмите → [F1] на клавиатуре для входа в оболочку KSS, после выполнения данного действия на экран выводится страница Kraftway Secure Shell (см. Рисунок 3.2);

Рисунок 3.1 – Приглашение на вход в KSS

Вариант 2. При включенном ЭЗ.

1) пройти процедуру аутентификации в ЭЗ (см. п. 3.5);

2) при появлении окна *Приглашение на вход в KSS* (см. Рисунок 3.1) → [F1] на клавиатуре для входа в KSS, после выполнения данного действия на экран выводится страница *Kraftway Secure Shell* (см. Рисунок 3.2);

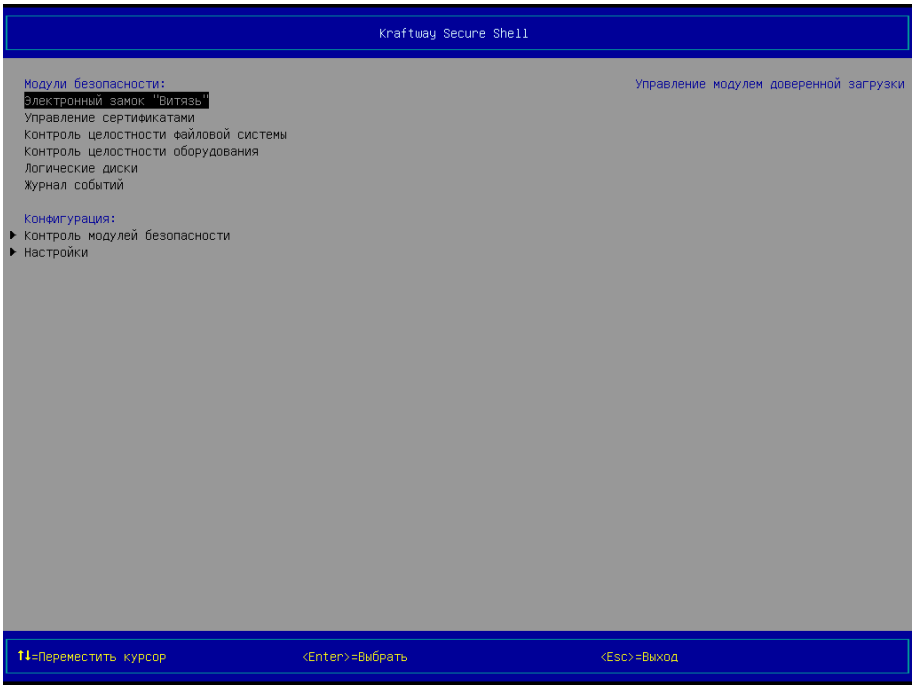


Рисунок 3.2 – Вид страницы Kraftway Secure Shell,
Главное меню оболочки

Примечания:

1. Если ранее не было выполнено никаких настроек в ЭЗ, то сразу же после отображения Logo-изображения материнской платы (см. Рисунок 3.38) администратору предлагается дождаться начала загрузки ОС или войти в оболочку Kraftway Secure Shell (см. Рисунок 3.1).

2. Все дальнейшие операции, связанные с ЭЗ, сертификатами пользователей и КЦ файловой системы, доступны администратору только после включения соответствующих модулей безопасности: *Электронный замок “Витязь”*, *Управление сертификатами*,

Контроль целостности файловой системы, Контроль целостности оборудования, Логические диски, Журнал событий, Управление обновлениями.

3.1.2 Выход из оболочки Kraftway Secure Shell

Для выхода из оболочки KSS следует:

1) перейти в главное меню оболочки KSS (см. Рисунок 3.2);

2) → [Esc] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.3), запрашивающее подтверждение на выход из оболочки KSS;

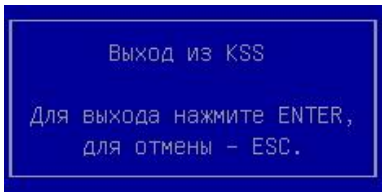


Рисунок 3.3 – Запрос подтверждения на выход из оболочки KSS

3) → [Enter] на клавиатуре, после выполнения данного действия, администратору предлагается дождаться загрузки ОС.

Примечание. При выходе из оболочки KSS осуществляется очистка оперативной памяти от остаточной информации работы KSS.

3.1.3 Описание интерфейса оболочки Kraftway Secure Shell

Интерфейс оболочки KSS, представленный на Рисунок 3.4, состоит из следующих элементов: область № 1 для отображения названия пункта/подпункта меню, область № 2 – для отображения пунктов/подпунктов меню, дополнительной или справочной информации, область № 3 – для отображения подсказок.

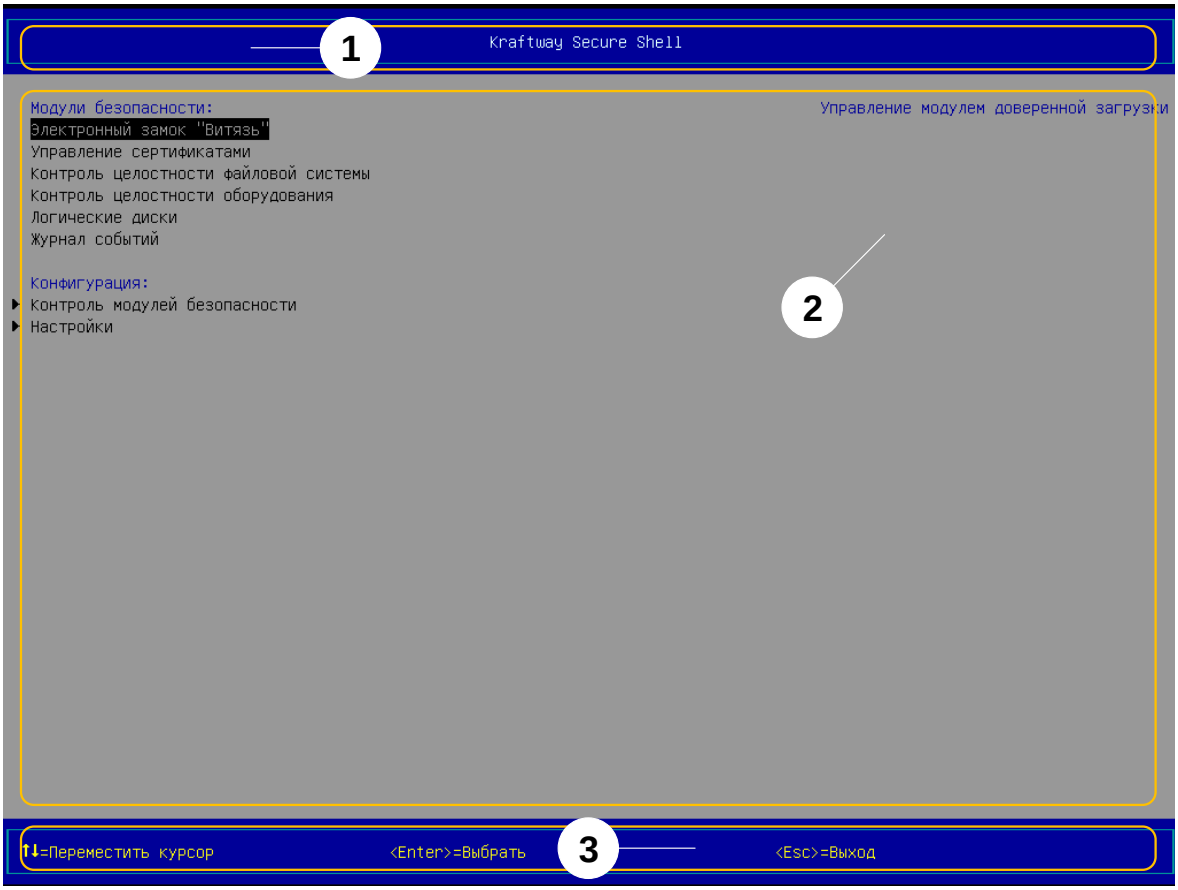


Рисунок 3.4 – Элементы оболочки KSS

Область № 1 предназначена для вывода названий пунктов или подпунктов меню оболочки KSS, которые, в свою очередь, являются ещё и названиями страниц оболочки KSS. Страница оболочки KSS – это область, которая состоит из всех областей, представленных на Рисунок 3.4.

В области № 2 выводятся:

- в левой её части пункты и подпункты меню KSS;
- в правой её части дополнительная информация о выбранном пункте/подпункте меню или справочная информация о выбранном пункте/подпункте (параметре) из левой части данной области;
- результаты проверок КЦ объектов, отчёт о состоянии ЭЗ (вывод информации выполняется почти на всю область).

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

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

Главное меню оболочки KSS состоит из двух основных разделов и пунктов:

– Модули безопасности:
  – Электронный замок «Витязь» (см. пункт 3.4);
  – Управление сертификатами (см. пункт 3.8);
  – Контроль целостности файловой системы (см. пункт 3.9);
  – Контроль целостности оборудования (см. пункт 3.10);
  – Логические диски (см. пункт 3.11);
  – Журнал событий (см. пункт 3.12);
– Конфигурация (см. пункт 3.2):
  – Контроль модулей безопасности;
  – Настройки.

3.2 Конфигурация параметров KSS

3.2.1 Установка времени ожидания для входа в KSS

Для установки времени ожидания (паузы) перед загрузкой ОС для возможности выполнения входа в KSS следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

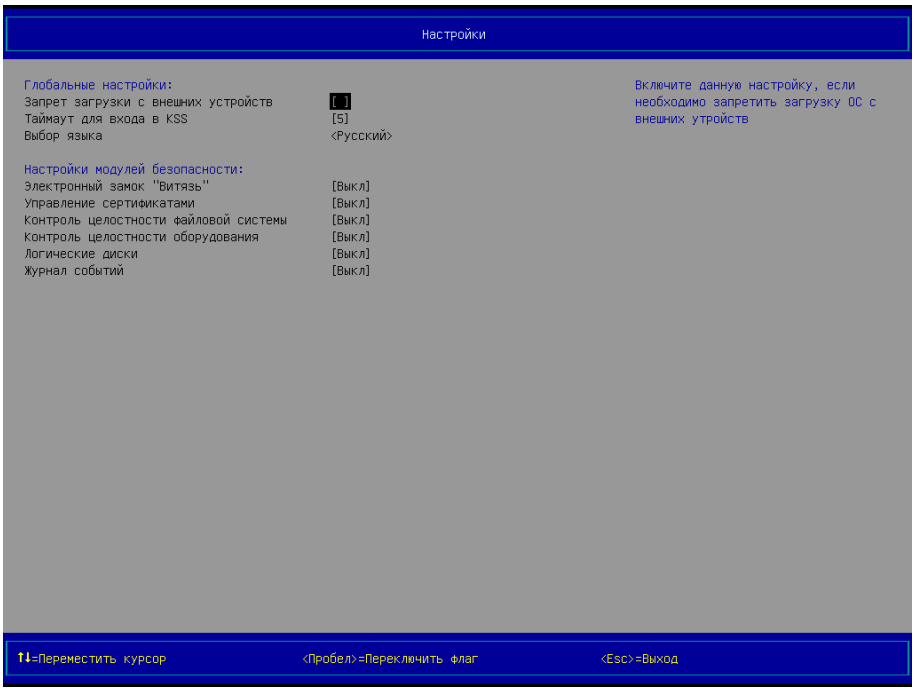


Рисунок 3.5 – Страница *Настройки* (вид 1),
все модули безопасности выключены

3) выбрать параметр *Таймаут для входа в KSS* в разделе *Глобальные настройки*;

4) → [Enter] на клавиатуре;

5) установить требуемое значение времени ожидания воспользовавшись клавишами [+]/[-], расположенных на цифровом блоке клавиатуры (допустимые значения параметра: 1-99, единица измерения – секунда).

Примечания:

1. По умолчанию значение параметра *Таймаут для входа в KSS* равно 5 (пяти).
2. Установить требуемое значение времени ожидания на странице *Настройки* также можно следующим образом:
   1) выбрать параметр *Таймаут для входа в KSS* в разделе *Глобальные настройки* (см. Рисунок 3.5);
   2) → [Enter] на клавиатуре;
   3) ввести необходимое значение времени ожидания воспользовавшись клавишами цифрового блока клавиатуры;
   4) → [Enter] на клавиатуре.

3.2.2 Изменение языка интерфейса оболочки KSS

Для изменения языка интерфейса оболочки KSS следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Выбор языка* в разделе *Глобальные настройки*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.6), предлагающее выбрать язык интерфейса оболочки KSS (доступные значения параметра: «English», «Русский»);

Рисунок 3.6 – Окно для выбора языка интерфейса KSS

5) выбрать требуемый язык интерфейса KSS в окне выбора;

6) → [Enter] на клавиатуре.

3.2.3 Запрет загрузки с внешних устройств

Для запрета загрузки ОС с внешних устройств:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Запрет загрузки с внешних устройств* в разделе *Глобальные настройки*;

4) → [Spacebar] на клавиатуре, включить запрет;

5) → [Spacebar] на клавиатуре, повторно, выключить запрет.

3.3 Конфигурация параметров замка

3.3.1 Установка максимального количества попыток аутентификации

Администратору предоставляется возможность установки максимального допустимого количества последовательных попыток аутентификации пользователя.

Под максимальным допустимым количеством последовательных попыток аутентификации пользователя следует понимать максимальное допустимое количество последовательных подключений (путем перебора) АН пользователя к USB-порту компьютера. После превышения данного количества попыток выполняется автоматическая перезагрузка компьютера.

Для установки максимального количества попыток аутентификации следует:

1) выбрать пункт *Электронный замок “Витязь”* в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.7);

Рисунок 3.7 – Страница *Электронный замок «Витязь»* (вид 2)

3) выбрать пункт *Конфигурация* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Конфигурация* (см. Рисунок 3.8);

Рисунок 3.8 – Страница *Конфигурация* (вид 1),
Максимальное количество попыток аутентификации

5) выбрать строку *Максимальное количество попыток аутентификации*;

6) установить требуемое максимально допустимое количество попыток аутентификации с помощью клавиш [+], [-], расположенных на цифровом блоке клавиатуры.

7) → [Esc] на клавиатуре, для выхода.

Примечания:

1. Установка максимального количества попыток аутентификации возможна только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. По умолчанию максимальное количество попыток аутентификации равно 7 (семи).

3. Установить максимальное количество попыток аутентификации после перехода на страницу *Конфигурация* также можно следующим образом:

   a) → [Enter] на клавиатуре;

   b) ввести необходимое значение используя цифровой блок клавиатуры (допустимые значения параметра: 0-255,

где 0 – максимальное количество попыток аутентификации не установлено);

c) → [Enter] на клавиатуре.

3.3.2 Проверка длины пароля

Администратору предоставляется возможность установки значения минимальной длины пароля пользователя.

Для установки значения минимальной длины пароля следует:

1) выбрать пункт *Электронный замок “Витязь”* в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.7);

3) выбрать пункт *Конфигурация* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Конфигурация* (см. Рисунок 3.9);

Рисунок 3.9 – Страница *Конфигурация* (вид 2), *Минимальная длина пароля*

5) выбрать строку *Минимальная длина пароля*;

6) установить требуемое значение минимальной длины пароля с помощью клавиш [+], [-], расположенных на цифровом блоке клавиатуры.

7) → [Esc] на клавиатуре, для выхода.

Примечания:

1. Установка минимальной длины пароля возможна только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).
2. Значение минимально допустимой длины пароля должно быть не меньше 4 (четырех).
3. По умолчанию минимальное значение длины пароля равно 6 (шести).
4. Установить значение минимальной длины пароля после перехода на страницу *Конфигурация* также можно следующим образом:
   a) → [Enter] на клавиатуре;
   b) ввести необходимое значение используя цифровой блок клавиатуры (допустимые значения параметра: 4-255, где 4 – значения минимальной длины пароля);
   c) → [Enter] на клавиатуре.

3.3.3 Установка длительности ожидания для ввода пароля

Для установки значения временного интервала длительности ожидания для ввода пароля:

1) выберите пункт *Электронный замок “Витязь”* в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.7);

3) выберите пункт *Конфигурация* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Конфигурация* (см. Рисунок 3.10);

Рисунок 3.10 – Страница *Конфигурация* (вид 3),
Таймаут на ввод пароля

5) выберите строку *Таймаут на ввод пароля*;

6) установите требуемое значение длительности ожидания ввода пароля с помощью клавиш на цифровом блоке клавиатуры.

7) → [Esc] на клавиатуре, для выхода.

Примечания:

1. Установка значения времени таймаута на ввод пароля возможна только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. По умолчанию значение длительности ожидания равно 60 секундам.

3. По истечении срока отведенного для ввода пароля, в случае, если пароль не будет введен, откроется окно сообщения «Превышено время ввода пароля» (см. Рисунок 3.11). Это событие будет засчитано как неудачная попытка аутентификации.

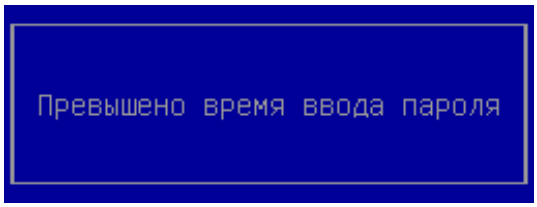


Рисунок 3.11 – сообщение «Превышено время ввода пароля»

4. Информация о изменении длительности ожидания записывается в Журнал событий.

3.4 Модуль безопасности *Электронный замок “Витязь”*

Внимание! ЭЗ начнет выполнять свои функции только после создания профиля первого администратора. Рекомендуется создать профиль первого администратора сразу же после включения ЭЗ для дальнейшей работы в нём (см. п. 3.5.1).

3.4.1 Включение ЭЗ. Метод 1

Для включения ЭЗ в первый раз или после выключения ЭЗ с очисткой всех данных следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Электронный замок “Витязь”* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”*: *Настройки* с одним пунктом: *Включить электронный замок* (см. Рисунок 3.12);

Рисунок 3.12 – Страница *Электронный замок “Витязь”: Настройки* (вид 1), пункт *Включить электронный замок*

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.13), запрашивающее подтверждение на включение ЭЗ;

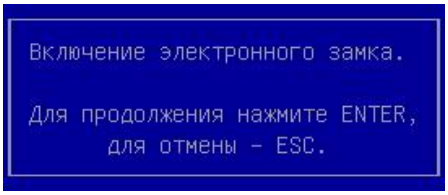


Рисунок 3.13 – Диалоговое окно, запрашивающее подтверждение на включение ЭЗ

6) → [Enter] на клавиатуре, после выполнения этого действия на экран выводится страница *Лицензионное соглашение* (см. Рисунок 3.14);

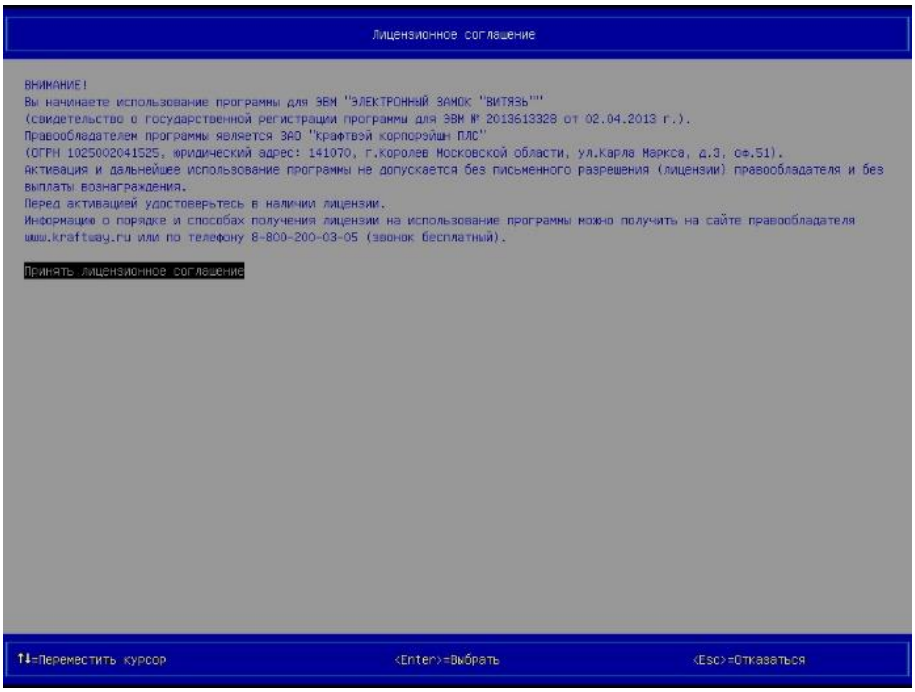


Рисунок 3.14 – Страница *Лицензионное соглашение*,
пункт *Принять лицензионное соглашение* выбран по умолчанию

7) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: Настройки* (см. Рисунок 3.15);

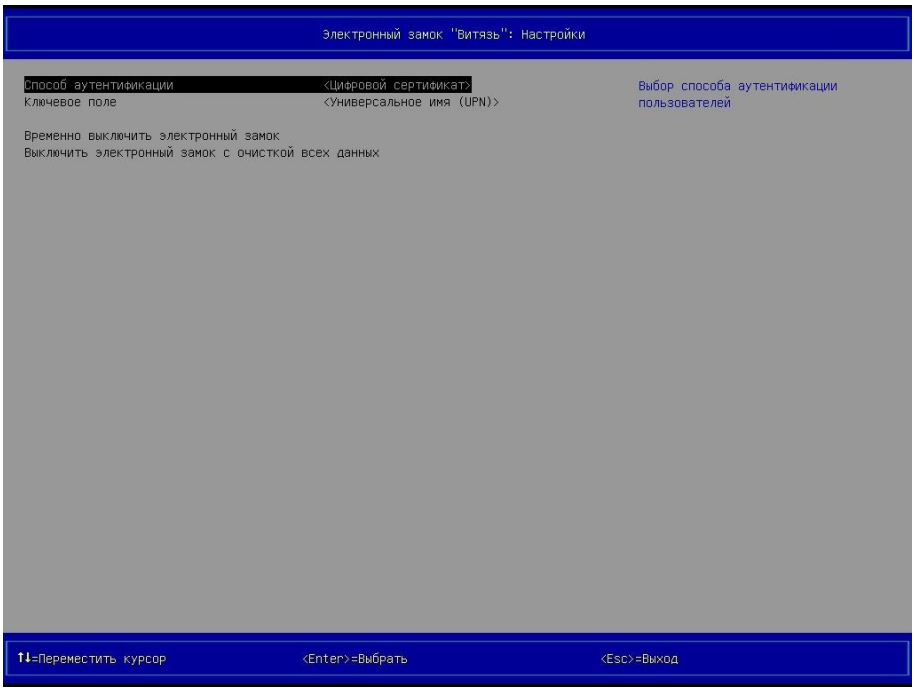


Рисунок 3.15 – Страница *Электронный замок “Витязь”: Настройки* (вид 2), *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — «Универсальное имя (UPN)»

8) выбрать пункт *Способ аутентификации*;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.16), предлагающее выбрать способ аутентификации пользователя (доступные значения параметра: «Цифровой сертификат», «Электронный ключ», «Цифровой сертификат и электронный ключ»);

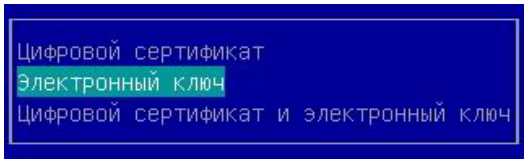


Рисунок 3.16 – Окно для выбора способа аутентификации пользователя

10) выбрать требуемый способ аутентификации в окне выбора;

11) → [Enter] на клавиатуре;

12) выбрать пункт *Ключевое поле* (см. Рисунок 3.15, данный пункт выполняется только, если параметру *Способ аутентификации* было назначено одно из двух следующих значений: «Цифровой сертификат», «Цифровой сертификат и электронный ключ»);

13) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.17), 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»);

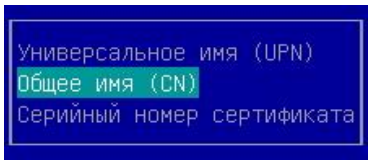


Рисунок 3.17 – Окно для выбора ключевого поля сертификата пользователя

14) → [Enter] на клавиатуре.

Примечания:

1. При попытке назначения параметрам: *Способ аутентификации Ключевое поле* новых значений, на экран выводится окно (см. Рисунок 3.18), запрашивающее подтверждение на внесение изменений.

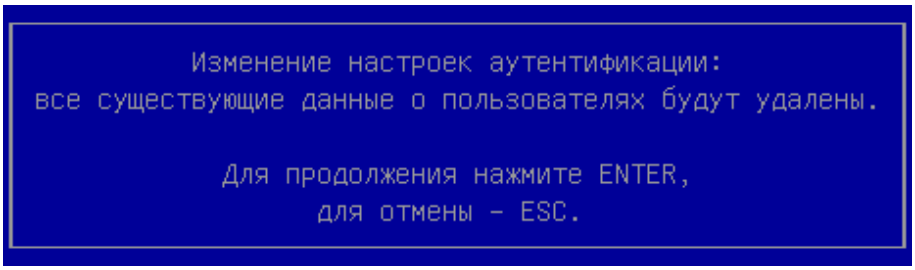


Рисунок 3.18 – Запрос подтверждения на внесение изменений

2. Пункт *Ключевое поле* не выводится на странице *Электронный замок “Витязь”: Настройки* (см. Рисунок 3.19), если параметру *Способ аутентификации* было присвоено значение «Электронный ключ».

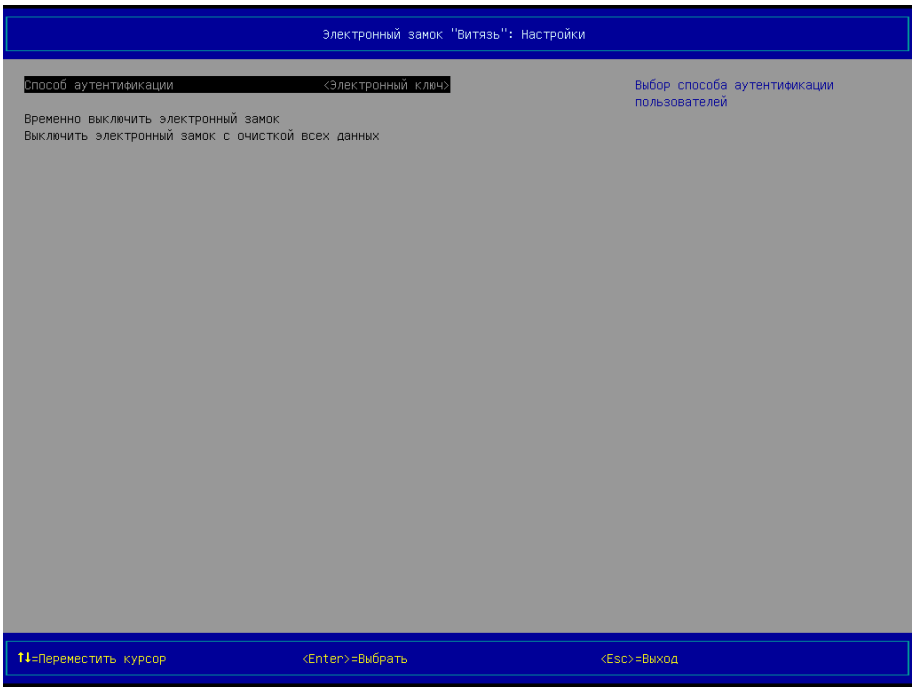


Рисунок 3.19 – Страница *Электронный замок “Витязь”: Настройки* (вид 3), *Способ аутентификации* – «Электронный ключ»

3. После включения ЭЗ статус модуля безопасности *Электронный замок “Витязь”* меняется с «Выкл» на «Вкл» на странице *Настройки* (см. Рисунок 3.20).

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

3.4.2 Включение ЭЗ. Метод 2

Для включения ЭЗ после временного его выключения следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Электронный замок “Витязь”* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: Настройки* с одним пунктом для включения ЭЗ (см. Рисунок 3.12);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.13), запрашивающее подтверждение на включение ЭЗ;

6) → [Enter] на клавиатуре, после выполнения этого действия на экран выводится страница *Локальная аутентификация* (см. Рисунок 3.40), в которой администратору предлагается подключить АН к свободному USB-порту персонального компьютера;

7) для прохождения аутентификации выполнить:

а) действия 3-5 п. 3.5.2, если до временного выключения ЭЗ в его настройках был выбран способ аутентификации пользователя по электронному ключу;

б) действия 3-8 п. 3.5.3, если до временного выключения ЭЗ в его настройках был выбран способ аутентификации пользователя по цифровому сертификату или цифровому сертификату и электронному ключу;

8) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Лицензионное соглашение* (см. Рисунок 3.14);

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: Настройки* (см. Рисунок 3.15);

10) выполнить действия 8-14 п. 3.4.1, при необходимости.

Примечание. После включения ЭЗ статус модуля безопасности *Электронный замок “Витязь”* меняется с «Выкл» на «Вкл» на странице *Настройки* (см. Рисунок 3.20).

3.4.3 Выключение ЭЗ с очисткой всех данных

Для выключения ЭЗ с очисткой всех данных следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

Рисунок 3.20 – Страница *Настройки* (вид 2),
все модули безопасности включены

3) выбрать пункт *Электронный замок “Витязь”* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: Настройки* (см. Рисунок 3.15, Рисунок 3.19);

5) выбрать пункт *Выключить электронный замок с очисткой всех данных*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.21), запрашивающее подтверждение на выключение ЭЗ с очисткой всех данных;

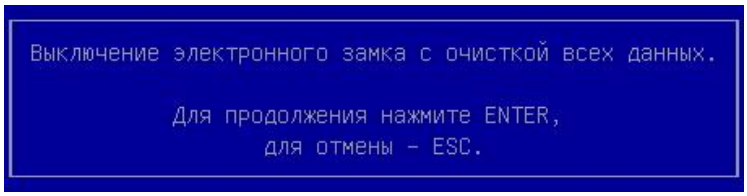


Рисунок 3.21 – Запрос подтверждения на выключение ЭЗ
с очисткой всех данных

7) → [Enter] на клавиатуре, после выполнения данного действия происходит выключение ЭЗ с удалением ранее введённых данных (информация о пользователях, жур-

нал событий ЭЗ), параметрам настроек присваиваются значения по умолчанию, на экран выводится страница *Настройки*, статус модуля безопасности меняется с «Вкл» на «Выкл», (см. Рисунок 3.20).

3.4.4 Временное выключение ЭЗ

Для выключения ЭЗ без очистки всех данных следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Электронный замок "Витязь"* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок "Витязь": Настройки* (см. Рисунок 3.15, Рисунок 3.19);

5) выбрать пункт *Временно выключить электронный замок*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.22), запрашивающее подтверждение на выключение ЭЗ;

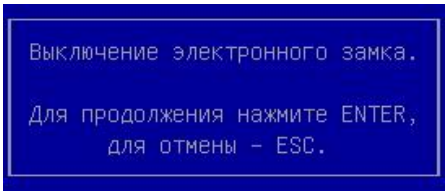


Рисунок 3.22 – Запрос подтверждения на выключение ЭЗ

7) → [Enter] на клавиатуре, после выполнения данного действия происходит выключение ЭЗ без удаления ранее введённых данных (информация о пользователях, журнал событий ЭЗ), значения параметров настроек не изменяются на значения по умолчанию, статус модуля безопасности на странице *Настройки* меняется с «Вкл» на «Выкл», на экран выводится страница *Настройки* (см. Рисунок 3.5).

3.4.5 Просмотр Отчёта о состоянии ЭЗ

Для просмотра отчёта о состоянии ЭЗ следует:

1) выбрать пункт *Электронный замок “Витязь”* в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.7);

3) выбрать пункт *Отчет о состоянии замка* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Отчет о состоянии замка* (см. Рисунок 3.23);

Рисунок 3.23 – Страница *Отчет о состоянии замка*

5) просмотреть и проанализировать выведенную информацию.

Примечания:

1. Просмотр отчёта о состоянии ЭЗ возможен только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. Если отчёт о состоянии ЭЗ состоит из большого количества записей, которые не умещаются в области № 2 оболочки KSS, то в данной области выводятся стрелки красного

цвета: ↑ – дополнительные записи располагаются выше, ↓ – дополнительные записи располагаются ниже.

3. Перемещение по записям отчёта о состоянии ЭЗ выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре.

4. Постраничный вывод записей отчёта о состоянии ЭЗ выполняется с помощью клавиш [Page Up], [Page Down], расположенных на клавиатуре.

3.4.6 Сохранение Отчёта о состоянии ЭЗ в файл

Для сохранения отчёта о состоянии ЭЗ в файл следует:

1) выполнить действия 1-5 п. 0;

2) подключить USB-диск к свободному USB-порту компьютера;

3) → [F10] клавиатуры, после выполнения данного действия в корне USB-диска сохраняется текстовый файл *Report-dd-mm-hh-mm-ss.json* с данными о состоянии ЭЗ, где *dd* – день, *mm* – месяц, *hh* – часы, *mm* – минуты, *ss* – секунды, а на экран выводится окно (см. Рисунок 3.24), информирующее администратора об успешном сохранении отчёта о состоянии ЭЗ;

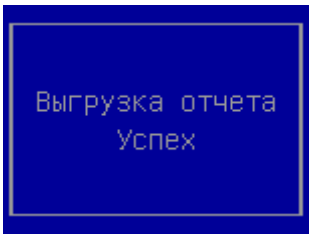


Рисунок 3.24 – Окно *Выгрузка отчета Успех*

4) нажать любую клавишу на клавиатуре.

Примечания:

1. Сохранение отчёта о состоянии ЭЗ в файл возможно только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

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 отчёта следует открыть данный файл в соответствующем текстовом редакторе.

3. При отсутствии подключенного USB-диска к компьютеру, после нажатия на клавишу [F10] на экран выводится окно (см. Рисунок 3.136), информирующее об отсутствии устройства памяти.

4. Если сохранить журнал событий в файл невозможно, то на экран выводится окно (см. Рисунок 3.137).

3.5 Аутентификация в ЭЗ

Для загрузки компьютера необходимо пройти процедуру аутентификации в ЭЗ.

В ПК ЭЗ «Витязь» В2.2 реализовано три способа аутентификации: по цифровому сертификату, по электронному ключу (серийный номер АН), по цифровому сертификату и электронному ключу (см. п. 3.4).

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» В2.2 аутентификация пользователей проводится посредством предъявления АН на этапе загрузки компьютера и дополнительного фактора.

Одному пользователю соответствует одно АН.

Для всех АН выбирается один общий способ аутентификации.

При предъявлении АН выполняется проверка наличия серийного номера АН в БД ЭЗ, в которой хранятся серийные номера АН, зарегистрированные ранее в БД.

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

В ПК ЭЗ «Витязь» В2.2 реализована аутентификация по одному из трёх факторов: по PIN-коду к АН, по ключевому полю цифрового сертификата пользователя, по PIN-коду к АН и ключевому полю цифрового сертификата пользователя. (см. Таблица 3.1)

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 ЭЗ, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы профили пользователей в ЭЗ. При данном варианте аутентификации количество попыток ввода пароля пользователя также 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 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 ЭЗ, в которой хранятся значения ключевых полей цифровых сертификатов пользователей, для которых ранее были созданы профили пользователей в ЭЗ. При данном варианте аутентификации количество попыток ввода пароля пользователя также ограничивается политикой безопасности организации.

Таблица 3.1 – Способы аутентификации

	Вариант аутентификации	Ключевое поле по выбору	Фактор аутентификации	Действие
1	Цифровой сертификат	Универсальное имя (UPN) Общее имя (CN) Серийный номер сертификата	Пароль + выбор сертификата	Проверка ключевого поля
2	Электронный ключ		Пароль	Проверка s/n ключа
3	Цифровой сертификат и электронный ключ	Универсальное имя (UPN) Общее имя (CN) Серийный номер сертификата	Пароль + выбор сертификата	Проверка ключевого поля + 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 ЭЗ, UEFI и выполняется в соответствии с ролевой моделью, описанной в п. 1.6.

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

Далее по тексту приводится описание процедуры аутентификации с различными вариантами аутентификации.

3.5.1 Создание профиля первого администратора

После входа в оболочку KSS и первого включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4) пользователю предоставляются права администратора. В ЭЗ изначально профиль администратора не создан. Только после создания профиля первого администратора можно: создавать профили новых пользователей, изменять профили пользователей, блокировать, 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.

В данном подразделе описывается создание профиля первого администратора при следующих настройках ЭЗ: *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.

Для создания профиля первого администратора следует:

1) выбрать пункт *Электронный замок “Витязь”* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.25);

Рисунок 3.25 – Страница *Электронный замок “Витязь”* (вид 2), до создания первого администратора

3) выбрать пункт *Список пользователей* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”: список пользователей* (см. Рисунок 3.26), на которой предлагается создать профиль нового пользователя;

Рисунок 3.26 – Страница *Электронный замок “Витязь”: список пользователей* (вид 5), профили пользователей ещё не создавались

5) выбрать пункт *Создать профиль нового пользователя* в разделе *Управление пользователями*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран вводится диалоговое окно (см. Рисунок 3.27), предлагающее администратору выбрать одно из следующих действий:

a. использовать АН пользователя при создании профиля администратора;

b. вручную - не использовать АН пользователя при создании профиля администратора;

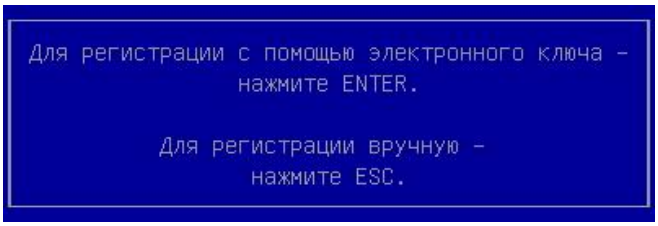


Рисунок 3.27 – Вид диалогового окна для выбора использования АН пользователя при создании профиля пользователя

7) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.28), предлагающее подключить АН пользователя к свободному USB-порту компьютера;

Рисунок 3.28 – Приглашение на подключение АН пользователя

8) подключить АН первого администратора к свободному USB-порту компьютера;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно для ввода пароля пользователя (см. Рисунок 3.29);

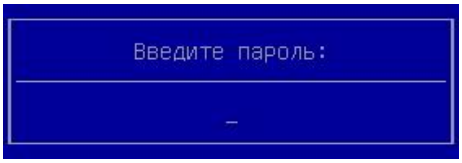


Рисунок 3.29 – Окно для ввода пароля пользователя

10) ввести пароль администратора в окне ввода;

11) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно, информирующее о поиске сертификатов пользователей, после завершения процесса поиска сертификатов пользователей на экран выводится окно (см. Рисунок 3.30), в котором администратору предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов;

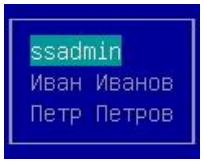


Рисунок 3.30 – Выбор значения ключевого поля *Общее имя (CN)*

12) выбрать нужное значение в окне выбора;

13) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: создание нового профиля пользователя* (см. Рисунок 3.31);

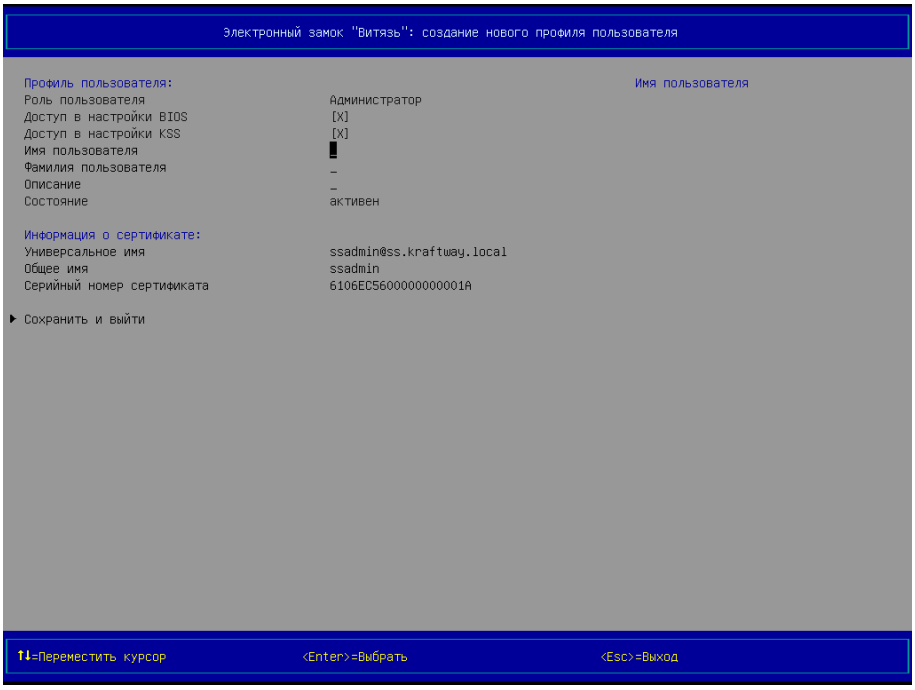


Рисунок 3.31 – Страница *Электронный замок “Витязь”: создание нового профиля пользователя* (вид 1)

14) выбрать параметр *Имя пользователя*;

15) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.32), предлагающее ввести имя пользователя;

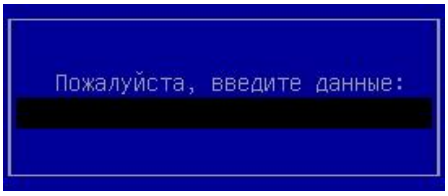


Рисунок 3.32 – Окно для ввода разного рода данных

16) ввести имя администратора;

17) → [Enter] на клавиатуре;

18) выбрать параметр *Фамилия пользователя*;

19) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.32), предлагающее ввести фамилию пользователя;

20) ввести фамилию администратора;

21) → [Enter] на клавиатуре;

22) выбрать параметр *Описание*;

23) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.33) для ввода описания пользователя;

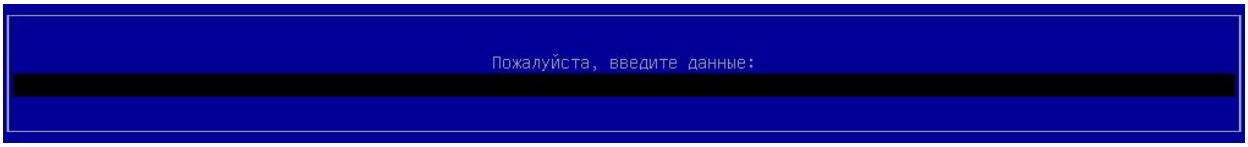


Рисунок 3.33 – Окно для ввода описания пользователя

24) ввести описание администратора;

25) → [Enter] на клавиатуре;

26) выбрать пункт *Сохранить и выйти*;

27) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”: список пользователей* (см. Рисунок 3.34), на которой появился первый созданный пользователь и предлагается создать профиль нового пользователя;

Рисунок 3.34 – Страница *Электронный замок “Витязь”: список пользователей* (вид 6), профиль пользователя создан

Примечания:

1. Создание профиля первого администратора возможно только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. Если при создании профиля первого администратора было принято решение о создании данного профиля без использования АН администратора, т.е. была нажата клавиша [ESC] на клавиатуре (см. Рисунок 3.27), то тогда создание профиля первого администратора продолжается на странице *Электронный замок “Витязь”: создание нового профиля пользователя* (см. Рисунок 3.35). 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.

Рисунок 3.35 – Страница *Электронный замок “Витязь”: создание нового профиля пользователя* (вид 2)

3. Администратору следует быть предельно внимательным при вводе PIN-кода к АН. При инициализации (форматировании) АН с помощью программного обеспечения,

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 ЭЗ. Превышение данного количества попыток ввода PIN-кода к АН приводит к блокировке этого АН на аппаратном уровне и к необходимости его повторной инициализации (форматированию).

4. Изменение языка ввода с английского на русский и наоборот выполняется с помощью клавиши [F9] клавиатуры.

5. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Электронный ключ» – администратору не предлагается выбрать значение ключевого поля сертификата, и он не выполняет пункты 11, 12 последовательности действий, описанной в п. 3.5.1.

6. При следующих настройках ЭЗ: *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 11 п. 3.5.1), администратору предлагается выбрать универсальное имя из списка (см. Рисунок 3.36).

Рисунок 3.36 – Окно для выбора универсального имени из списка

7. При следующих настройках ЭЗ: *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 11 п. 3.5.1), администратору предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. Рисунок 3.37).

Рисунок 3.37 – Окно для выбора серийного номера сертификата из списка

8. 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. Рисунок 3.31, Рисунок 3.35). Таким образом, администратор, для которого был создан профиль первого администратора, всегда имеет доступ к настройкам BIOS материнской платы и к настройкам оболочки KSS.

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

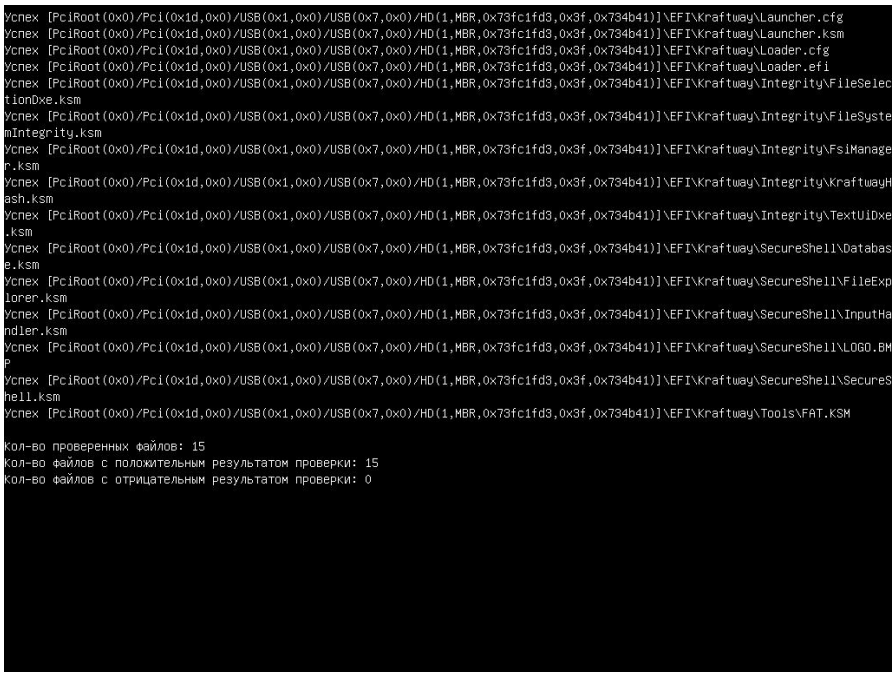
3.5.2 Прохождение аутентификации (вариант 1)

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

Для прохождения аутентификации следует:

1) включите персональный компьютер, после выполнения данного действия на экране монитора отображается Logo-изображение материнской платы компьютера (см. Рисунок 3.38), после этого запускаются Модули ЭЗ. Процесс проверки КЦ виден на экране (см. Рисунок 3.39);

Рисунок 3.38 – Logo-изображение материнской платы компьютера



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

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

Рисунок 3.39 – Процесс проверки КЦ Модулями ЭЗ

2) после окончания процесса КЦ объектов пользователю предлагается подключить АН к свободному USB-порту персонального компьютера (см. Рисунок 3.40);

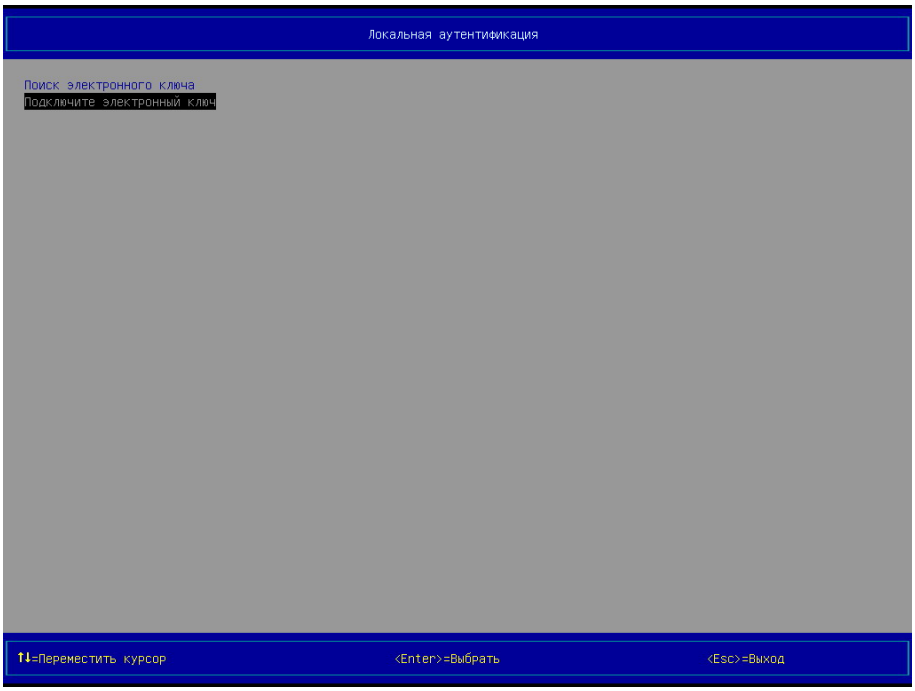


Рисунок 3.40 – Страница *Локальная аутентификация* (вид 1), предложение на подключение АН

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

4) после обнаружения системой подключенного АН предлагается ввести пароль (см. Рисунок 3.41);

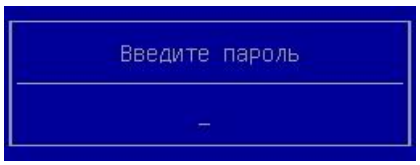


Рисунок 3.41 – Предложение ввода пароля пользователя

5) введите пароль пользователя;

6) → [Enter] на клавиатуре, после выполнения данного действия и успешной аутентификации пользователя, предлагается дождаться загрузки ОС или войти в оболочку Kraftway Secure Shell → [F1] (см. Рисунок 3.42).

Рисунок 3.42 – Приглашение на вход в KSS

Примечание. Процесс аутентификации пользователя выполняется после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

3.5.3 Прохождение аутентификации (вариант 2)

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

Для прохождения аутентификации:

1) включите персональный компьютер, после выполнения данного действия на экране монитора отображается Logo-изображение материнской платы компьютера (см. Рисунок 3.38), после этого запускаются Модули КЦ ЭЗ. Процесс проверки КЦ виден на экране (см. Рисунок 3.39);

2) после окончания процесса КЦ объектов пользователю предлагается подключить АН к свободному USB-порту персонального компьютера (см. Рисунок 3.40);

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

4) после обнаружении системой подключенного АН пользователю предлагается ввести пароль (см. Рисунок 3.41);

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

5) введите пароль пользователя;

6) → [Enter] на клавиатуре, после выполнения данного действия осуществляется поиск сертификатов пользователей, расположенных на АН, во время поиска сертификатов на экран выводится окно следующего вида (см. Рисунок 3.43);

Рисунок 3.43 – Окно, информирующее о поиске сертификатов

7) после завершения поиска сертификатов пользователю предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов на странице *Локальная аутентификации* (см. Рисунок 3.44);

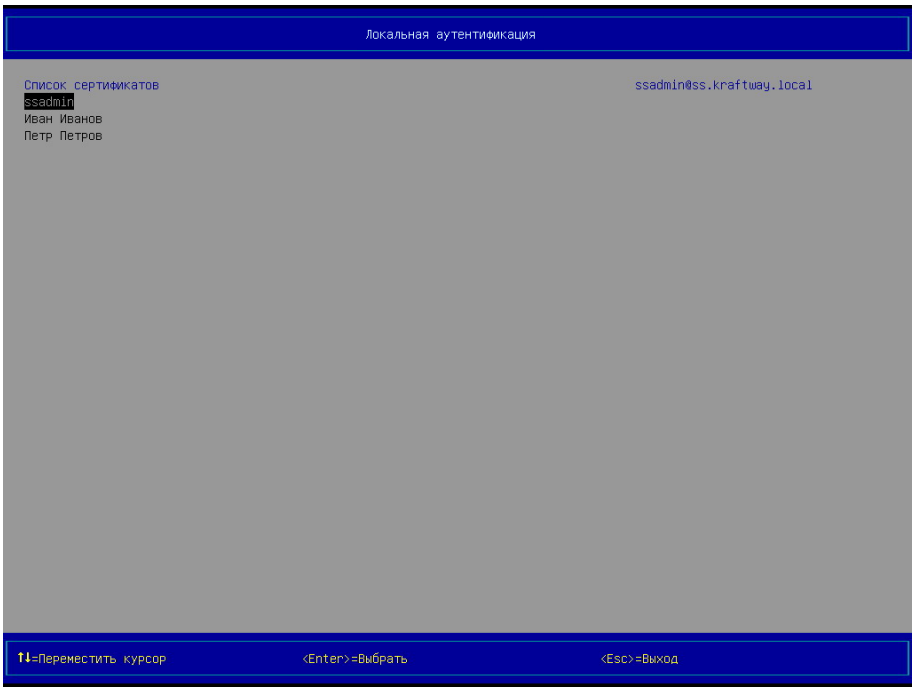


Рисунок 3.44 – Страница *Локальная аутентификация* (вид 2), выбор значения ключевого поля *Общее имя (CN)* из списка сертификатов пользователя

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

9) → [Enter] на клавиатуре, после выполнения данного действия и успешной аутентификации, пользователю предлагается дождаться загрузки ОС или войти в оболочку Kraftway Secure Shell → [F1] (см. Рисунок 3.42).

Примечания:

1. Процесс аутентификации пользователя выполняется после включения модуля безопасности *Электронный замок “Витязь”* (см. п.3.4).

2. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)», – после завершения поиска сертификатов, пользователю предлагается выбрать универсальное имя из списка (см. Рисунок 3.45).

Рисунок 3.45 – Страница *Локальная аутентификация* (вид 3), выбор универсального имени сертификата

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата», – после завершения поиска сертификатов, пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. Рисунок 3.46).

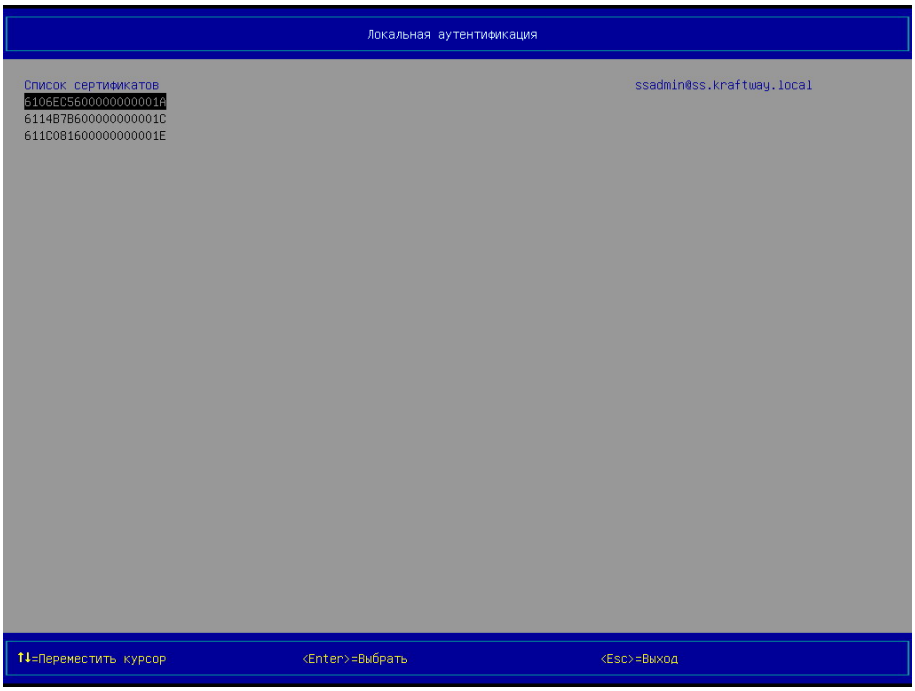


Рисунок 3.46 – Страница *Локальная аутентификация* (вид 4), выбор серийного номера сертификата

3.5.4 Прохождение аутентификации (вариант 3)

В данном пункте описывается прохождение аутентификации пользователем при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Общее имя (CN)».

Для прохождения аутентификации следует выполнить действия, описанные в пункте 3.5.3.

Примечания:

1. Процесс аутентификации пользователя выполняется после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», – после завершения поиска сертификатов, пользователю предлагается выбрать универсальное имя из списка (см. Рисунок 3.45).

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – «Се-

рийный номер сертификата», — после завершения поиска сертификатов, пользователю предлагается выбрать требуемый серийный номер одного из найденных сертификатов (см. Рисунок 3.46).

3.5.5 Дополнительные сведения о процедуре аутентификации в ЭЗ

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:

– 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 ЭЗ больше будет невозможно.

2. Аутентификация пользователей без сертификата УЦ

Аутентификация пользователей без сертификата допустима. Но так как добавление сертификата влечет выключение замка, то добавление некорректного УЦ влечет за собой отсутствие возможности включить модуль замка.

Отсутствие УЦ небезопасно, но Аутентификация пользователей возможна.

При добавлении пользователя без УЦ выводится два сообщения:

1) Сообщение для подтверждения добавления пользователя по сертификату не прошедшему КРИПТОГРАФИЧЕСКУЮ проверку (т.к. сертификата УЦ нет, то и проверку пройти не получится).

2) Сообщение с предупреждением, о том, что нет сертификатов УЦ и это небезопасно, хотя возможно.

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

3. Аутентификация пользователей с сертификатом УЦ

Если ранее в ЭЗ администратором был добавлен сертификат удостоверяющего центра (УЦ) (см. п. 3.8.3), 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 Kraftway Secure Shell (см. Рисунок 3.42).

4. Особенности работы с картами Микрон.

В картах Микрон ПИН, если ранее не меняли, может быть задан в шестнадцатиричном представлении, что не позволяет ввести в замке. И в этом случае ПИН нужно сменить, используя стороннюю программу Smart Card Shell, скачать можно тут : http://www.openscdp.org/scsh3/ .

Существуют два вида карт Микрон, с объектами 0x0B и 0x07:
card.sendApdu(0x00, 0x20, 0x00, 0x0B, new ByteString("949D1257815C6C64", HEX));
card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("0E2FC22362BCBC7D", HEX));
,где 949D1257815C6C64 – заводской пин карты.

Алгоритм Смена ПИН (для ПИН объекта 0x07, аналогично для 0x0B):

```
// Проверить, что заводской ПИН подходит
card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("0E2FC22362BCBC7D", HEX));
// Сменить на «12345678»
card.sendApdu(0x00, 0x24, 0x00, 0x07, new
ByteString("0E2FC22362BCBC7D3132333435363738", HEX));
// Проверить новый ПИН «12345678»
card.sendApdu(0x00, 0x20, 0x00, 0x07, new ByteString("3132333435363738", HEX));
```

Примечание. Результат проверки сертификата пользователя на подлинность считается положительным, если сертификат пользователя, размещённый в защищённой области АН, был подписан с помощью сертификата УЦ, а данный сертификат УЦ, в свою очередь, был добавлен в ЭЗ (см. п. 3.8.3).

Результат проверки сертификата пользователя на подлинность считается отрицательным, если:

а) сертификат пользователя, размещённый в защищённой области АН, был подписан с помощью сертификата УЦ, который не был добавлен в ЭЗ (см. п. 3.8.3);

б) сертификат пользователя, размещённый в защищённой области АН, не был подписан с помощью какого-либо сертификата УЦ, а является самозаверенным сертификатом.

3.6 Работа со списком пользователей

3.6.1 Просмотр списка пользователей

Для просмотра списка пользователей следует:

1) выбрать пункт *Электронный замок “Витязь”* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.47);

Рисунок 3.47 – Страница *Электронный замок “Витязь”* (вид 1), после создания первого администратора

3) выбрать пункт *Список пользователей* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”: список пользователей* (см. рисунки 3.48 - 3.51), на которой представлен список профилей пользователей;

Рисунок 3.48 – Страница *Электронный замок “Витязь”: список пользователей* (вид 1), созданы профили пользователей, *Способ аутентификации* — «Электронный ключ»

Рисунок 3.49 – Страница *Электронный замок “Витязь”: список пользователей* (вид 2), созданы профили пользователей, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — «Общее имя (CN)»

Рисунок 3.50 – Страница *Электронный замок “Витязь”: список пользователей* (вид 3), созданы профили пользователей, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* — «Универсальное имя (UPN)»

Рисунок 3.51 – Страница *Электронный замок “Витязь”: список пользователей* (вид 4), созданы профили пользователей, *Способ аутентификации* — «Цифровой сертификат», *Ключевое поле* – «Серийный номер сертификата»

Примечания:

1. Просмотр списка пользователей возможен только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4), создания хотя бы одного профиля пользователя.

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

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата» – страница *Электронный замок “Витязь”: список пользователей*, практически аналогична тем, страницам, что представлены на рисунках 3.49 - 3.51, когда параметру ЭЗ *Способ аутентификации* присвоено значение «Цифровой сертификат». Разница заключается только в выводе дополнительных сведений о профиле пользователя (*идентификатор электронного ключа*, *название электронного ключа*) в правой части области № 2 данной страницы. Т.е. представление дополнительной информации о профиле пользователя в правой части области № 2 страницы *Электронный замок “Витязь”: список пользователей* идентичен представлению дополнительной информации при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Электронный ключ» (см. Рисунок 3.48).

3.6.2 Создание профиля нового пользователя

Процедура создания профиля нового пользователя практически идентична процедуре создания профиля первого администратора (см. п. 3.5.1). При создании профиля нового пользователя можно присваивать значения параметру *Роль пользователя* (см. рисунки 3.31, 3.35).

В данном подразделе описывается создание профиля пользователя при следующих настройках ЭЗ: *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 (см. Рисунок 3.27).

Для создания профиля нового пользователя следует:

1) выбрать пункт *Электронный замок “Витязь”* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.47);

3) выбрать пункт *Список пользователей* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”: список пользователей* (см. Рисунок 3.52), на которой предлагается создать профиль нового пользователя;

Рисунок 3.52 – Страница *Электронный замок “Витязь”: список пользователей* (вид 6), создан профиль первого администратора

5) выбрать пункт *Создать профиль нового пользователя* в разделе *Управление пользователями*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран вводится диалоговое окно (см. Рисунок 3.27), предлагающее администратору выбрать одно из следующих действий: использовать АН пользователя при создании профиля пользователя, не использовать АН пользователя при создании профиля пользователя;

7) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.28), предлагающее подключить АН пользователя к свободному USB-порту компьютера;

8) подключить АН пользователя, для которого создаётся профиль, к свободному USB-порту компьютера;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно для ввода пароля пользователя (см. Рисунок 3.29);

10) ввести пароль пользователя;

11) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.43), информирующее о чтении списка сертификатов пользователей, после завершения чтения списка сертификатов на экран выводится окно (см. Рисунок 3.30), в котором администратору предлагается выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов;

12) выбрать нужное значение;

13) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: создание нового профиля пользователя* (см. Рисунок 3.53);

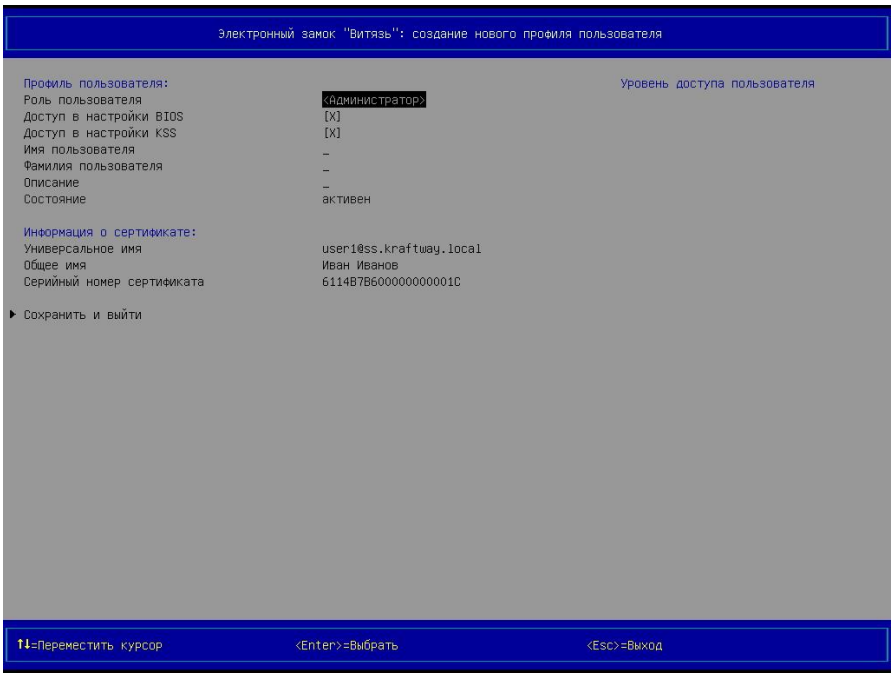


Рисунок 3.53 – Страница *Электронный замок “Витязь”: создание нового профиля пользователя* (вид 3)

14) выбрать параметр *Роль пользователя*;

15) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.54), предлагающее выбрать роль пользователя;

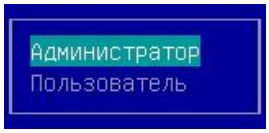


Рисунок 3.54 – Окно для выбора роли пользователя

16) выбрать требуемую роль пользователя;

17) → [Enter] на клавиатуре;

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

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

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

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

Примечание. Если на этом этапе создания нового профиля пользователя выбрать пункт *Сохранить и выйти*, то откроется окно предупреждения с текстом «Недостаточно информации». Необходимо ввести дополнительную информацию о пользователе (см. Рисунок 3.55).

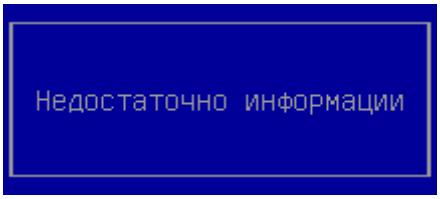


Рисунок 3.55 – Окно предупреждение

22) выберите параметр *Имя пользователя*;

23) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.32), предлагающее ввести имя пользователя;

24) введите имя пользователя;

25) → [Enter] на клавиатуре;

26) выберите параметр *Фамилия пользователя*;

27) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.32), предлагающее ввести фамилию пользователя;

28) введите фамилию пользователя;

29) → [Enter] на клавиатуре;

30) выберите параметр *Описание*;

31) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.33) для ввода описания пользователя;

32) введите описание пользователя;

33) → [Enter] на клавиатуре;

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

35) → [Enter] на клавиатуре;

36) установите требуемое максимальное количество попыток ввода пароля с помощью клавиш, расположенных на цифровом блоке клавиатуры (допустимые значения параметра: 1-4);

37) → [Enter] на клавиатуре;

38) выберите пункт *Сохранить и выйти*;

39) → [Enter] на клавиатуре.

Примечания:

1. Создание профиля нового пользователя возможно только после включения модуля безопасности *Электронный замок "Витязь"* (см. п. 3.4), создания профиля первого администратора (см. п. 3.5.1).

2. Если при создании профиля пользователя было принято решение о создании данного профиля без использования АН, т.е. была нажата клавиша [ESC] на клавиатуре (см. Рисунок 3.27), то тогда создание профиля пользователя продолжается на странице *Электронный замок "Витязь": создание нового профиля пользователя* (см. Рисунок 3.35). При создании профиля пользователя 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 окнах, которые практически аналогичны тем, что представлены на рисунках 3.32, 3.22, отличаются только размерами.

3. Администратору следует быть предельно внимательным при вводе PIN-кода к АН. При инициализации (форматировании) АН с помощью программного обеспечения, 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 задаётся в программном обеспечении, поставляемом с АН, и не имеет ничего общего со значением параметра ЭЗ *Максимальное количество попыток ввода пароля*, которое присваивается данному параметру при создании профиля нового пользователя. Следует избегать ситуации, когда максимальное количество попыток ввода PIN-кода и значение, присваиваемое параметру ЭЗ *Максимальное количество попыток ввода пароля*, совпа-

дают, т.к. при превышении значения любого из данных параметров (максимальное количество попыток ввода PIN-кода, *Максимальное количество попыток ввода пароля*) электронным замком будет заблокирован профиль пользователя и заблокирован АН на аппаратном уровне. Максимальное количество попыток ввода PIN-кода накладывает ограничение со стороны конкретного АН, а не ЭЗ. Превышение данного количества попыток ввода PIN-кода к АН приводит к блокировке этого АН на аппаратном уровне и к необходимости его повторной инициализации (форматированию).

4. Изменение языка ввода с английского на русский и наоборот выполняется с помощью клавиши [F9] клавиатуры.

5. При следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Электронный ключ» – администратору не предлагается выбрать значение ключевого поля сертификата, и он не выполняет пункты 11, 12 последовательности действий, описанной в п. 3.6.

6. При следующих настройках ЭЗ: *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. Рисунок 3.36).

7. При следующих настройках ЭЗ: *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. Рисунок 3.37).

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

9. При создании профиля администратора (профиля пользователя с ролью *Администратор*) параметр *Максимальное количество попыток ввода пароля* отсутствует на странице *Электронный замок 'Витязь': создание профиля нового пользователя* (см. рисунки 3.31, 3.35, 3.53), а при создании профиля пользователя данный параметр присутствует (см. Рисунок 3.56), т.к. на администраторов ЭЗ не накладывается ограничение ЭЗ относительно максимального количества попыток ввода пароля. Ограничение относительно максимального количества попыток ввода пароля накладывается на администраторов ЭЗ только со стороны используемого АН. Данное количество устанавливается при

инициализации АН с помощью программного обеспечения, идущего в комплекте с АН, и определённо в эксплуатационной документации на АН.

10. Общее количество пользователей, созданных в ЭЗ, зависит от свободного объёма памяти на микросхеме SPI Flash.

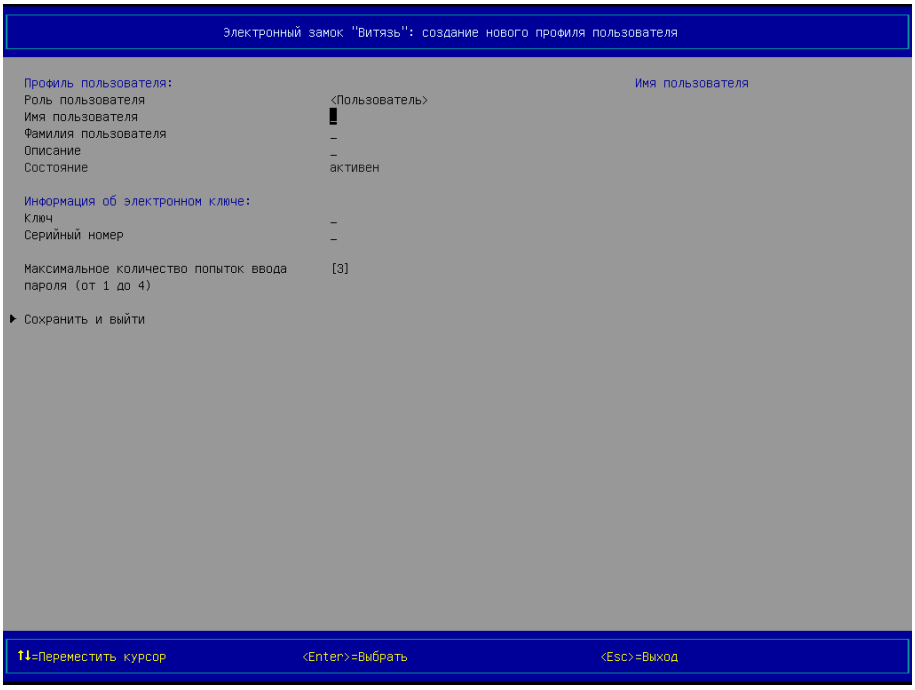


Рисунок 3.56 – Страница *Электронный замок “Витязь”: создание нового профиля пользователя* (вид 4)

3.6.3 Изменение способа аутентификации пользователя

Для изменения способа аутентификации пользователя следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Электронный замок “Витязь”* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: Настройки* (см. рисунки 3.15, 3.19);

5) выполнить действия 8-14 п. 3.4.1 для изменения способа аутентификации пользователя.

Примечание. Изменение способа аутентификации пользователя возможно только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

3.6.4 Изменение профиля пользователя

Для изменения профиля пользователя следует:

1) выполнить действия 1-4 п. 3.6.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см.
рисунки 3.48 - 3.51);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. рисунки 3.57, 3.71), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

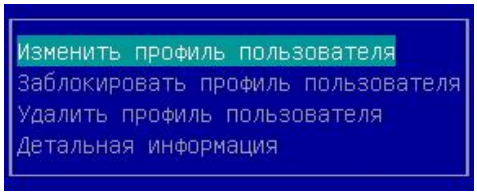


Рисунок 3.57 – Окно для выбора действия
над профилем пользователя (вид 1)

4) выбрать пункт *Изменить профиль пользователя* в окне выбора;

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: изменение профиля пользователя* (см. рисунки 3.58 – 3.63);

Рисунок 3.58 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 1), профиль пользователя, *Способ аутентификации* — «Электронный ключ»

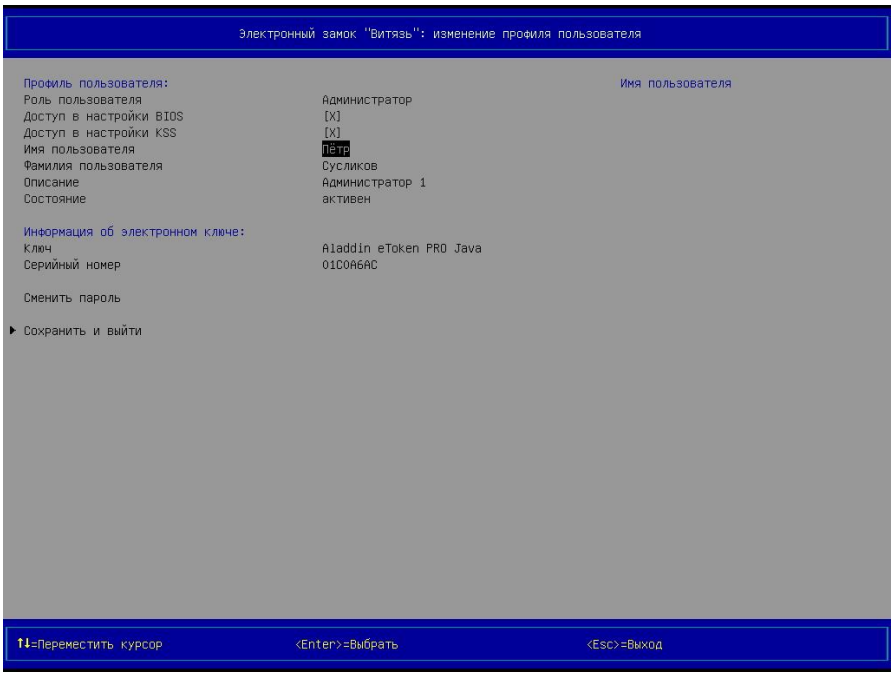


Рисунок 3.59 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 2), профиль администратора, *Способ аутентификации* — «Электронный ключ»

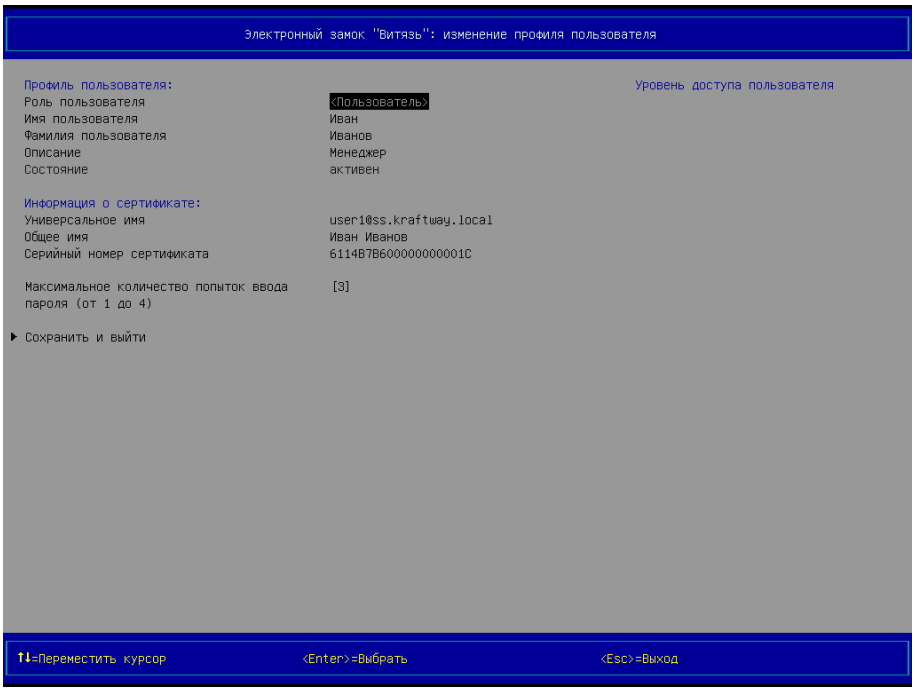


Рисунок 3.60 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 3), профиль пользователя, *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

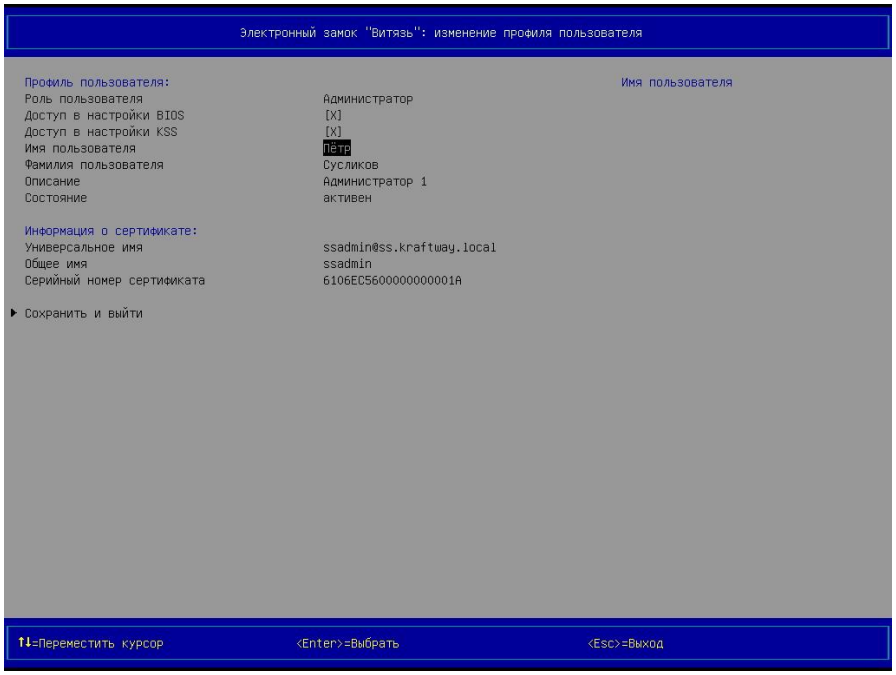


Рисунок 3.61 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 4), профиль администратора, *Способ аутентификации* – «Цифровой сертифи-

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

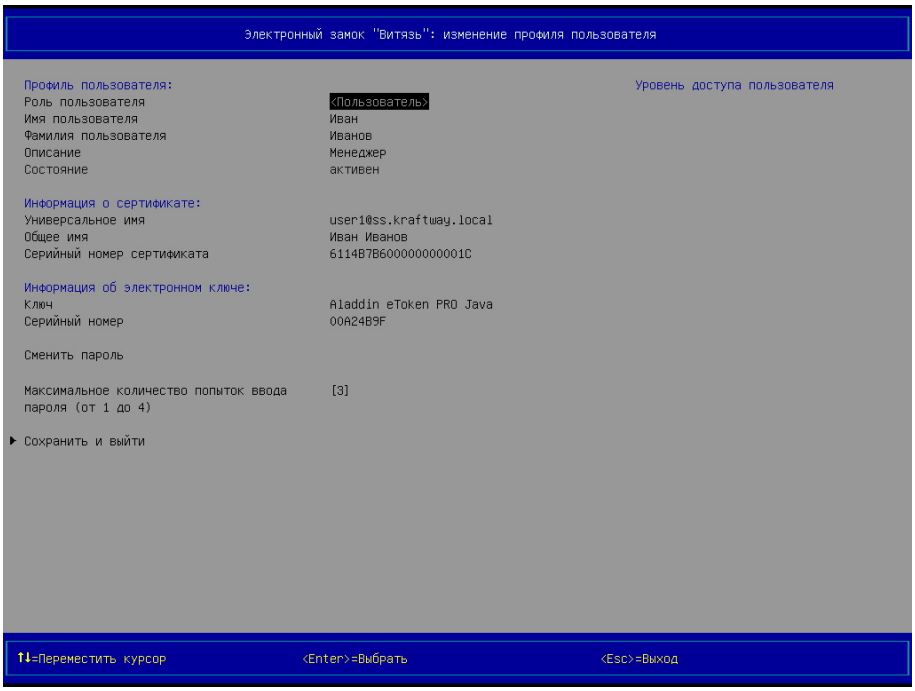


Рисунок 3.62 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 5), профиль пользователя, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное имя (UPN)»,

или «Серийный номер сертификата»

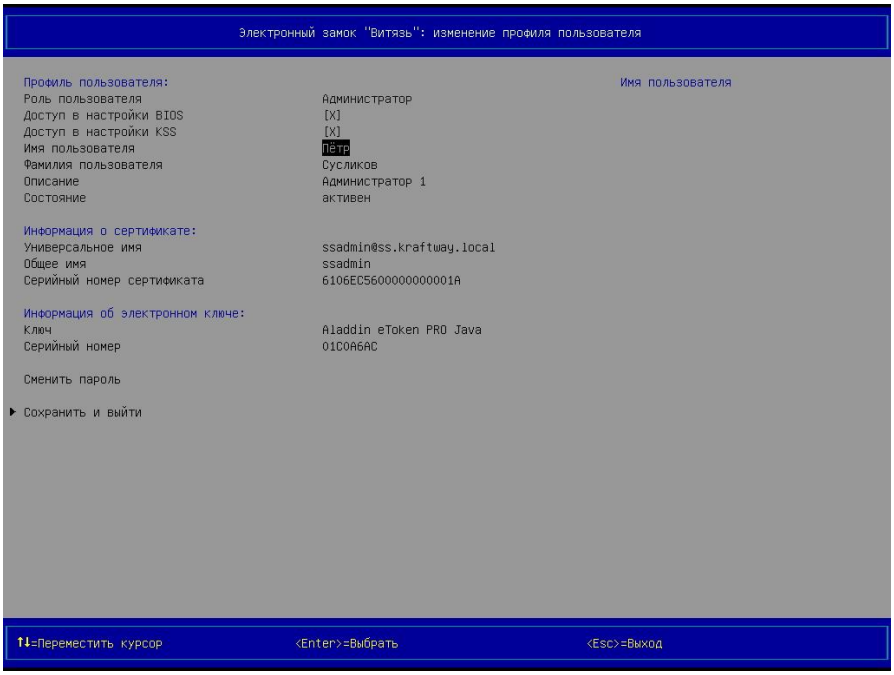


Рисунок 3.63 – Страница *Электронный замок “Витязь”: изменения профиля пользователя* (вид 6), профиль администратора, *Способ аутентификации* – «Цифровой сертификат и электронный ключ», *Ключевое поле* – или «Общее имя (CN)», или «Универсальное

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

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 п. 3.6;

7) изменить пароль пользователя при необходимости (см. п. 3.6.5);

8) выбрать пункт *Сохранить и выйти*;

9) → [Enter] на клавиатуре.

Примечания:

1. Изменение профиля пользователя возможно только после включения модуля безопасности *Электронный замок "Витязь"* (см. п. 3.4), создания профиля первого администратора (см. п. 3.5.1).

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. рисунок 3.31, 3.35). 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 ЭЗ становятся доступными для изменения следующие параметры: *Роль пользователя*, *Доступ в настройки BIOS*, *Доступ в настройки KSS*.

4. Администратор ЭЗ, который прошёл процедуру аутентификации в ЭЗ 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 ЭЗ, который прошёл процедуру аутентификации в ЭЗ 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.

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

8. При следующих настройках ЭЗ: *Электронный замок "Витязь"* — «Вкл», *Способ аутентификации* — «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок "Витязь": изменения профиля пользователя* (см. рисунки 3.60, 3.61). При данном способе аутентификации в ЭЗ изменить пароль пользователя нельзя (см. п. 3.6.5).

9. При изменении профиля администратора (профиля пользователя с ролью *Администратор*) параметр *Максимальное количество попыток ввода пароля* отсутствует на странице *Электронный замок "Витязь": изменение профиля пользователя* (см. рисунок 3.59, 3.61, 3.63), т.к. на администраторов ЭЗ не накладывается ограничение ЭЗ относительно максимального количества попыток ввода пароля. Ограничение относительно максимального количества попыток ввода пароля накладывается на администраторов ЭЗ только со стороны используемого АН. Данное количество устанавливается при инициализации АН с помощью программного обеспечения, идущего в комплекте с АН, и определённо в эксплуатационной документации на АН.

3.6.5 Изменение пароля пользователя

Для изменения пароля пользователя следует:

1) выполните действия 1-5 п. 3.6.4;

2) выберите параметр *Сменить пароль*;

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

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно для ввода старого пароля пользователя (см. Рисунок 3.64);

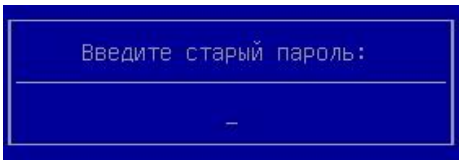


Рисунок 3.64 – Окно для ввода старого пароля пользователя

5) введите старый пароль в окно;

6) → [Enter] на клавиатуре, на экран выводится окно для ввода нового пароля пользователя (см. Рисунок 3.65);

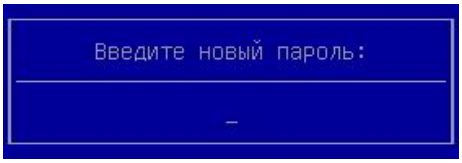


Рисунок 3.65 – Окно для ввода нового пароля пользователя

7) введите новый пароль пользователя;

8) → [Enter] на клавиатуре, на экран выводится окно для подтверждения нового пароля пользователя (см. Рисунок 3.66);

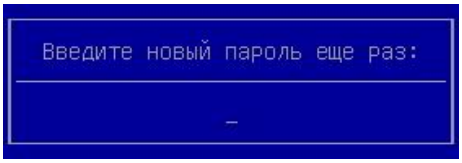


Рисунок 3.66 – Окно для подтверждения нового пароля пользователя

9) введите новый пароль пользователя;

10) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.67), информирующее об успешном изменении пароля;

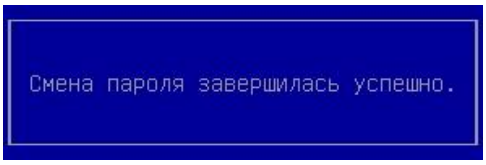


Рисунок 3.67 – Окно, информирующее об успешном изменении пароля пользователя

11) нажать любую клавишу на клавиатуре.

Примечания:

1. Изменение пароля пользователя возможно только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4), создания профиля первого администратора (см. п. 3.5.1).

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

3. При следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» – параметр *Сменить пароль* отсутствует на странице *Электронный замок “Витязь”: изменения профиля пользователя* (см. рисунки 3.60, 3.61).

3.6.6 Блокировка профиля пользователя

Для выполнения блокировки профиля пользователя следует:

1) выполнить действия 1-3 п. 3.6.4;

2) выбрать пункт *Заблокировать профиль пользователя* в окне (см. Рисунок 3.57);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.68), запрашивающее подтверждение на блокировку профиля пользователя;

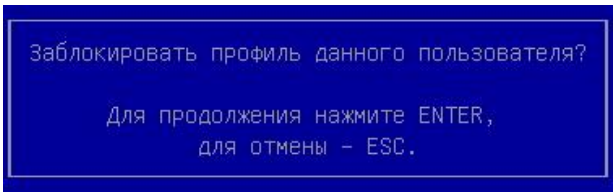


Рисунок 3.68 – Запрос подтверждения на блокировку профиля пользователя

4) → [Enter] на клавиатуре, после выполнения данного действия состояние пользователя меняется с «активен» на «заблокирован» (см. Рисунок 3.69).

Рисунок 3.69 – Страница *Электронный замок “Витязь”: список пользователей* (вид 7), состояние профиля пользователя – «заблокирован»

Примечания:

1. Блокировка профиля пользователя возможна только при выполнении следующих условий:
   - включён модуль безопасности *Электронный замок “Витязь”* (см. п. 3.4);
   - создан профиль первого администратора (см. п. 3.5.1);
   - 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, определённое администратором для профиля пользователя, профиль пользователя блокируется ЭЗ.

3. Если в ЭЗ был создан профиль только для одного администратора, то выполнить блокировку его профиля невозможно. При попытке заблокировать единственный профиль администратора на экран выводится окно следующего вида (см. Рисунок 3.70).

Рисунок 3.70 – Невозможно выполнить операцию для профиля пользователя

4. Невозможно заблокировать профиль администратора, который выполнил вход в оболочку Kraftway Secure Shell. При попытке блокировки его профиля на экран выводится окно следующего вида (см. Рисунок 3.70).

3.6.7 Разблокировка профиля пользователя

Для разблокировки профиля пользователя следует:

1) выполнить действия 1-4 п. 3.6.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см.
рисунки 3.48 - 3.51);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.71), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

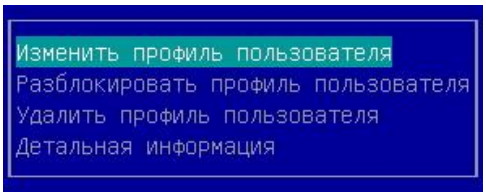


Рисунок 3.71 – Окно для выбора действия
над профилем пользователя (вид 2)

4) выбрать пункт *Разблокировать профиль пользователя* в окне выбора;

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.72), запрашивающее подтверждение на разблокировку профиля пользователя;

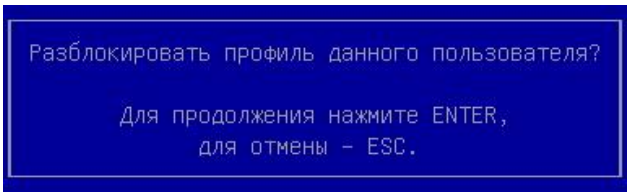


Рисунок 3.72 – Запрос подтверждения на разблокировку
профиля пользователя

6) → [Enter] на клавиатуре, после выполнения данного действия состояние профиля пользователя меняется с «заблокирован» на «активен» (см. Рисунок 3.73).

Рисунок 3.73 – Страница *Электронный замок “Витязь”: список пользователей* (вид 8), состояние профиля пользователя – «активен»

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

- включён модуль безопасности *Электронный замок “Витязь”* (см. п. 3.4);
- создан профиль первого администратора (см. п. 3.5.1);
- создан хотя бы один профиль пользователя или второй профиль администратора, который обладает правом доступа к настройкам KSS.

3.6.8 Удаление профиля пользователя

Для удаления профиля пользователя следует:

1) выполнить действия 1-4 п. 3.6.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см.
рисунки 3.48 - 3.51);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. рисунки 3.57, 3.71), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

4) выбрать пункт *Удалить профиль пользователя* в окне (см. рисунки 3.57, 3.71);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.74), запрашивающее подтверждение на удаление профиля пользователя;

Рисунок 3.74 – Запрос подтверждения на удаление профиля пользователя

6) → [Enter] на клавиатуре, после выполнения данного действия профиль пользователя удаляется.

Примечания:

1. Удаление профиля пользователя возможно только при выполнении следующих условий:
   - создан профиль первого администратора (см. п. 3.5.1);
   - создан хотя бы один профиль пользователя или второй профиль администратора, который обладает правом доступа к настройкам KSS.

2. Если в ЭЗ был создан только один администратор, то выполнить удаление его профиля невозможно. При попытке удалить единственный профиль администратора на экран выводится окно следующего вида (см. Рисунок 3.70).

3. Невозможно удалить профиль администратора, который выполнил вход в оболочку Kraftway Secure Shell. При попытке удаления его профиля на экран выводится окно следующего вида (см. Рисунок 3.70).

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*.

3.6.9 Вывод детальной информации о пользователе

Для вывода детальной информации о пользователе следует:

1) выполнить действия 1-4 п. 3.6.1;

2) выбрать требуемый профиль пользователя в разделе *Профили пользователей* (см.
рисунки 3.48 - 3.51);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. рисунки 3.57, 3.71), предлагающее выбрать действие, которое необходимо выполнить над профилем пользователя;

4) выбрать пункт *Детальная информация* в диалоговом окне (см. рисунки 3.57, 3.71);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Электронный замок “Витязь”: детальная информация о пользователе* (см.
рисунки 3.75, 3.76).

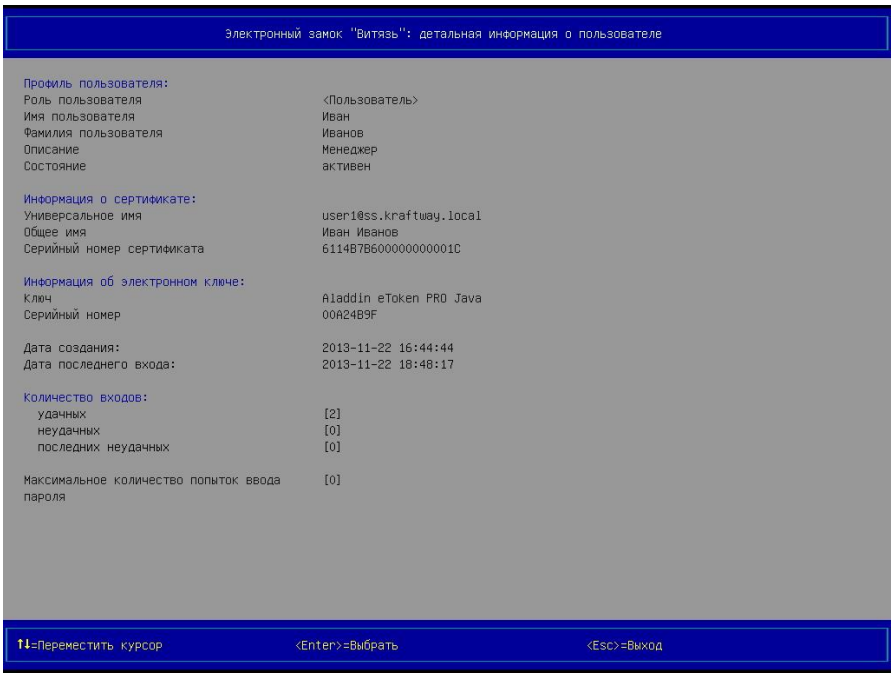


Рисунок 3.75 – Страница *Электронный замок “Витязь”: детальная информация о пользователе*,

профиль пользователя, *Способ аутентификации* — «Цифровой сертификат и электронный ключ», *Ключевое поле* — или «Общее имя (CN)», или «Универсальное имя (UPN)», или «Серийный номер сертификата»

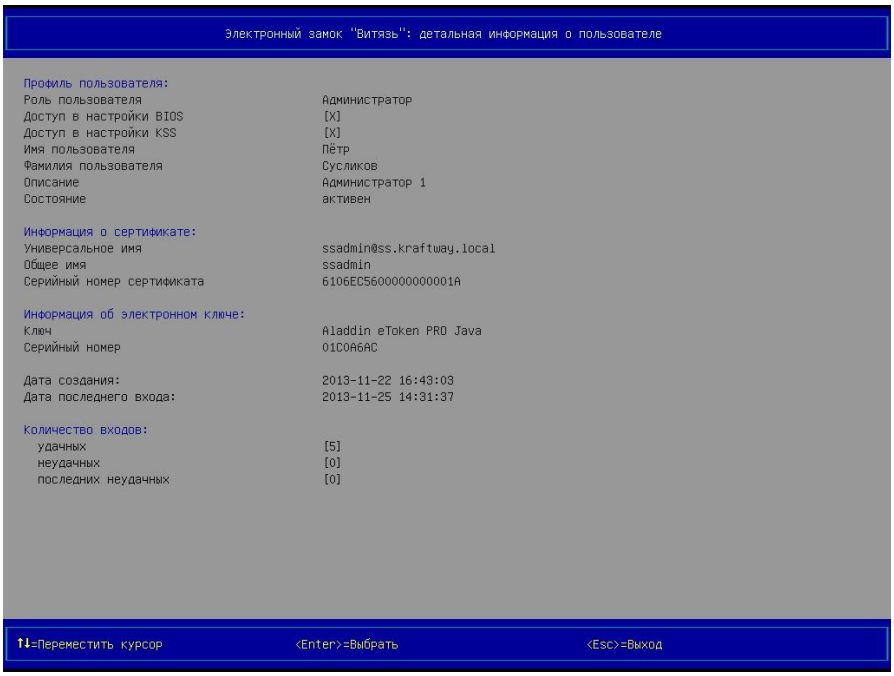


Рисунок 3.76 – Страница *Электронный замок “Витязь”: детальная информация о пользователе*,

профиль администратора, *Способ аутентификации* — «Цифровой сертификат и элек-

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

Примечания:

1. Вывод детальной информации о пользователе возможен после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4), создания профиля первого администратора (см. п. 3.5.1).

2. Количество параметров и их значений, выводимых на странице *Электронный замок “Витязь”: детальная информация о пользователе* (см. рисунки 3.75, 3.76), зависит от способа *аутентификации*, который был установлен администратором в настройках ЭЗ, и от профиля пользователя, детальную информацию о котором требуется вывести и просмотреть.

Может быть выведена следующая информация о пользователе:

1) роль пользователя (администратор или пользователь);
2) доступ к настройкам BIOS (только для профиля пользователя с ролью *Администратор*);
3) доступ к настройкам KSS (только для профиля пользователя с ролью *Администратор*);
4) имя пользователя;
5) фамилия пользователя;
6) описание пользователя (должность, например, инженер);
7) состояние профиля пользователя (активен или заблокирован);
8) информация о сертификате:
   – универсальное имя;
   – общее имя;
   – серийный номер сертификата;
9) информация об АН;
   – ключ;
   – серийный номер;
10) дата создания пользователя;
11) дата последнего входа пользователя;

12) количество входов:
   - количество удачных входов;
   - количество неудачных входов;
   - количество последних неудачных входов;
13) максимальное количество попыток ввода пароля.

Примечания:

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

2. Сведения о максимальном количестве попыток ввода пароля приводится только для профилей пользователей, а для профилей администраторов данная информация не приводится (см. примечания п. 3.6, 3.6.4).

3.7 Контроль целостности модулей безопасности

При включении ЭЗ происходит процедура контроля целостности модулей безопасности и целостности драйверов ЭЗ.

Для вывода результата процедуры контроля целостности модулей безопасности и целостности драйверов ЭЗ следует:

1) выбрать пункт *Контроль модулей безопасности* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль модулей безопасности* (см. Рисунок 3.77);

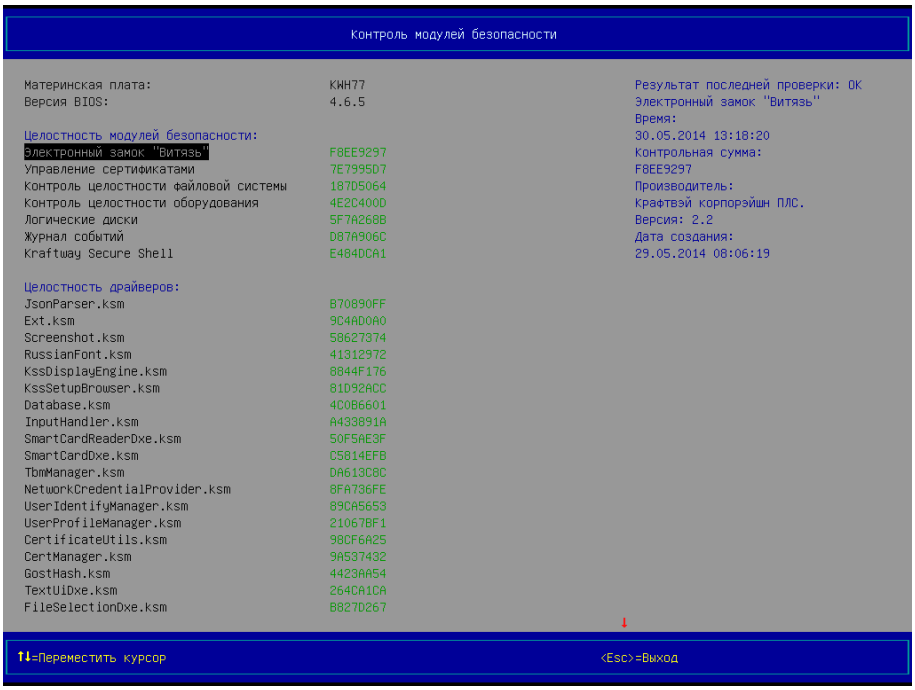


Рисунок 3.77 – Страница *Контроль модулей безопасности*

3) выбрать требуемый модуль безопасности в разделе *Целостность модулей безопасности* с помощью клавиш [↑], [↓], расположенных на клавиатуре, для вывода дополнительной информации в правой части области № 2 оболочки KSS;

4) выбрать требуемый драйвер в разделе *Целостность драйверов* с помощью клавиш [↑], [↓], расположенных на клавиатуре, для вывода дополнительной информации в правой части области № 2 оболочки KSS;

Примечания:

1. Контроль целостности БД ЭЗ происходит при каждом старте компьютера.

2. С правой стороны каждого модуля безопасности и драйвера ЭЗ приводится его контрольная сумма.

3. После выбора требуемого модуля безопасности или драйвера ЭЗ в правой части области № 2 оболочки KSS выводится следующая дополнительная информация:

– результат последней проверки;

– название объекта, прошедшего процедуру КЦ;

– время проверки объекта;

– контрольная сумма объекта;

– название производителя объекта;

– название версии объекта;

– дата создания объекта.

Под объектом следует понимать модуль безопасности или драйвер ЭЗ.

4. Для выбора самого первого модуля безопасности ЭЗ на странице *Контроль модулей безопасности* следует нажать на клавишу [Page Up] клавиатуры, для выбора самого последнего драйвера ЭЗ – [Page Down] клавиатуры.

3.8 Модуль безопасности *Управление сертификатами*

3.8.1 Включение модуля безопасности *Управление сертификатами*

Для включения модуля безопасности *Управление сертификатами* следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Управление сертификатами* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами: Настройки* (см. Рисунок 3.78);

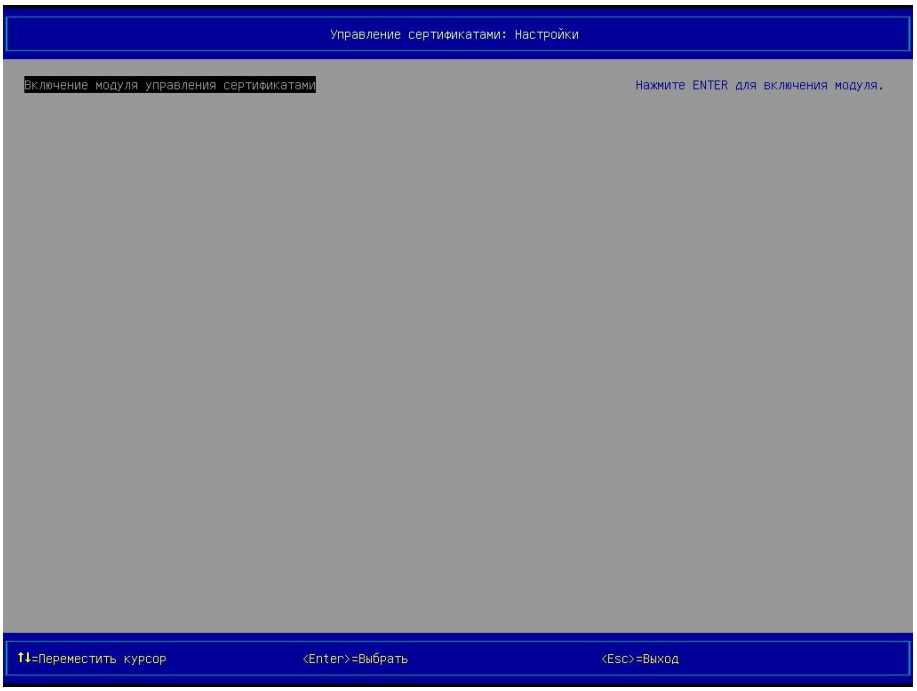


Рисунок 3.78 – Страница *Управление сертификатами: Настройки* (вид 1), пункт для включения модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.79), запрашивающее подтверждение на включение модуля;

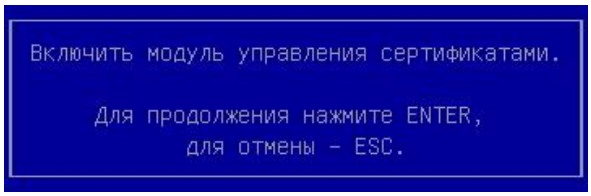


Рисунок 3.79 – Запрос подтверждения на включение модуля *Управление сертификатами*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля безопасности *Управление сертификатами*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.20).

3.8.2 Выключение модуля безопасности *Управление сертификатами*

Для выключения модуля безопасности *Управление сертификатами* следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Управление сертификатами* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами: Настройки* (см. Рисунок 3.80) с пунктом для выключения модуля;

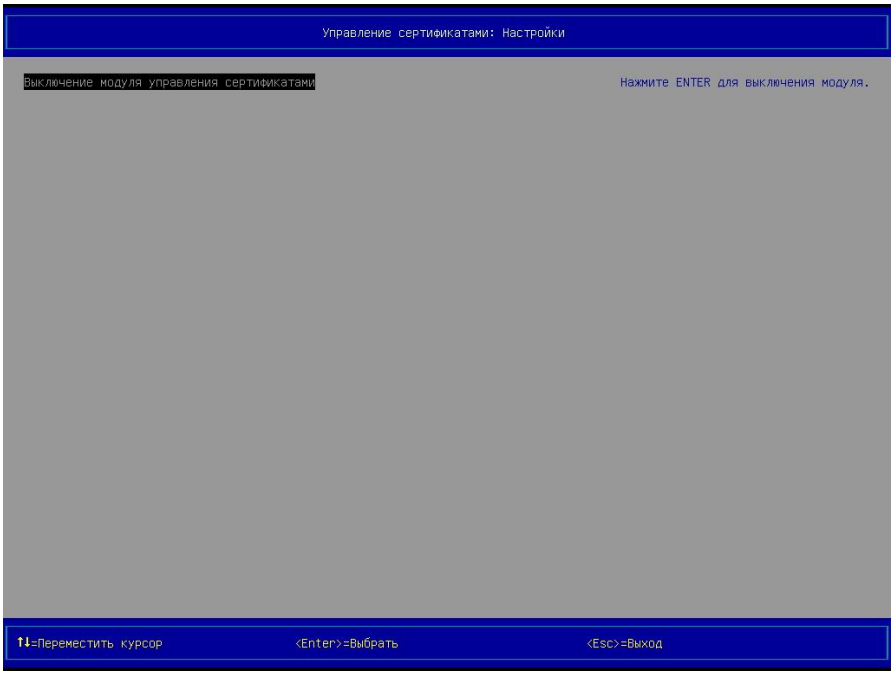


Рисунок 3.80 – Страница *Управление сертификатами: Настройки* (вид 2), пункт для выключения модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.81), запрашивающее подтверждение на выключение модуля;

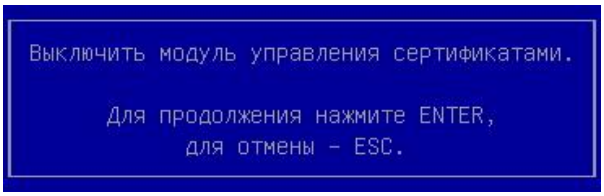


Рисунок 3.81 – Запрос подтверждения на выключение модуля *Управление сертификатами*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля безопасности *Управление сертификатами*, на экран выводится страница *Настройки*, статус модуля изменяется с «Вкл» на «Выкл» (см. Рисунок 3.5).

3.8.3 Добавление сертификата удостоверяющего центра в ЭЗ

ВНИМАНИЕ: АДМИНИСТРАТОР ДОЛЖЕН ДОБАВЛЯТЬ ТОЛЬКО ТЕ СЕРТИФИКАТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА (УЦ), С ПОМОЩЬЮ КОТОРЫХ БЫЛИ ПОДПИСАНЫ СЕРТИФИКАТЫ ПОЛЬЗОВАТЕЛЕЙ, ХРАНЯЩИЕСЯ НА АН! НЕСОБЛЮДЕНИЕ ДАННОГО ТРЕБОВАНИЯ ПРИВЕДЁТ К НЕВОЗМОЖНОСТИ АУТЕНТИФИКАЦИИ В ЭЗ!

Для добавления сертификата удостоверяющего центра (УЦ) в ЭЗ следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. рисунки 3.82, 3.85);

Рисунок 3.82 – Страница *Управление сертификатами* (вид 1), сертификаты УЦ отсутствуют

3) подключить USB-диск к свободному порту персонального компьютера, если необходимый сертификат УЦ расположен на нём (при добавлении сертификата УЦ с разделов жёстких дисков персонального компьютера данный пункт следует пропустить);

4) выбрать пункт *Добавить сертификат УЦ* (см. рисунки 3.82, 3.85, 3.89, 3.90);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Файловый менеджер* (см. рисунок 3.83);

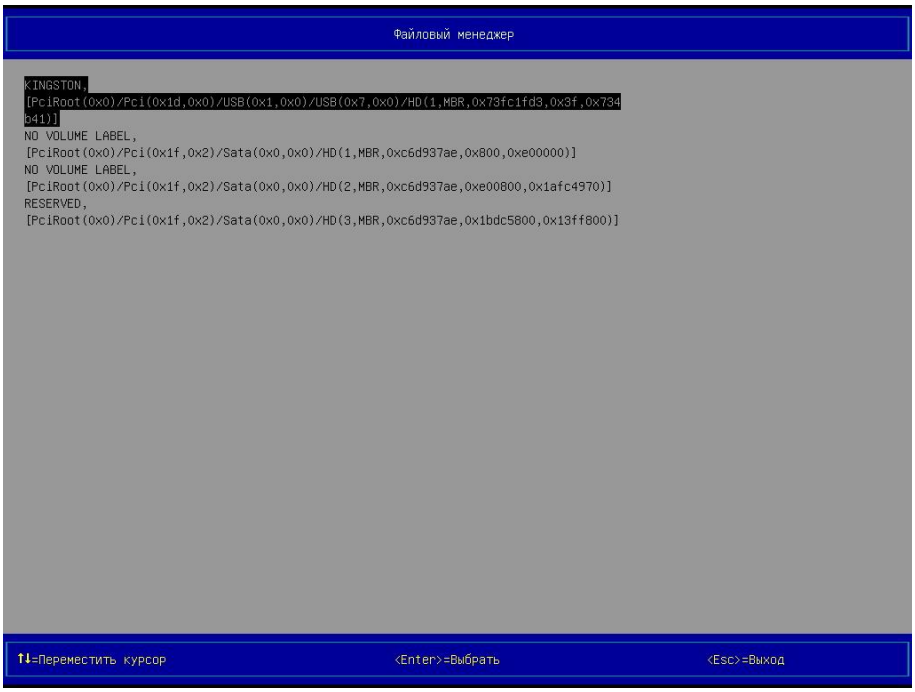


Рисунок 3.83 – Страница *Файловый менеджер*

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

7) → [Enter] на клавиатуре;

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

9) выделить необходимый файл, который является сертификатом УЦ;

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.84), информирующее о добавлении сертификата УЦ в ЭЗ;

Рисунок 3.84 – Сертификат УЦ добавлен

11) → [Enter] на клавиатуре.

Примечания:

1. Добавление сертификата УЦ в ЭЗ возможно только после включения модуля безопасности *Управление сертификатами* (см. п. 3.8.1).

2. Действия на странице *Файловый менеджер* (см. Рисунок 3.83): перемещение по объектам (локальные диски, папки, подпапки, файлы) страницы выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре; открытие папки, подпапки, переход в родительский каталог, выбор выделенного элемента выполняется с помощью клавиши [Enter], расположенной на клавиатуре.

3.8.4 Просмотр информации о сертификате удостоверяющего центра

Для просмотра информации о сертификате УЦ следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. Рисунок 3.85);

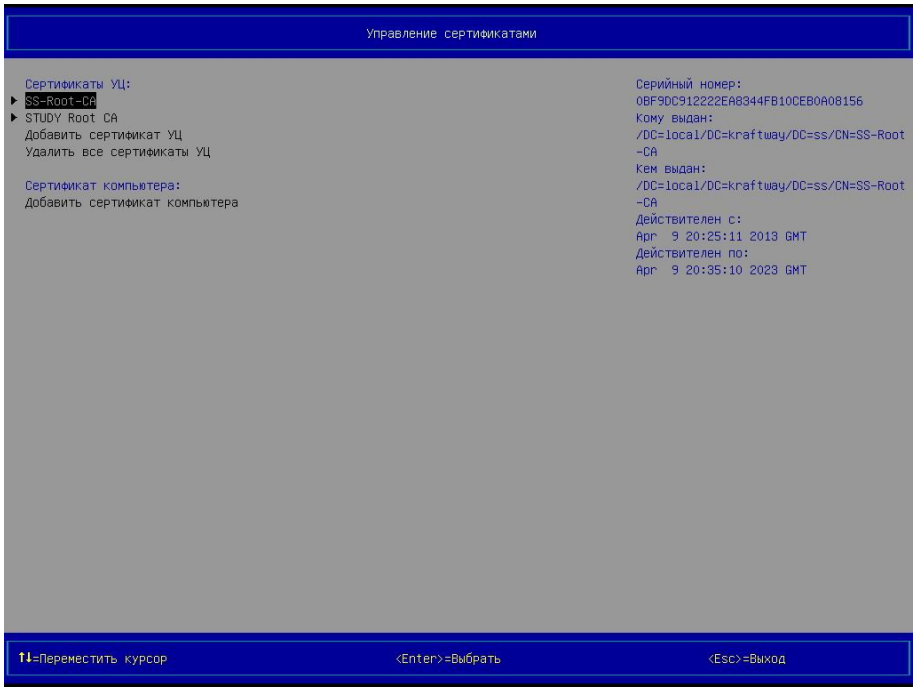


Рисунок 3.85 – Страница *Управление сертификатами* (вид 2), два сертификата УЦ добавлены

3) выбрать сертификат УЦ, информацию о котором требуется просмотреть, после выполнения данного действия в правой части области № 2 оболочки KSS 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 безопасности *Управление сертификатами* (см. п. 3.8.1), и добавления хотя бы одного сертификата УЦ.

2. Просмотр справочной информации о разрешенном минимальном и максимальном количестве дней для пункта "Оповещать об истечении срока действия сертификата".

Для просмотра данной информации:

1) перейдите в меню *Управление сертификатами*.

2) проверьте информацию в пункте "Оповещать об истечении срока действия сертификата";

3) проверьте границы значений.

Первоначальное количество дней задано по умолчанию. Фактически можно добавлять минимум 4, максимум 222.

3.8.5 Удаление всех сертификатов удостоверяющего центра из ЭЗ

Для удаления всех сертификатов УЦ из ЭЗ следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. Рисунок 3.85);

3) выбрать пункт *Удалить все сертификаты УЦ* в разделе *Сертификаты УЦ*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.86), запрашивающее подтверждение на удаление всех сертификатов УЦ, ранее добавленных в ЭЗ;

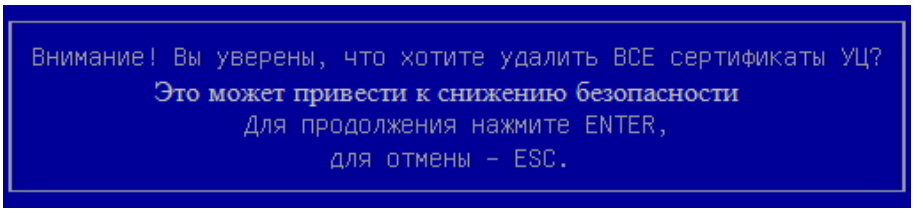


Рисунок 3.86 – Запрос подтверждения на удаление всех сертификатов УЦ

5) → [Enter] на клавиатуре, после выполнения данного действия все сертификаты УЦ, ранее добавленные в ЭЗ, удаляются из ЭЗ, а на экран выводится окно (см. Рисунок 3.87), информирующее об удалении всех сертификатов УЦ;

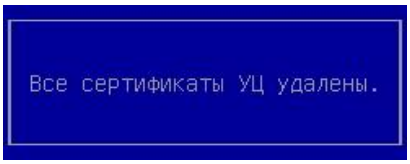


Рисунок 3.87 – Все сертификаты УЦ удалены

6) → [Enter] на клавиатуре.

Примечание. Удаление всех сертификатов УЦ из ЭЗ возможно только после включения модуля безопасности *Управление сертификатами* (см. п. 3.8.1), добавления хотя бы одного сертификата УЦ в ЭЗ.

3.8.6 Добавление сертификата компьютера в ЭЗ

Для добавления сертификата компьютера в ЭЗ следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. рисунки 3.82, 3.85);

3) подключить USB-диск к свободному порту персонального компьютера, если необходимый сертификат компьютера расположен на нём (при добавлении сертификата компьютера с разделов жёстких дисков персонального компьютера данный пункт следует пропустить);

4) выбрать пункт *Добавить сертификат компьютера* в разделе *Сертификат компьютера* (см. рисунки 3.82, 3.85);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Файловый менеджер* (см. Рисунок 3.83);

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

7) → [Enter] на клавиатуре;

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

9) выделить необходимый файл, который является сертификатом компьютера;

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.41), предлагающее ввести пароль для выделенного файла сертификата;

11) вывести пароль для выделенного файла сертификата;

12) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.88), информирующее о добавлении сертификата компьютера в ЭЗ;

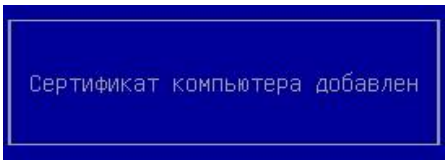


Рисунок 3.88 – Сертификат компьютера добавлен

13) → [Enter] на клавиатуре.

Примечания:

1. Добавление сертификата компьютера в ЭЗ возможно только после включения модуля безопасности *Управление сертификатами* (см. п. 3.8.1).

2. Действия на странице *Файловый менеджер* (см. Рисунок 3.83): перемещение по объектам (локальные диски, папки, подпапки, файлы) страницы выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре; открытие папки, подпапки, переход в родительский каталог, выбор выделенного элемента выполняется с помощью клавиши [Enter], расположенной на клавиатуре.

3. Только один сертификат компьютера можно добавить в ЭЗ.

3.8.7 Просмотр информации о сертификате компьютера

Для просмотра сертификата компьютера следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. Рисунок 3.89);

Рисунок 3.89 – Страница *Управление сертификатами* (вид 3), сертификат компьютера добавлен

3) выбрать сертификат компьютера, информацию о котором требуется просмотреть, после выполнения данного действия в правой части области № 2 оболочки KSS выводится информация о выбранном сертификате компьютера, а именно: серийный номер сертификата, кем выдан, кому выдан, даты и время начала срока действия сертификата, даты и время окончания срока действия сертификата (см. Рисунок 3.90);

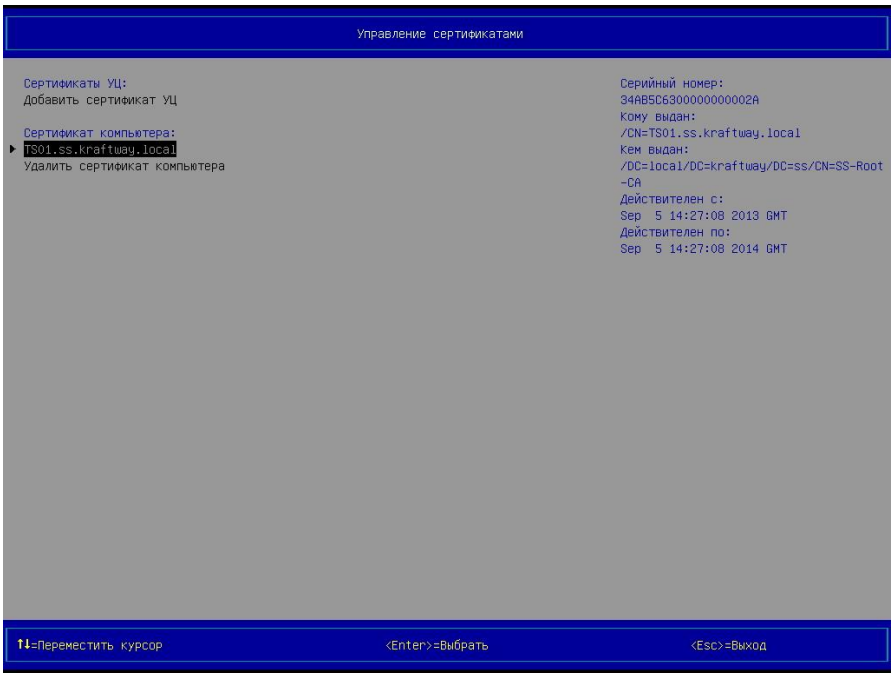


Рисунок 3.90 – Страница *Управление сертификатами* (вид 4), информация о сертификате компьютера выведена

4) просмотреть и проанализировать данную информацию.

Примечание. Просмотр информации о сертификате компьютера возможен только после включения модуля безопасности *Управление сертификатами* (см. п. 3.8.1), добавления сертификата компьютера в ЭЗ.

3.8.8 Удаление сертификата компьютера из ЭЗ

Для удаления сертификата компьютера из ЭЗ следует:

1) выбрать пункт *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами* (см. рисунки 3.89, 3.90);

3) выбрать пункт *Удалить сертификат компьютера* в разделе *Сертификат компьютера* (см. рисунки 3.89, 3.90);

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.91), запрашивающее подтверждение на удаление сертификата компьютера, ранее добавленного в ЭЗ;

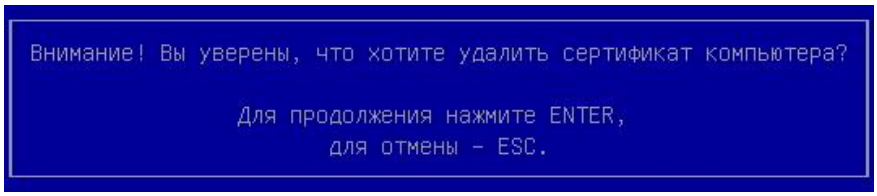


Рисунок 3.91 – Запрос подтверждения на удаление сертификата компьютера

5) → [Enter] на клавиатуре, после выполнения данного действия сертификат компьютера, ранее добавленный в ЭЗ, удаляется из ЭЗ, а на экран выводится окно (см. Рисунок 3.92), информирующее об удалении сертификата компьютера;

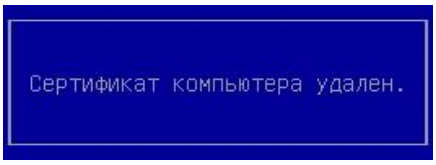


Рисунок 3.92 – Сертификат компьютера удалён

6) → [Enter] на клавиатуре.

Примечание. Удаление сертификата компьютера из ЭЗ возможно только после включения модуля безопасности *Управление сертификатами* (см. п. 3.8.1), добавления сертификата компьютера в ЭЗ.

3.9 Модуль безопасности *Контроль целостности файловой системы*

3.9.1 Включение КЦ файловой системы

Для включения КЦ файловой системы следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. рисунок 3.5);

3) выбрать пункт *Контроль целостности файловой системы* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности файловой системы: Настройки* с пунктом включения модуля (см. Рисунок 3.93);

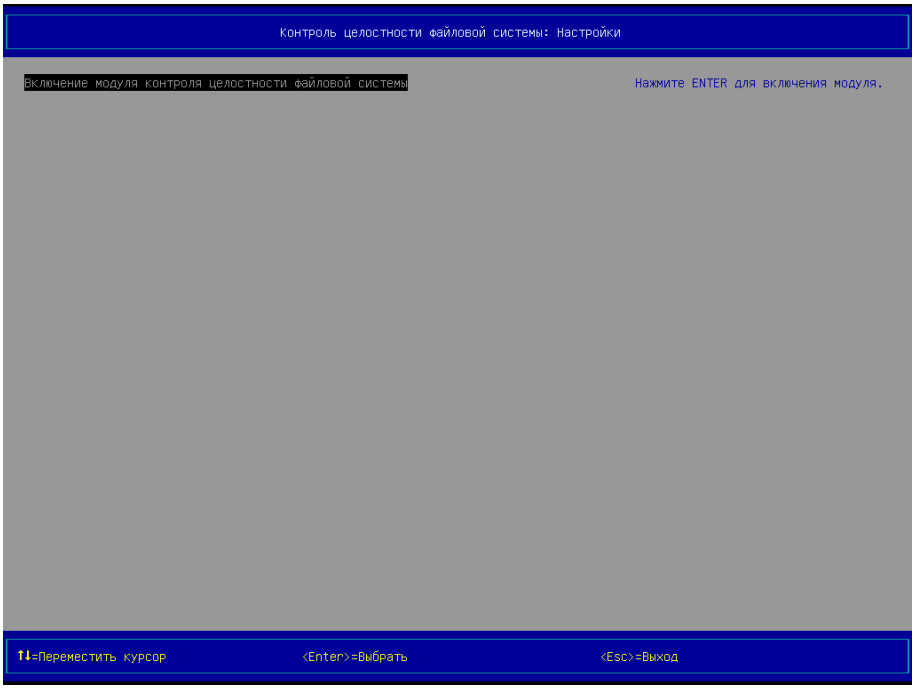


Рисунок 3.93 – Страница *Контроль целостности файловой системы: Настройки* (вид 1), пункт для включения модуля КЦ ФС

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.94), запрашивающее подтверждение на включение модуля;

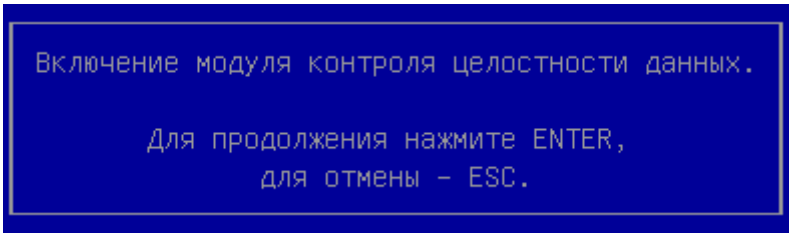


Рисунок 3.94 – Запрос подтверждения на включение модуля *Контроль целостности файловой системы*

6) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности файловой системы: Настройки* (вид 2), с возможностью выбора хеш-функции (см. Рисунок 3.95);

Рисунок 3.95 – Страница *Контроль целостности файловой системы: Настройки* (вид 2), пункт выбора хеш-функции

7) выбрать пункт *Выберите хеш-функцию*;

8) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.96), предлагающее выбрать хеш-функцию из списка;

Рисунок 3.96 – Окно для выбора хеш-функции

9) выбрать требуемую хэш-функцию, с помощью клавиш [↑], [↓], расположенных на клавиатуре. Выбранная хеш-функция будет использоваться для контроля целостности данных;

10) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля безопасности;

11) → [Esc] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.20), статус модуля безопасности *Контроль целостности файловой системы* изменяется с «Выкл» на «Вкл».

Примечания:

1. Выбор хеш-функции осуществляется исходя из политики безопасности принятой в организации.

2. По умолчанию выбрана хеш-функция «CBI».

3.9.2 Выбор хеш-функции

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

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Контроль целостности файловой системы* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности файловой системы: Настройки* (см. Рисунок 3.95) с пунктом для выбора хеш-функции;

5) выбрать пункт *Выберите хеш-функцию*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.96), предлагающее выбрать хеш-функцию из списка;

7) выбрать требуемую хэш-функцию, с помощью клавиш [↑], [↓], расположенных на клавиатуре. Выбранная хеш-функция будет использоваться для контроля целостности данных;

8) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля безопасности;

9) → [Esc] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.20).

3.9.3 Выключение КЦ файловой системы

Для выключения КЦ файловой системы следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Контроль целостности файловой системы* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности файловой системы: Настройки* (см. Рисунок 3.97) с пунктом для выключения модуля и удаления всех списков контроля целостности;

Рисунок 3.97 – Страница *Контроль целостности файловой системы: Настройки* (вид 2), пункт для выключения модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.98), запрашивающее подтверждение на выключение модуля и удаления всех списков контроля целостности;

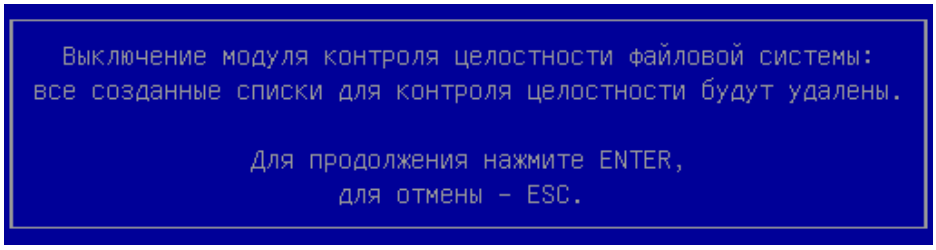


Рисунок 3.98 – Диалоговое окно, запрашивающее подтверждение на выключение модуля КЦ ФС и удаление всех списков контроля целостности

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля безопасности *Контроль целостности файловой системы* и удаление всех списков контроля целостности, на экран выводится страница *Настройки*, статус модуля КЦ ФС изменяется с «Вкл» на «Выкл» (см. Рисунок 3.5).

3.9.4 Создание списка файлов, подлежащих КЦ

Для создания списка файлов, подлежащих КЦ, следует:

1) выбрать пункт *Контроль целостности файловой системы* в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности файловой системы* (см. Рисунок 3.99);

Рисунок 3.99 – Страница *Контроль целостности файловой системы* (вид 1), ни одного списка файлов, подлежащих КЦ, не было создано

3) выбрать пункт *Добавить новый список файлов* в разделе *Выбор задачи*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Создание списка файлов* (см. Рисунок 3.100);

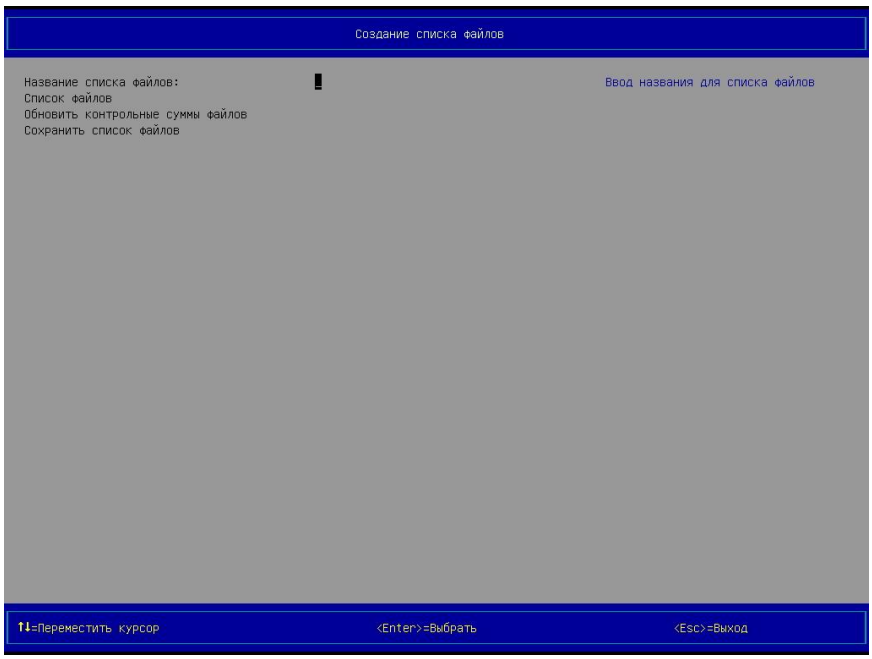


Рисунок 3.100 – Страница *Создание списка файлов*

5) выбрать пункт *Название списка файлов*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно для ввода названия списка файлов (см. Рисунок 3.101);

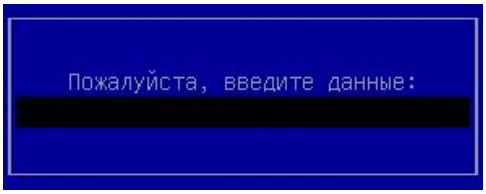


Рисунок 3.101 – Окно для ввода названия списка файлов

7) ввести название списка файлов;

8) → [Enter] на клавиатуре;

9) выбрать пункт С*писок файлов* (см. Рисунок 3.100);

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно файлового менеджера (см. Рисунок 3.102), в котором предлагается выбрать объекты (файлы, папки), подлежащие КЦ;

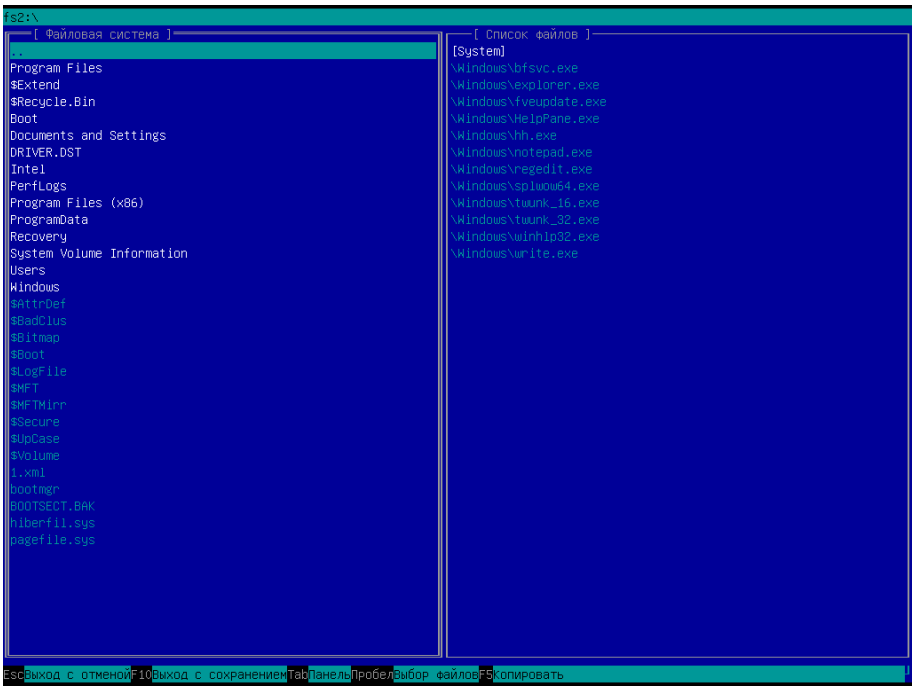


Рисунок 3.102 – Окно файлового менеджера

11) выбрать требуемый локальный диск в панели *Файловая система* с помощью клавиш [↑], [↓], расположенных на клавиатуре;

12) → [Enter] на клавиатуре;

13) в панели *Файловая система*, выделить объекты (файлы, папки), подлежащие КЦ;

14) скопировать выделенные объекты в правую панель *Список файлов* с помощью клавиши [F5];

15) выбрать другие объекты (файлы, папки), подлежащие КЦ, расположенные на этом локальном диске при необходимости;

16) выбрать объекты (файлы, папки), подлежащие КЦ, расположенные на других локальных дисках при необходимости;

17) удалить объект или объекты, которые не подлежат КЦ, из панели *Список файлов* при необходимости (см. примечание ниже);

18) → [F10] на клавиатуре для сохранения сделанных изменений и выхода из файлового менеджера;

19) выбрать пункт *Обновить контрольные суммы файлов* (см. Рисунок 3.100);

20) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.103), информирующее об успешном обновлении (создании) контрольных сумм (КС) файлов;

Рисунок 3.103 – Окно, информирующее об успешном обновлении КС файлов

21) → [Enter] на клавиатуре;

22) выбрать пункт *Сохранить список файлов* (см. Рисунок 3.100);

23) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.104), информирующее о выполнении сохранения списка файлов.

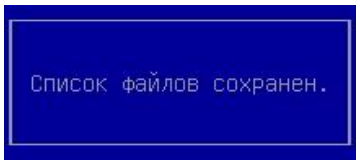


Рисунок 3.104 – Окно, информирующее о сохранении списка файлов

– → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно *Контроль целостности файловой системы*, с именем созданного списка в разделе *Контрольные списки файлов* (см. Рисунок 3.105). Справа вверху высветится информация о созданном файле, Дата и время: - Создания; - Изменения; - Последней проверки.

Примечания:

1. Создание списка файлов, подлежащих КЦ, возможно только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9).

2. Выбор требуемых объектов в панелях *Файловая система* и *Список файлов* выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре (см. Рисунок 3.102).

3. Выделение объектов в панелях *Файловая система* и *Список файлов* выполняется следующими способами:

   1) выбрать объект, который подлежит КЦ;
   2) → [Пробел] на клавиатуре.

   или

   1) выбрать объект, который подлежит КЦ;
   2) → [Insert] на клавиатуре.

Отличие второго способа от первого заключается в том, что для выделения следующих нескольких объектов, расположенных за первым выделенным файлом, следует нажимать только клавишу [Insert].

4. Перемещение между панелями *Файловая система* и *Список файлов* выполняется с помощью клавиши [Tab].

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

6. Удаление объекта из панели *Список файлов* выполняется следующим образом:

   1) выбрать требуемый объект, который не подлежит КЦ;
   2) нажать клавишу [F8] или клавишу [Delete] на клавиатуре.

7. Удаление сразу нескольких объектов из панели *Список файлов* выполняется следующим образом:

1) выбрать несколько объектов, которые не подлежат КЦ (см. п. 2 данного примечания);
2) нажать клавишу [F8] или клавишу [Delete] на клавиатуре.

3.9.5 Просмотр списка файлов, подлежащих КЦ

Для просмотра списка файлов, подлежащих КЦ, следует:

1) выбрать пункт *Контроль целостности файловой системы* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности файловой системы* (см. Рисунок 3.105);

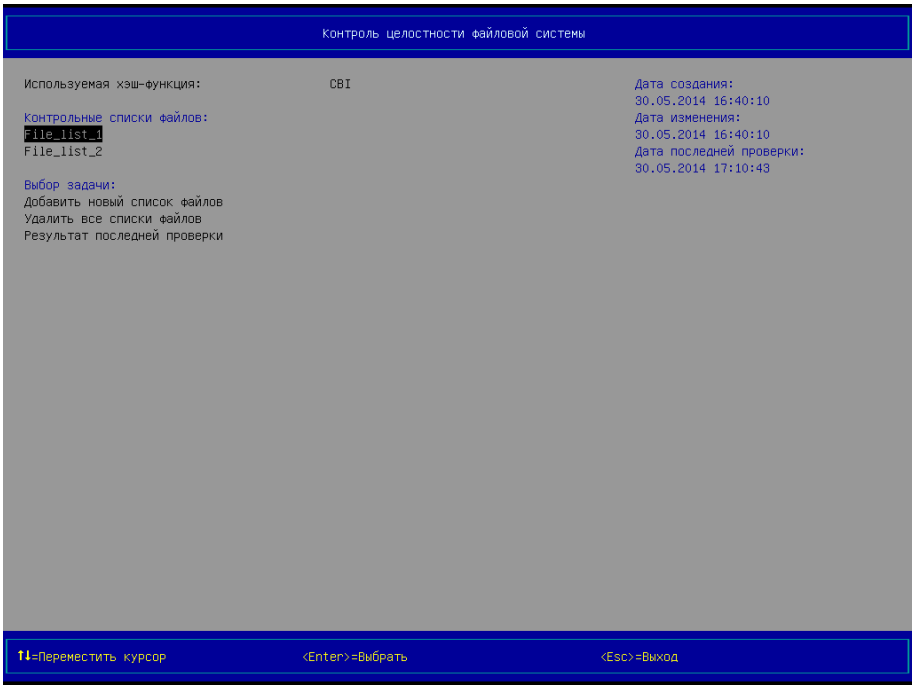


Рисунок 3.105 – Страница *Контроль целостности файловой системы* (вид 2), созданы два списка файлов, подлежащих КЦ

3) выбрать требуемый список файлов, подлежащих КЦ, с помощью клавиш [↑], [↓], расположенных на клавиатуре;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.106), предлагающее выбрать действие, которое необходимо выполнить над выбранным списком файлов;

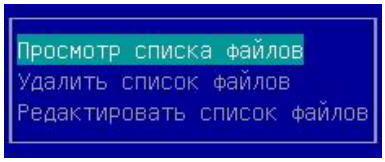


Рисунок 3.106 – Окно для выбора действия над выбранным списком файлов

5) выбрать пункт *Просмотр списка файлов* в окне выбора;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Просмотр списка файлов* (см. рисунок 3.107);

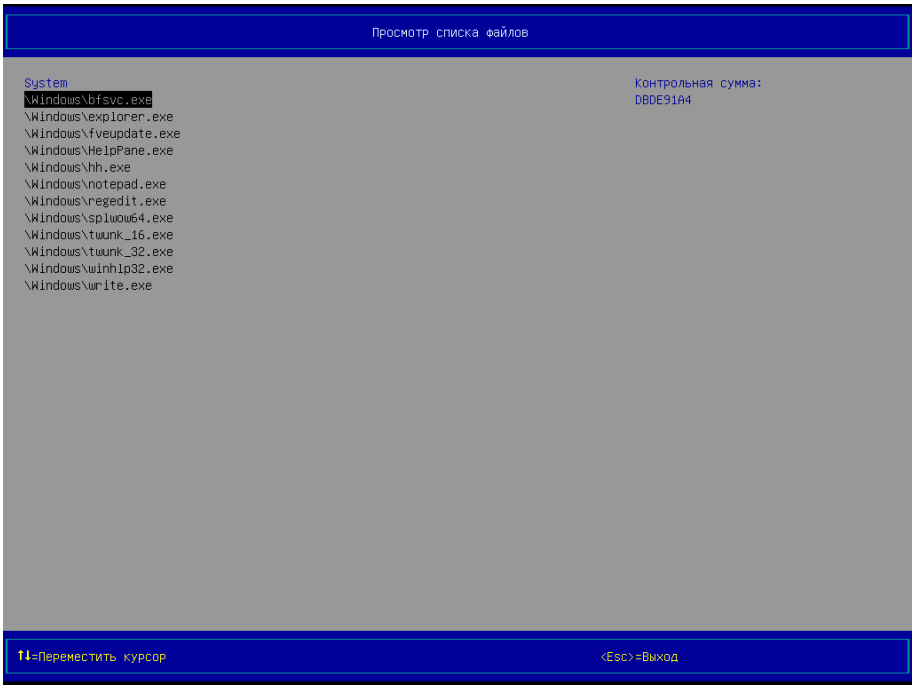


Рисунок 3.107 – Страница *Просмотр списка файлов*

Примечания:

1. Просмотр списка файлов, подлежащих КЦ, возможен только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9), создания хотя бы одного списка файлов, подлежащих КЦ.

2. Если список файлов состоит из большого количества записей, которые не умещаются в области № 2 оболочки KSS, то в данной области выводятся стрелки красного цвета: ↑ – дополнительные записи располагаются выше, ↓ – дополнительные записи располагаются ниже.

3. Перемещение по записям списка файлов выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре.

4. После выбора какой-либо записи списка файлов в правой части области № 2 выводится контрольная сумма объекта, указанного в выбранной записи.

5. Постраничный вывод записей списка файлов выполняется с помощью клавиш [Page Up], [Page Down], расположенных на клавиатуре.

3.9.6 Редактирование списка файлов, подлежащих КЦ

Для редактирования списка файлов, подлежащих КЦ, следует:

1) выполнить действия 1-4 п. 3.9.5,

2) выбрать пункт *Редактировать список файлов* в окне (см. Рисунок 3.106);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Редактировать список файлов* (см. Рисунок 3.108);

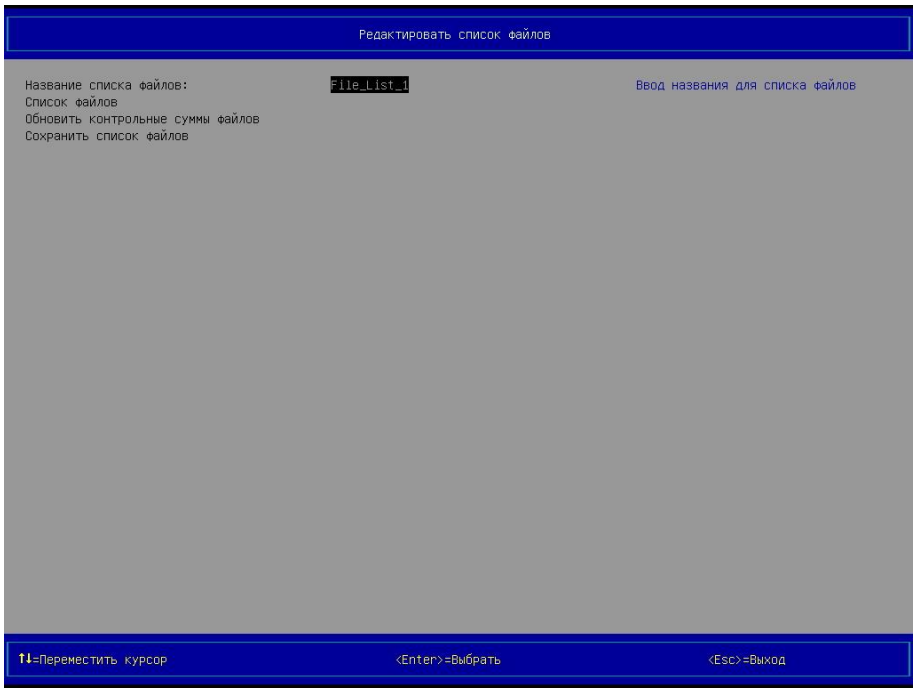


Рисунок 3.108 – Страница *Редактировать список файлов*

4) выполнить изменение названия списка файлов при необходимости (см. действия 5-8 п. 3.9.4);

5) изменить состав списка файлов при необходимости (см. действия 9-18 п. 3.9.4);

6) обновить контрольные суммы файлов (см. действия 19-21 п. 3.9.4), если состав списка файлов был изменён;

7) сохранить список файлов (см. действия 22-24 п. 3.9.4), если состав списка файлов был изменён.

Примечание. Редактирование списка файлов, подлежащих КЦ, возможно только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9), создания хотя бы одного списка файлов, подлежащих КЦ.

3.9.7 Удаление списка файлов, подлежащих КЦ

Для удаления списка файлов, подлежащих КЦ, следует:

1) выполнить действия 1-4 п. 3.9.5,

2) выбрать пункт *Удалить список файлов* в окне (см. Рисунок 3.106);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.109), запрашивающее подтверждение на удаление выбранного списка файлов;

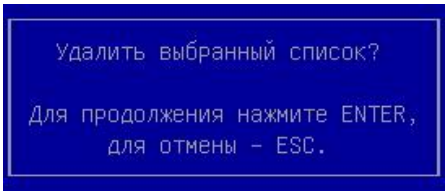


Рисунок 3.109 – Запрос подтверждения на удаление выбранного списка файлов

4) → [Enter] на клавиатуре, после выполнения данного действия происходит удаление выбранного списка файлов.

Примечание. Удаление списка файлов, подлежащих КЦ, возможно только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9), создания хотя бы одного списка файлов, подлежащих КЦ.

3.9.8 Вывод результата последнего выполнения процедуры КЦ файлов

Для вывода результата последнего выполнения процедуры КЦ файлов следует:

1) выполнить действия 1, 2 п. 3.9.4;

2) выбрать пункт *Результат последней проверки* (см. Рисунок 3.105);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Результат последней проверки* (см. рисунки 3.110, 3.111);

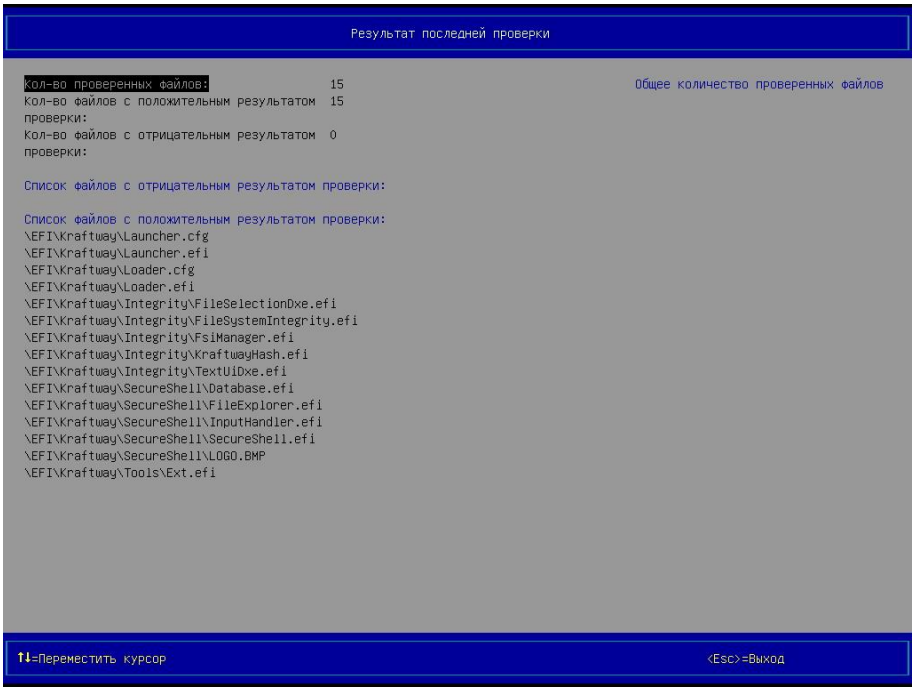


Рисунок 3.110 – Страница *Результат последней проверки* (вид 1), файлы с отрицательным результатом проверки отсутствуют

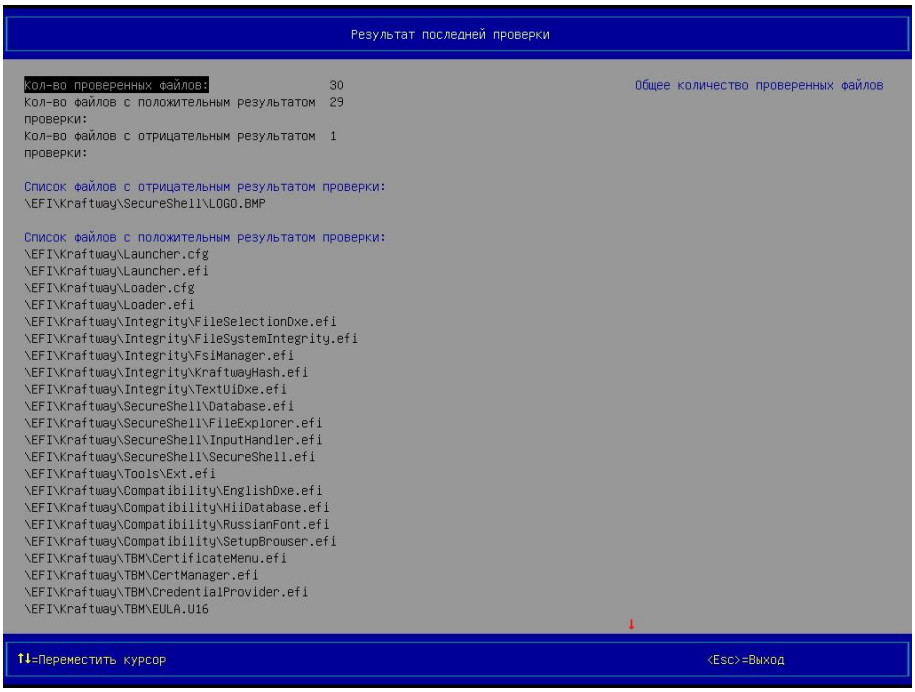


Рисунок 3.111 – Страница *Результат последней проверки* (вид 2), выведен файл с отрицательным результатом проверки

4) выбрать требуемый файл в разделе *Список файлов с отрицательным результатом проверки* с помощью клавиш [↑], [↓], расположенных на клавиатуре, для вывода дополнительной информации (имя устройства хранения, на котором размещается требуемый файл, контрольная сумма требуемого файла) в правой части области № 2;

5) выполнить действие 4 для других файлов раздела *Список файлов с отрицательным результатом проверки* при необходимости;

6) выбрать требуемый файл в категории *Список файлов с положительным результатом проверки* с помощью клавиш [↑], [↓], расположенных на клавиатуре, для вывода дополнительной информации (имя устройства хранения, на котором размещается требуемый файл, контрольная сумма требуемого файла) в правой части области № 2;

7) выполнить действие 6 для других файлов раздела *Список файлов с положительным результатом проверки* при необходимости.

Примечания:

1. Вывод результата последнего выполнения процедуры КЦ файлов возможен только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9), создания хотя бы одного списка файлов, подлежащих КЦ, первой перезагрузки персонального компьютера.

2. Если записи о результате последнего выполнения процедуры КЦ файлов, выводимые на странице *Результат последней проверки*, не умещаются в области № 2 оболочки KSS, то в данной области выводятся стрелки красного цвета: ↑ – дополнительные записи располагаются выше, ↓ – дополнительные записи располагаются ниже.

3. Перемещение по записям в области № 2 оболочки KSS выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре.

4. Постраничный вывод записей в области № 2 оболочки KSS выполняется с помощью клавиш [Page Up], [Page Down], расположенных на клавиатуре.

3.9.9 Удаление всех списков файлов, подлежащих КЦ

Для удаления всех списков файлов, подлежащих КЦ, следует:

1) выполнить действия 1, 2 п. 3.9.4;

2) выбрать пункт *Удалить все списки файлов* (см. Рисунок 3.105);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.112), запрашивающее подтверждение на удаление всех списков файлов;

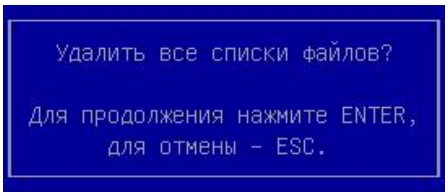


Рисунок 3.112 – Запрос подтверждения на удаление всех списков файлов

4) → [Enter] на клавиатуре, после выполнения данного действия происходит удаление всех ранее созданных списков файлов, подлежащих КЦ.

Примечание. Удаление всех списков файлов, подлежащих КЦ, возможно только после включения модуля безопасности *Контроль целостности файловой системы* (см. п. 3.9), создания хотя бы одного списка файлов, подлежащих КЦ.

3.10 Модуль безопасности *Контроль целостности оборудования*

3.10.1 Включение КЦ оборудования

Для включения КЦ оборудования следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Контроль целостности оборудования* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности оборудования: Настройки* с пунктом для включения модуля (см. Рисунок 3.113);

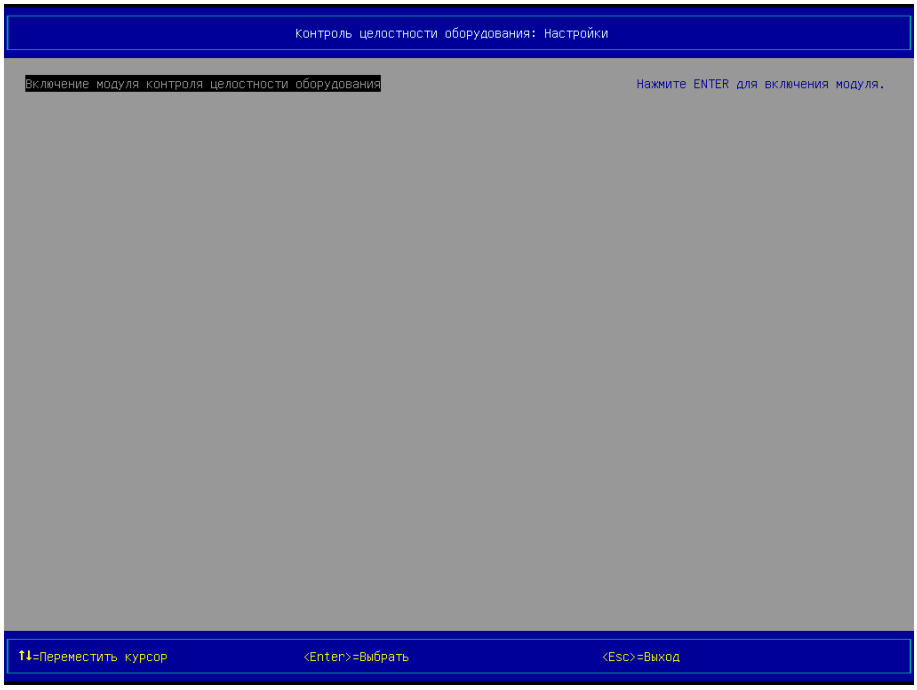


Рисунок 3.113 – Страница *Контроль целостности оборудования: Настройки* (вид 1), пункт для включения модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.114), запрашивающее подтверждение на включение модуля;

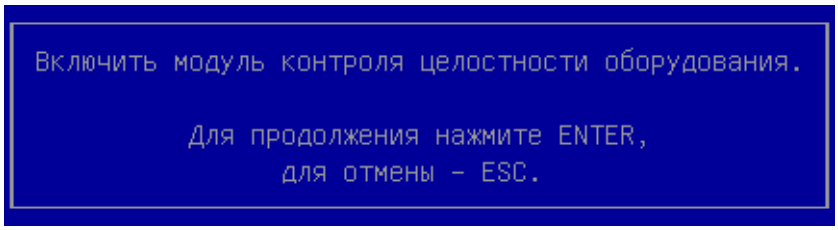


Рисунок 3.114 – Запрос подтверждения на включение *Модуля контроль целостности оборудования*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля безопасности *Контроль целостности оборудования*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.20).

3.10.2 Проверка целостности системного блока

Администратору предоставляется возможность активации функции контроля целостности системного блока. Этот параметр реагирует на вскрытие корпуса системного блока. После активации функции и вскрытия корпуса системного блока пройти процедуру аутентификации сможет только пользователь с правами Администратора.

Для активации функции контроля целостности системного блока следует:

1) выбрать пункт *Электронный замок “Витязь”* в главном меню KSS (см. Рисунок 3.4);

2) → [Enter] на клавиатуре, на экран выводится страница *Электронный замок “Витязь”* (см. Рисунок 3.7);

3) выбрать пункт *Конфигурация* в разделе *Выберите действие*;

4) → [Enter] на клавиатуре, на экран выводится страница *Конфигурация* (см. Рисунок 3.115);

Рисунок 3.115 – Страница *Конфигурация* (вид 4), *Проверка целостности системного блока*

5) выбрать строку *Проверка целостности системного блока*;

6) активировать функцию контроля целостности системного блока → [Enter] на клавиатуре;

7) деактивировать функцию контроля целостности системного блока → [Enter] на клавиатуре.

8) → [Esc] на клавиатуре, для выхода.

Примечания:

1. Активация функции контроля целостности системного блока возможна только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. Нарушение параметра *Целостность системного блока* аналогично нарушению параметров КЦ ФС и КЦ оборудования и приводит к блокировке загрузки ОС.

3. Информация о работе *Модуля контроля целостности системного блока* записывается в Журнал событий. Сигнал поступает от датчика вскрытия системного блока при снятии защитного кожуха системного блока с возможностью доступа к компонентам компьютера.

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

3.10.3 Выключение КЦ оборудования

Для выключения КЦ оборудования следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Контроль целостности оборудования* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности оборудования: Настройки* (см. Рисунок 3.116) с пунктом *Выключение модуля контроля целостности оборудования*;

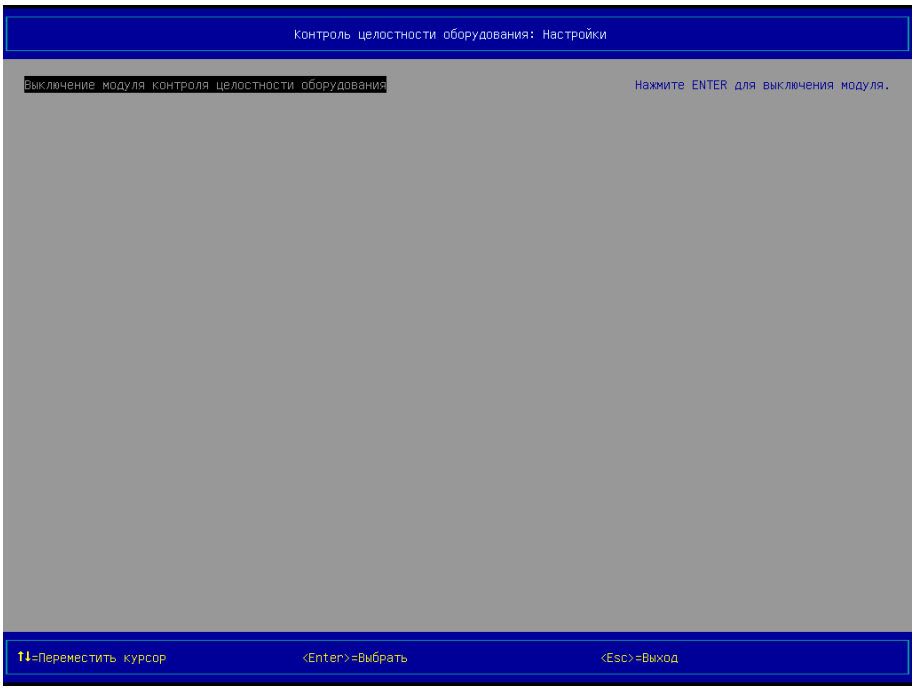


Рисунок 3.116 – Страница *Контроль целостности оборудования: Настройки* (вид 2), пункт выключение модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.117), запрашивающее подтверждение на выключение модуля;

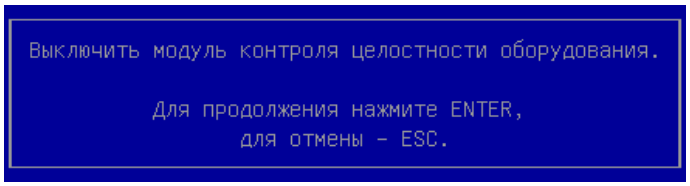


Рисунок 3.117 – Диалоговое окно, запрашивающее подтверждение на выключение модуля *Контроль целостности оборудования*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля безопасности *Контроль целостности оборудования*, на экран выводится страница *Настройки*, статус модуля изменяется с «Вкл» на «Выкл» (см. Рисунок 3.5).

3.10.4 Вывод результата последнего выполнения процедуры КЦ оборудования

Для вывода результата последнего выполнения процедуры КЦ оборудования следует:

1) выбрать пункт *Контроль целостности оборудования* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности оборудования* (см. Рисунок 3.118, Рисунок 3.119);

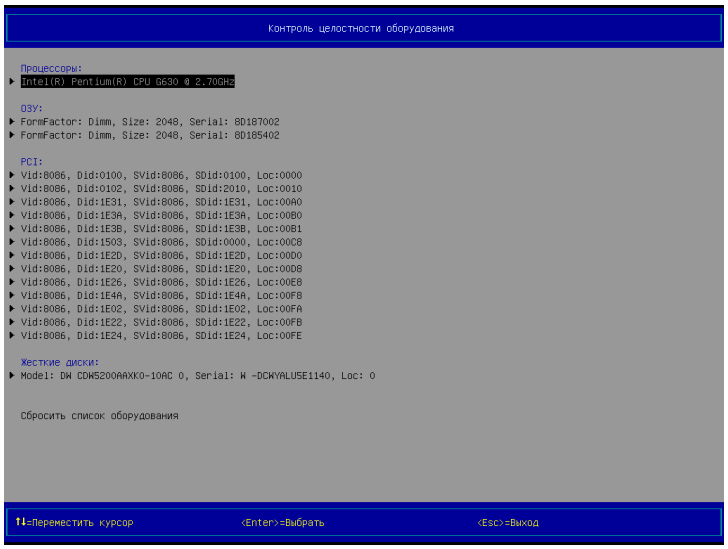


Рисунок 3.118 – Страница *Контроль целостности оборудования* (вид 1), с положительным результатом проверки

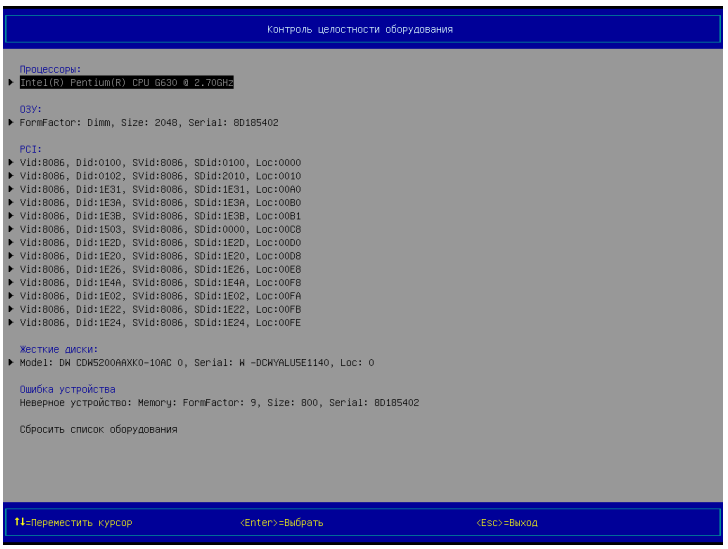


Рисунок 3.119 – Страница *Контроль целостности оборудования* (вид 2), с отрицательным результатом проверки

3) → [Esc] на клавиатуре, для возврата в главном меню KSS.

Примечания:

1. Вывод результата последнего выполнения процедуры КЦ оборудования возможен только после включения модуля безопасности *Контроль целостности оборудования* (см. п. 3.10) и первой перезагрузки персонального компьютера для создания контрольного списка оборудования.

2. При возникновении *Ошибки устройства* и последующем устранении ошибки, путем замены старого устройства на новое, необходимо выбрать пункт *Сбросить список оборудования*, для создания нового списка, при следующей перезагрузке для контроля целостности новой конфигурации оборудования (см. пункт 3.10.5).

3. Информация от *Модуля контроля целостности оборудования* сохраняется в *Журнале событий* (см. пункт 3.12).

4. Если записи о результате последнего выполнения процедуры КЦ оборудования, выводимые на странице *Результат последней проверки*, не умещаются в области № 2 оболочки KSS, то в данной области выводятся стрелки красного цвета: ↑ – дополнительные записи располагаются выше, ↓ – дополнительные записи располагаются ниже.

5. Перемещение по записям в области № 2 оболочки KSS выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре.

6. Постраничный вывод записей в области № 2 оболочки KSS выполняется с помощью клавиш [Page Up], [Page Down], расположенных на клавиатуре.

3.10.5 Сброс списка оборудования, подлежащего КЦ

Сброс списка оборудования применяется для обновления данных при контроле целостности оборудования.

Для сброса списка оборудования, подлежащего КЦ, следует:

1) выбрать пункт *Контроль целостности оборудования* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности оборудования* (см. Рисунок 3.118, Рисунок 3.119);

3) выбрать пункт *Сбросить список оборудования*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.120), запрашивающее подтверждение на сброс списка оборудования;

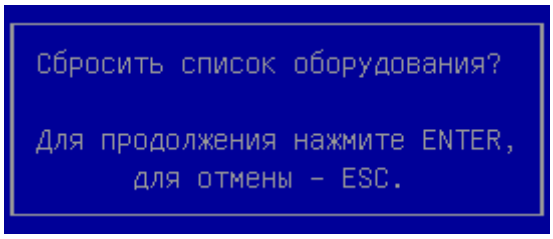


Рисунок 3.120 – Запрос подтверждения на сброс списка оборудования

5) → [Enter] на клавиатуре, после выполнения данного действия происходит сброс ранее созданного списка оборудования, подлежащих КЦ.

6) → [Esc] на клавиатуре, для возврата в главном меню KSS.

Примечание. Сбросить список оборудования, подлежащих КЦ, возможно только после включения модуля безопасности *Контроль целостности оборудования* (см. п. 3.10).

3.11 Логические диски

3.11.1 Включение модуля *Логические диски*

Для включения модуля *Логические диски* следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

3) выбрать пункт *Логические диски* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки модуля логических дисков* (см. Рисунок 3.121) с пунктом *Включение модуля управления логическими дисками*;

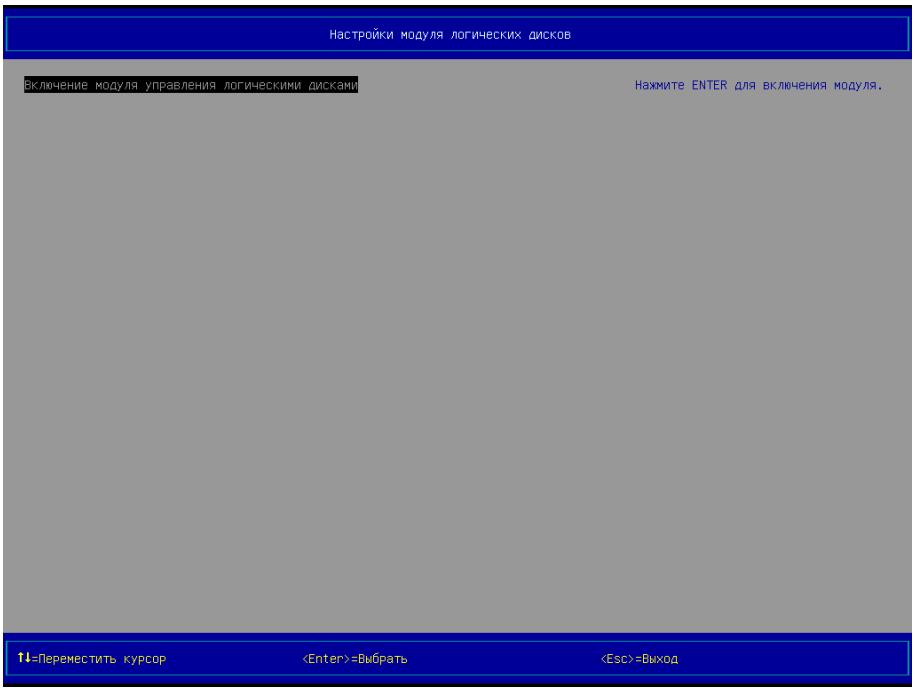


Рисунок 3.121 – Страница *Настройки модуля логических дисков* (вид 1), пункт *Включение модуля управления логическими дисками*

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.122), запрашивающее подтверждение на включение модуля;

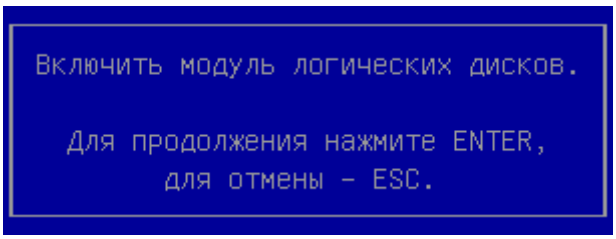


Рисунок 3.122 – Запрос подтверждения на *включение модуля управления логическими дисками*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля *Управление логическими дисками*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.20).

3.11.2 Выключение модуля *Логические диски*

Для выключения модуля *Логические диски* следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Логические диски* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки модуля логических дисков* (см. Рисунок 3.123) с пунктом *Выключение модуля управления логическими дисками*;

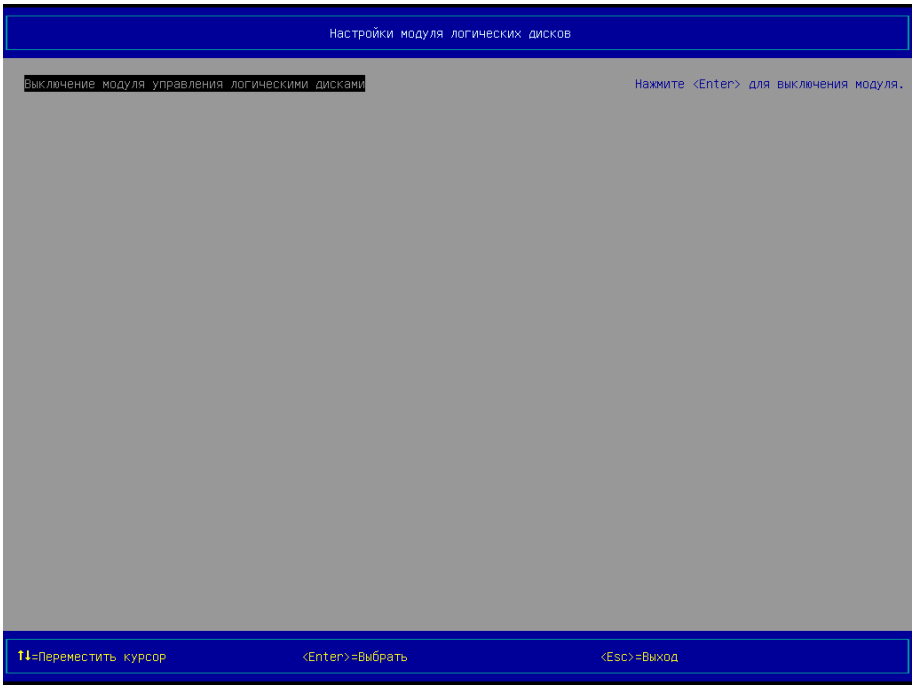


Рисунок 3.123 – Страница *Настройки модуля логических дисков* (вид 2), пункт *Выключение модуля управления логическими дисками*

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.124), запрашивающее подтверждение на выключение модуля;

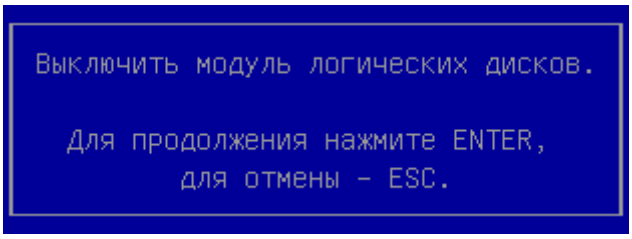


Рисунок 3.124 – Запрос подтверждения на
Выключение модуля управления логическими дисками

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля *Управление логическими дисками*, на экран выводится страница *Настройки*, статус модуля изменяется с «Вкл» на «Выкл» (см. Рисунок 3.5).

3.11.3 Редактирование имен логических дисков

В момент первого запуска, KSS присваивает каждому разделу на жестком диске или устройству собственное имя диска, которое по умолчанию выглядит как «fs0, fs1, fs2, fs3 и т.д». Для удобства работы с файлами рекомендуется присваивать дискам новые, ассоциативные имена, по которым диск легче распознать, например, раздел с операционной системой назвать «System».

Примечание. Измененное имя диска будет присутствовать на всех страницах KSS, в т.ч. и в файловом менеджере, при выборе файлов для контроля целостности файловой системы.

Чтобы переименовать диск или устройство, выполните следующие действия:

1) выбрать пункт *Логические диски* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Логические диски* (см. Рисунок 3.125).

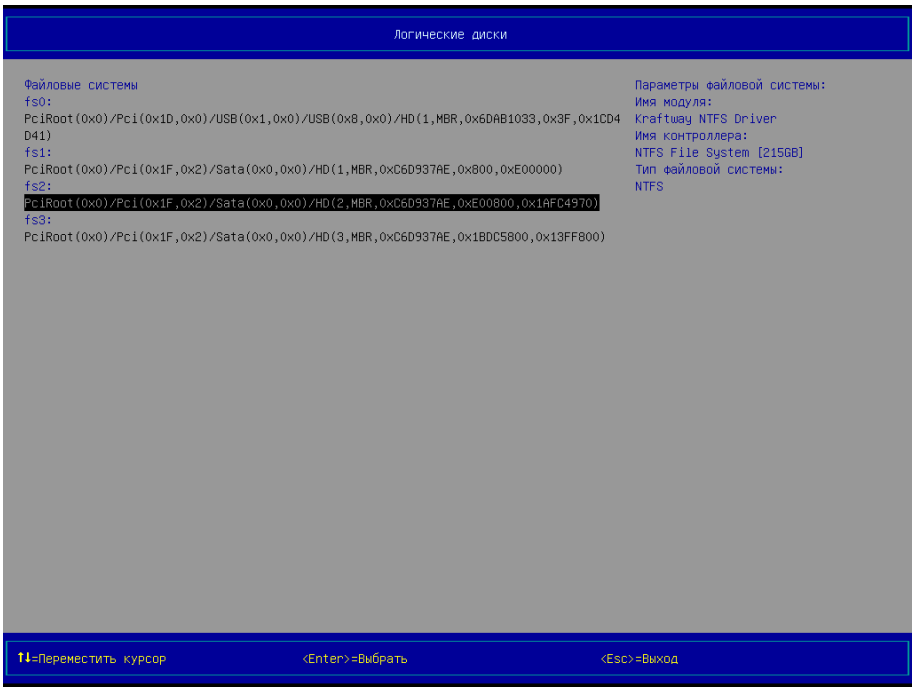


Рисунок 3.125 – Логические диски (вид 1)

3) выбрать требуемый для переименования диск в разделе *Файловые системы* при помощи клавиш [↑], [↓], расположенных на клавиатуре. Дополнительная информация о диске отображается в правой верхней части области № 2:

- имя модуля,
- имя контроллера,
- размер диска в Гб,
- тип файловой системы;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.126), с предложением ввести новое имя для выбранного диска;

Рисунок 3.126 – Окно *Введите имя* (вид 1),
имя диска, присвоенное KSS

5) → [Backspace] на клавиатуре, для удаления символов старого имени диска;

6) ввести новое имя диска, при помощи буквенного блока клавиатуры (см. Рисунок 3.127);

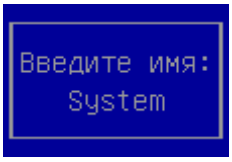


Рисунок 3.127 – Окно *Введите имя* (вид 2),
имя диска, присвоенное пользователем

7) → [Enter] на клавиатуре, новое имя диска сохранится в KSS (см. Рисунок 3.128);

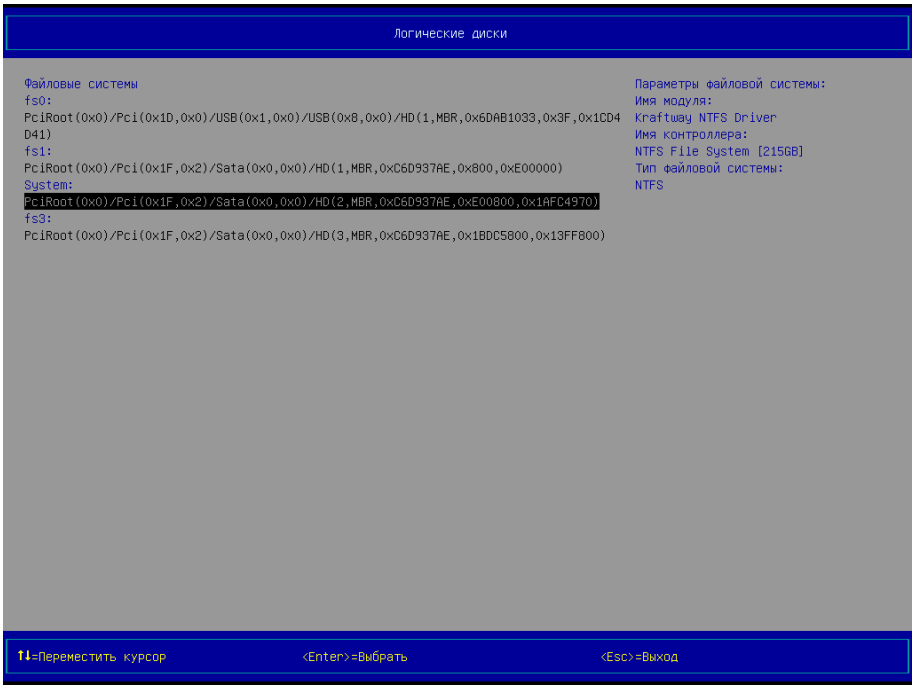


Рисунок 3.128 – Логические диски (вид 2)

8) → [Esc] на клавиатуре, для окончания работы на странице *Логические диски*.

3.12 Журнал событий

Записи о событиях всех модулей безопасности ЭЗ «Витязь» заносятся в общий Журнал событий.

3.12.1 Включение модуля *Журнал событий*

Для включения модуля управления *Журналом событий* следует:

7) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

8) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.5);

9) выбрать пункт *Журнал событий* в разделе *Настройки модулей безопасности*;

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление журналом событий: Настройки* (см. Рисунок 3.129) с пунктом *Включение модуля управления журналом событий*;

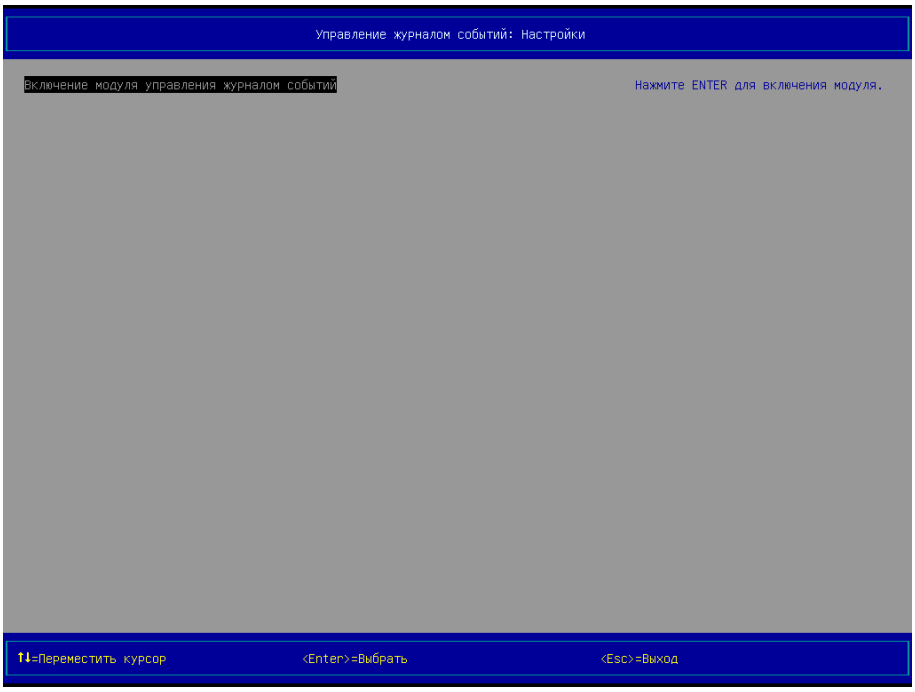


Рисунок 3.129 – Страница *Управление журналом событий: Настройки* (вид 1), пункт *Включение модуля управления журналом событий*

11) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.130), запрашивающее подтверждение на включение модуля;

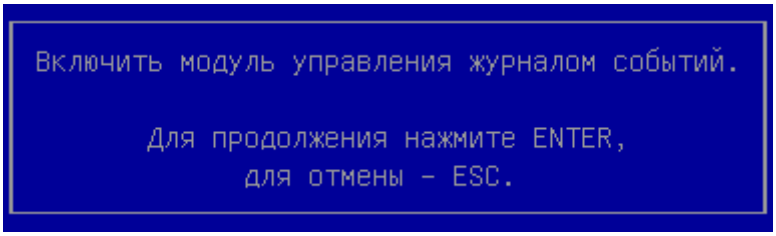


Рисунок 3.130 – Запрос подтверждения на
включение модуля управления журналом событий

12) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля *Управление журналом событий*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.20).

3.12.2 Выключение модуля *Журнал событий*

Для выключения модуля *Журнал событий* следует:

7) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

8) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

9) выбрать пункт *Журнал событий* в разделе *Настройки модулей безопасности*;

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление журналом событий: Настройки* (см. Рисунок 3.131) с пунктом *Выключение модуля управления журналом событий*;

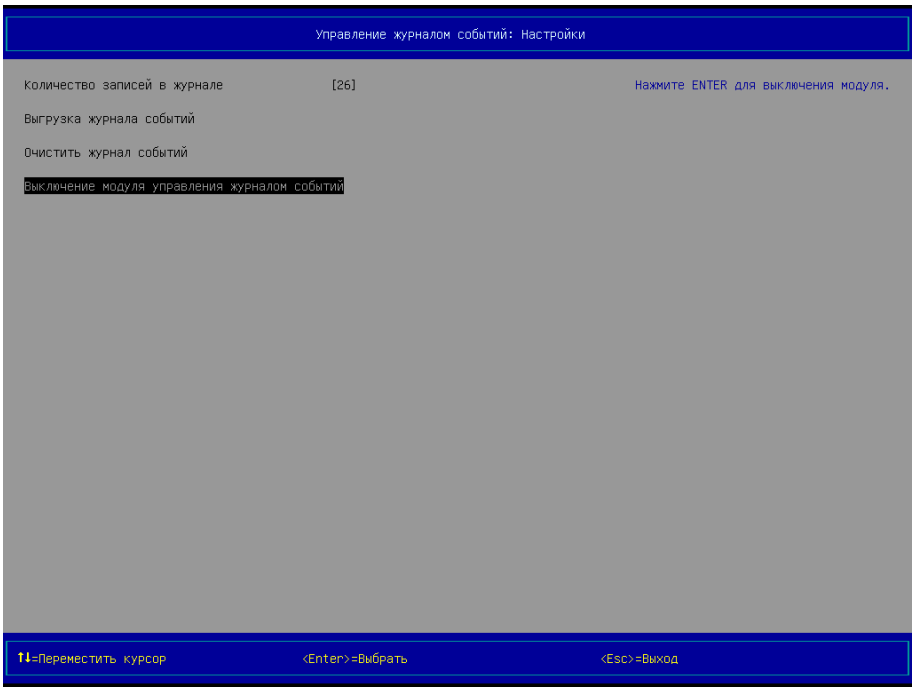


Рисунок 3.131 – Страница *Управление журналом событий: Настройки* (вид 2), пункт *Выключение модуля управления журналом событий*

11) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.132), запрашивающее подтверждение на выключение модуля;

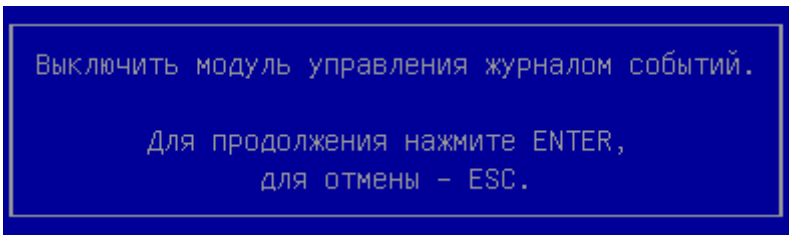


Рисунок 3.132 – Запрос подтверждения на *Выключение модуля управления журналом событий*

12) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля *Управление журналом событий*, на экран выводится страница *Настройки*, статус модуля изменяется с «Вкл» на «Выкл» (см. Рисунок 3.5).

3.12.3 Просмотр журнала событий

Для просмотра журнала событий следует:

1) выбрать пункт *Журнал событий* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Журнал событий* (см. Рисунок 3.133).

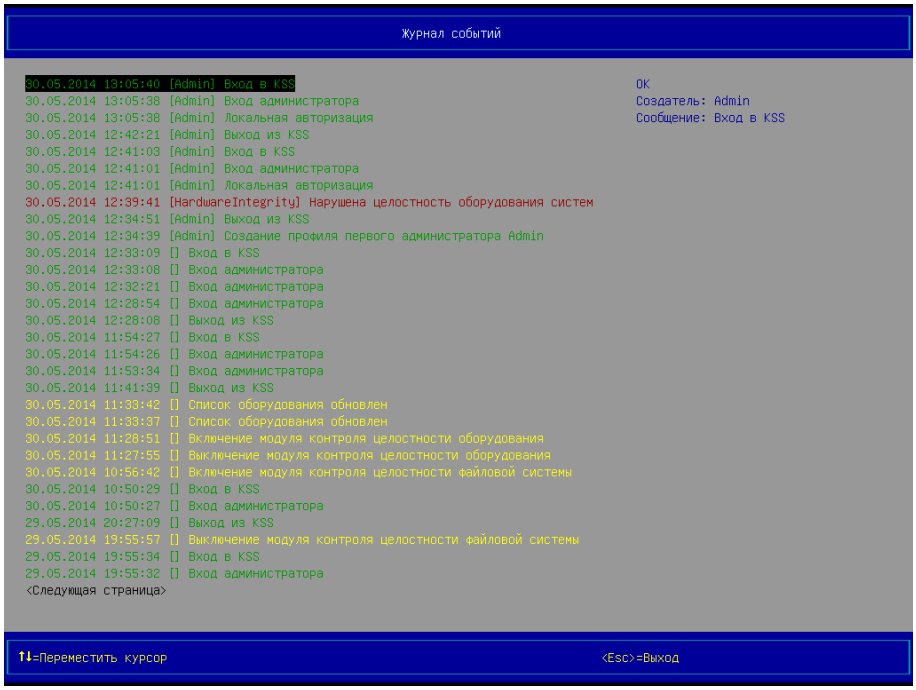


Рисунок 3.133 – Страница *Журнал событий*

Формат записи журнала событий:

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

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

Примечания:

1. Просмотр журнала событий ЭЗ возможен только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. Перемещение по строкам записей журнала событий ЭЗ выполняется при помощи клавиш [↑], [↓], расположенных на клавиатуре.

3. Перемещение курсора на первую и последнюю строки записей журнала событий ЭЗ выполняется при помощи клавиш [Page Up], [Page Down], расположенных на клавиатуре.

4. Постраничный вывод записей журнала событий ЭЗ выполняется при помощи клавиши [Enter], расположенной на клавиатуре, при перемещении курсора на строку <Следующая страница>.

5. В ЭЗ 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 контроля целостности оборудования.

– Красный – Ошибка. Событие обозначает нарушение контроля целостности системы. Например, когда нарушена целостность оборудования системы.

3.12.4 Сохранение журнала событий ЭЗ в файл

Для сохранения журнала событий ЭЗ в файл следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Журнал событий* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление журналом событий: Настройки* (см. Рисунок 3.134) с пунктом *Выгрузка журнала событий*;

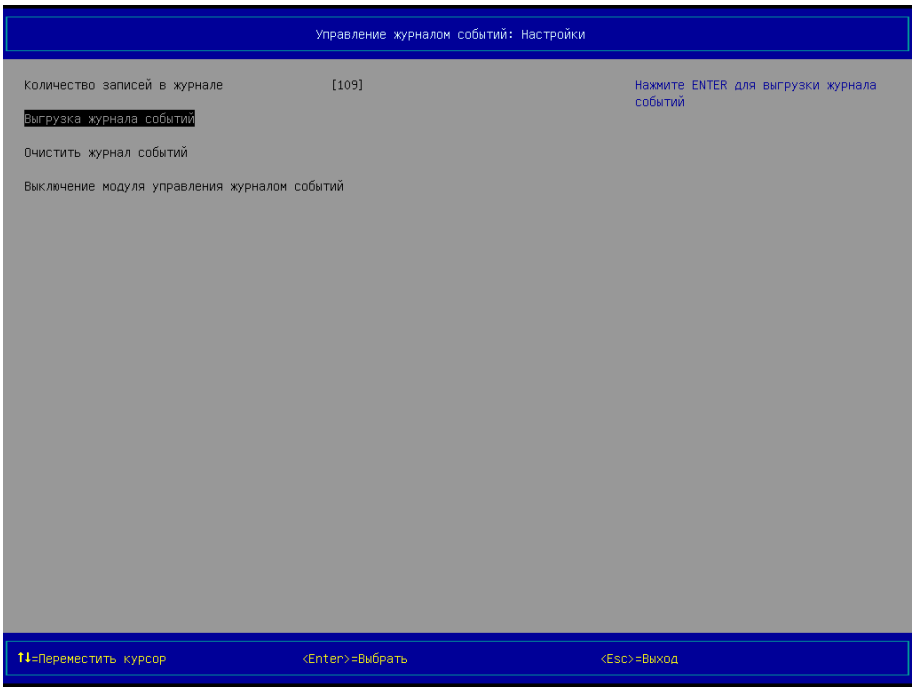


Рисунок 3.134 – *Управление журналом событий: Настройки, Выгрузка журнала событий*

5) подключить USB-диск к свободному USB-порту компьютера;

6) выбрать пункт *Выгрузка журнала событий*;

7) →[Enter] на клавиатуре, после выполнения данного действия 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, а на экран выводится окно (см. Рисунок 3.135), информирующее администратора об успешном сохранении журнала событий;

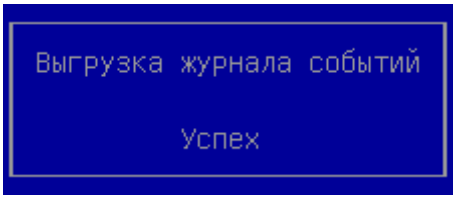


Рисунок 3.135 – Успешное сохранение журнала событий

8) нажать любую клавишу на клавиатуре.

Примечания:

1. Сохранение журнала событий ЭЗ в файл возможно только после включения модуля безопасности *Электронный замок “Витязь”* (см. п. 3.4).

2. Перемещение между строками меню осуществляется при помощи клавиш [↑], [↓], расположенных на клавиатуре.

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

4. При отсутствии подключенного USB-диска к компьютеру, после нажатия на клавишу [F10] на экран выводится окно (см. Рисунок 3.136), информирующее об отсутствии устройства памяти.

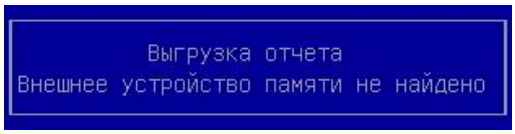


Рисунок 3.136 – Окно, информирующее об отсутствии устройства памяти

5. Если сохранить журнал событий в файл невозможно, то на экран выводится окно (см. Рисунок 3.137).

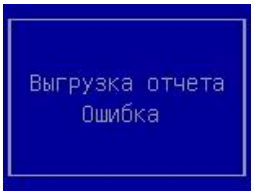


Рисунок 3.137 – Сохранить журнал в файл невозможно

3.12.5 Очистка журнала событий

Для очистки журнала событий следует:

1) выбрать пункт *Настройки* в разделе *Конфигурация*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Настройки* (см. Рисунок 3.20);

3) выбрать пункт *Журнал событий* в разделе *Настройки модулей безопасности*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление журналом событий: Настройки* (см. Рисунок 3.138) с пунктом *Очистить журнал событий*;

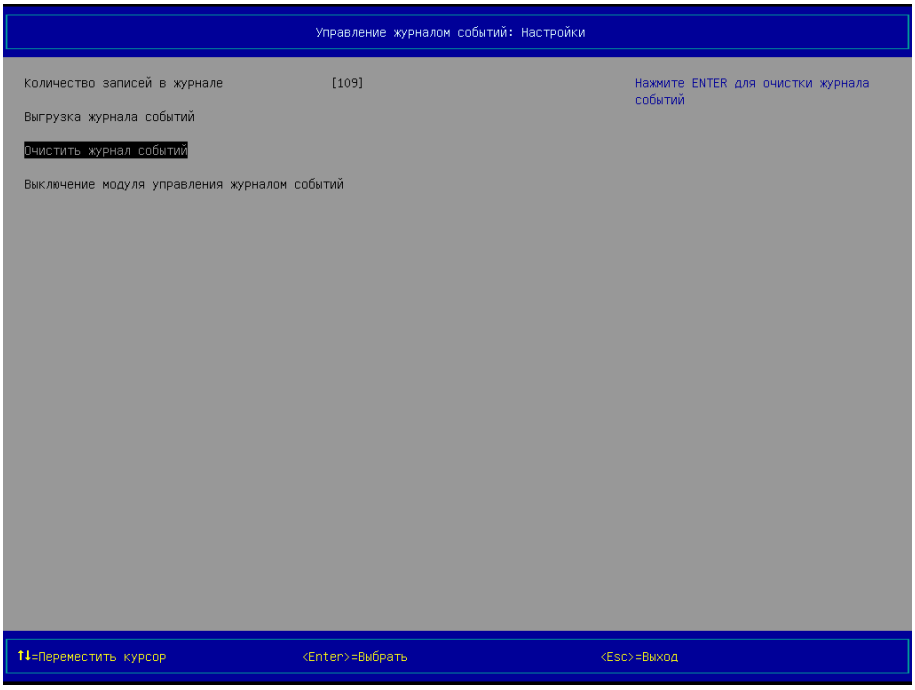


Рисунок 3.138 – *Управление журналом событий: Настройки, Очистить журнал событий*

5) выбрать пункт *Очистить журнал событий*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.139), запрашивающее подтверждение на очистку журнала событий;

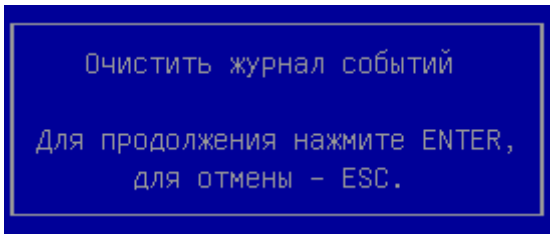


Рисунок 3.139 – Запрос подтверждения на очистку журнала событий

7) → [Enter] на клавиатуре, после выполнения данного действия происходит очистка ранее сформированного журнала событий;

8) → [Esc] на клавиатуре, для возврата на страницу.

3.13 Модуль безопасности *Антивирус*

3.13.1 Включение и выключение антивирусной проверки

Чтобы включить или выключить антивирусную проверку, выполните следующие действия:

1) нажмите клавишу F1 после включения компьютера.

2) программа перейдет в среду Kraftway Secure Shell.

3) в среде Kraftway Secure Shell перейдите в раздел *Настройка*.

4) выберите пункт *Антивирус Касперского для UEFI* и нажмите клавишу [ENTER].

5) откроется страница *Антивирус Касперского для UEFI* (см. Рисунок 3.140).

Рисунок 3.140 - Антивирус Касперского для UEFI

6) выберите пункт *Включить Антивирус Касперского для UEFI* и нажмите клавишу [ENTER].

7) Программа отобразит окно с текстом *Лицензионного соглашения*.

Текст *Лицензионного соглашения* приводится в сокращенном виде. Полный текст *Лицензионного соглашения* вы можете прочитать на официальном сайте «Лаборатории Касперского»
http://support.kaspersky.ru/kuefi/eula.

8) Далее выполните одно из следующих действий:

- Если вы согласны с условиями *Лицензионного соглашения*, нажмите на кнопку [Принять]. Для параметра *Включить Антивирус Касперского для UEFI* будет установлено значение [X]. Если Лицензионное соглашение принято, подсистема проверки Антивируса Касперского выполняет антивирусную проверку критически важных областей операционной системы и папок, используемых операционной системой, перед ее загрузкой.

- Если вы не согласны с условиями *Лицензионного соглашения*, нажмите на кнопку [Отказаться]. Значение параметра *Включить Антивирус Касперского для UEFI* не изменится. Если *Лицензионное* соглашение не принято, подсистема проверки Антивируса Касперского не выполняет антивирусную проверку критически важных областей операционной системы и папок, используемых операционной системой, перед ее загрузкой.

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

Примечание.

1. Параметр будет применен на компьютере после выхода из среды Kraftway Security Shell и перезагрузки компьютера.

2. По умолчанию антивирусная проверка выключена.

3.13.2 Включение и выключение загрузки антивирусных баз

Чтобы включить или выключить загрузку антивирусных баз из пользовательской папки, выполните следующие действия:

1) нажмите клавишу F1 после включения компьютера.

2) программа перейдет в среду Kraftway Secure Shell.

3) в среде Kraftway Secure Shell перейдите в раздел *Настройка*.

4) выберите пункт *Антивирус Касперского для UEFI* и нажмите клавишу [ENTER].

5) в списке *Параметры проверки* выберите пункт *Загружать антивирусные базы из*.

6) с помощью клавиши [ENTER] выберите один из следующих вариантов значения параметра:

- *Пользовательской папки* – антивирусные базы загружаются из пользовательской папки;

- *Папки по умолчанию* – антивирусные базы загружаются из папки, заданной по умолчанию.

Примечание.

1. Если загрузка антивирусных баз из пользовательской папки включена, но путь к папке не указан, подсистема проверки Антивируса Касперского по умолчанию выполнит поиск антивирусных баз в корневых папках всех дисков.

2. Параметр будет применен на компьютере после выхода из среды Kraftway Security Shell и перезагрузки компьютера.

3.13.3 Настройка пути к пользовательской папке

Чтобы настроить путь к пользовательской папке, выполните следующие действия:

1) Нажмите клавишу F1 после включения компьютера.

2) Программа перейдет в среду Kraftway Secure Shell.

3) В среде Kraftway Secure Shell перейдите в раздел *Настройка*.

4) Выберите пункт Антивирус Касперского для UEFI и нажмите клавишу [ENTER].

5) В списке *Параметры проверки* выберите пункт *Путь к пользовательской папке* и нажмите клавишу [ENTER].

6) В поле ввода укажите путь к пользовательской папке, из которой подсистема проверки будет загружать антивирусные базы.

Пример:

/var/db/kraftway/kuefi bases

kraftway\kuefi_bases

Примечание.

1. Указывайте полный путь к пользовательской папке.

2. Для всех файловых систем учитывается регистр при указании пути к пользовательской папке. Если при указании пути будет допущена ошибка в написании регистра, программа не найдет антивирусные базы во время антивирусной проверки.

3. Не используйте маски или переменные окружения при указании пути к пользовательской папке.

4. Не используйте имя диска при указании пути к пользовательской папке. Подсистема проверки Антивируса Касперского выполняет поиск пользовательской папки с антивирусными базами на всех дисках.

5. Если путь к папке задан неверно, программа отобразит сообщение об ошибке.

6. Если по указанному к папке пути подсистема проверки Антивируса Касперского не находит антивирусные базы во время антивирусной проверки, то загрузка операционной системы блокируется (см. Рисунок 3.141).

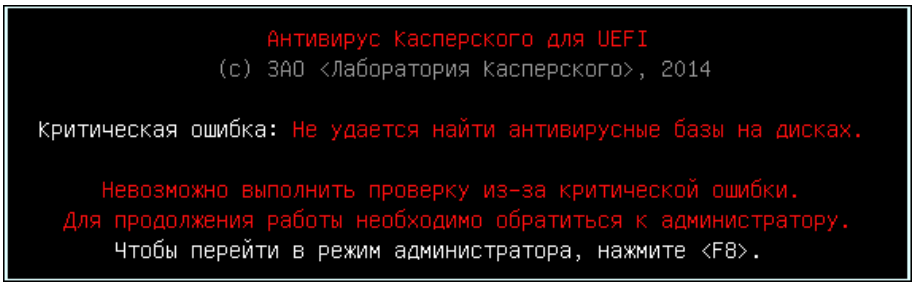


Рисунок 3.141 – Антивирус. Не удается найти антивирусные базы

7. Параметр будет применен на компьютере после выхода из среды Kraftway Security Shell и перезагрузки компьютера.

3.13.4 Исключение файлов из проверки

Чтобы исключить файлы из антивирусной проверки, выполните следующие действия:

1) нажмите клавишу F1 после включения компьютера.

2) программа перейдет в среду Kraftway Secure Shell.

3) в среде Kraftway Secure Shell перейдите в раздел *Настройка*.

4) выберите пункт *Антивирус Касперского для UEFI* и нажмите клавишу [ENTER].

5) в списке *Параметры проверки* выберите пункт *Пропускать файлы при проверке* и нажмите клавишу [ENTER].

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

Примечание.

1. Не используйте имя диска при указании пути к файлам. Подсистема проверки Антивируса Касперского выполняет поиск указанных файлов, масок имен файлов и путей к файлам на всех дисках.

2. Используйте знак «*» после имени папки, чтобы исключить из антивирусной проверки все файлы, расположенные в ней.

Пример:

\kav\logs*

3. Имена файлов записывайте в одну строку. В качестве разделителя используйте запятую или точку с запятой. Максимальное количество символов в строке – 255.

4. Для всех файловых систем учитывается регистр при задании имени файла и маски файла.

5. По умолчанию список файлов, исключенных из антивирусной проверки, пуст.

6. Параметр будет применен на компьютере после выхода из среды Kraftway Security Shell и перезагрузки компьютера.

7. Во время проверки критически важных областей операционной системы и папок, используемых операционной системой при загрузке, подсистема проверки будет пропускать указанные файлы.

3.13.5 Обновление антивирусных баз

Обновление антивирусных баз проводится Администратором вручную без применения средств автоматизации.

Источник обновлений антивирусных баз – локальная папка, содержащая файлы обновления антивирусных баз программы Антивирус Касперского.

Для того чтобы обновить антивирусные базы следует:

1) скачайте антивирусные базы из доверенного источника (сайта производителя антивирусных средств или производителя СДЗ);

2) проверьте целостность нового файла антивирусной базы;

3) скопируйте файл новой антивирусной базы в пользовательскую папку, путь к которой был ранее задан в настройках.

Файлы антивирусной базы содержит только информацию о вредоносном коде и не является исполняемым, поэтому его обновление нельзя рассматривать как обновление ПК ЭЗ Витязь 2.2.

Выполнение операции по обновлению антивирусных баз производится после завершения работы СДЗ.

3.14 Вход в программу настройки UEFI материнской платы

Администраторы Тип1 и Тип2 (см. п. 1.6), обладающие правом доступа к настройкам UEFI, могут входить в программу настройки UEFI материнской платы.

3.14.1 Вход в графический интерфейс UEFI при выключенном ЭЗ

Для входа в графический интерфейс UEFI материнской платы при выключенном ЭЗ следует:

1) включить персональный компьютер, после выполнения данного действия на экране монитора отображается Logo-изображение материнской платы компьютера (см. Рисунок 3.38), на следующем шаге загрузки на экран выводится приглашение на вход в KSS (см. Рисунок 3.42);

2) → [Delete] на клавиатуре в момент вывода на экран приглашения на вход в KSS, после выполнения данного действия приглашение на вход в KSS пропадает с экрана;

3) повторно нажать на клавишу [Delete] на клавиатуре, после выполнения данного действия на экран выводится графический интерфейс программы UEFI материнской платы.

3.14.2 Вход в графический интерфейс UEFI при включённом ЭЗ

Для входа в графический интерфейс UEFI материнской платы при включённом ЭЗ следует:

1) включить персональный компьютер;

2) пройти процедуру аутентификации в ЭЗ (см. п. 3.5);

3) → [Delete] на клавиатуре при выводе на экран приглашения на вход в KSS (см. Рисунок 3.42), после выполнения данного действия приглашение на вход в KSS пропадает с экрана;

4) повторно нажать на клавишу [Delete] на клавиатуре, после выполнения данного действия на экран выводится главное окно программы настройки UEFI материнской платы.

4 ПРОВЕРКА ПО

Администратор безопасности должен периодически (не реже одного раза в два месяца) проводить сверку контрольных сумм ПК ЭЗ «Витязь» В2.2 последней проверки КЦ ЭЗ с контрольными суммами, приведёнными в формуляре на данный ЭЗ.

5 СООБЩЕНИЯ АДМИНИСТРАТОРУ

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

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

5.1.1 Отображение информации о нарушении КЦ

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

Отображение информации сгенерированной *Модулем контроля целостности оборудования* на различных страницах и окнах KSS при наступлении одного и того же события – нарушении целостности оборудования.

1. В момент запуска компьютера – Проверка целостности оборудования (см. Рисунок 5.1)

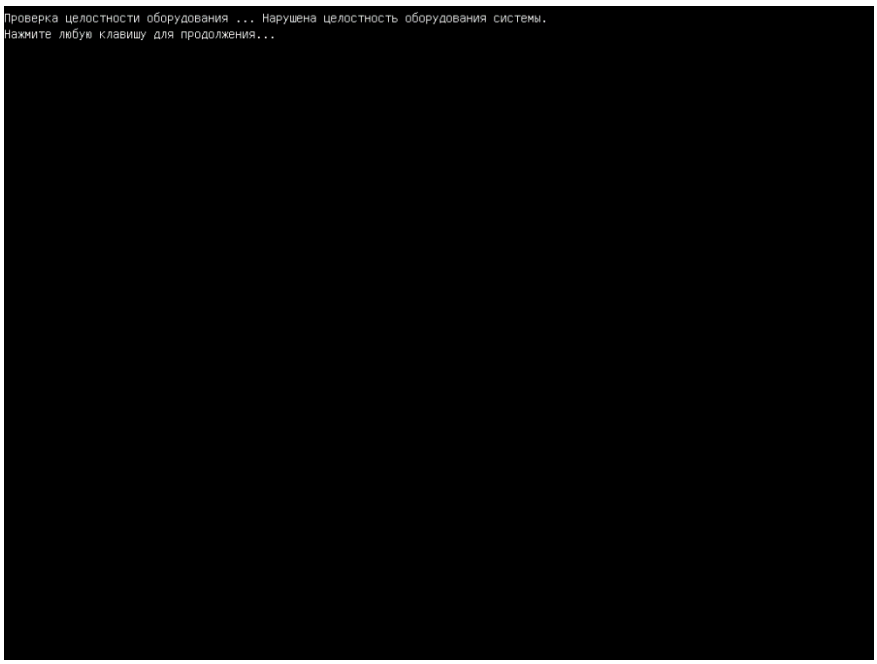


Рисунок 5.1 – Нарушена целостность оборудования системы.

2. В момент запуска графической оболочки KSS (см. Рисунок 5.2).

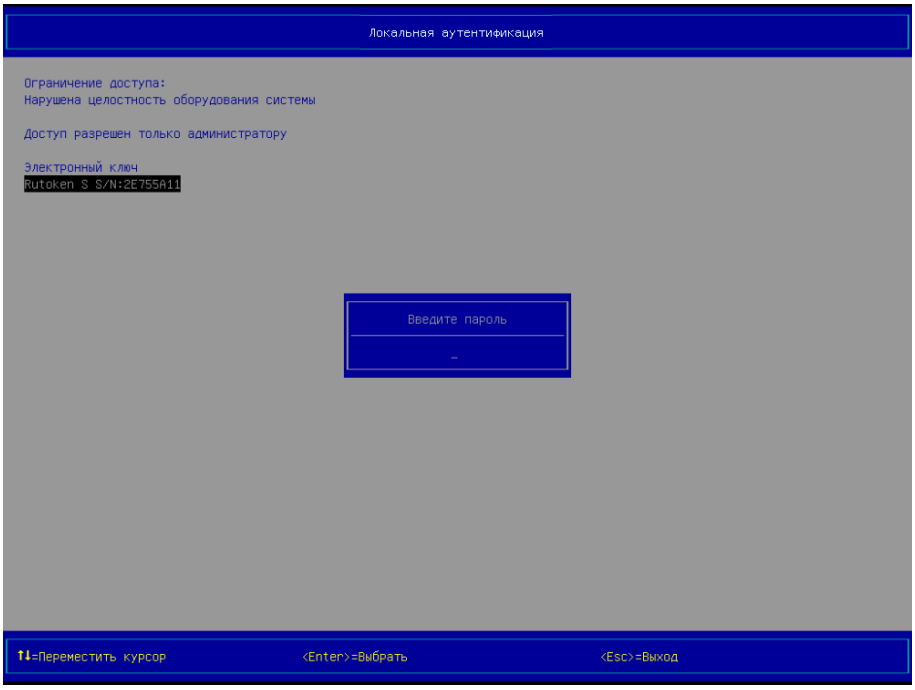


Рисунок 5.2 – Ограничение доступа: Нарушена целостность оборудования системы. Доступ разрешен только администратору.

3. Отчет модуля контроля целостности оборудования (см. Рисунок 5.3)

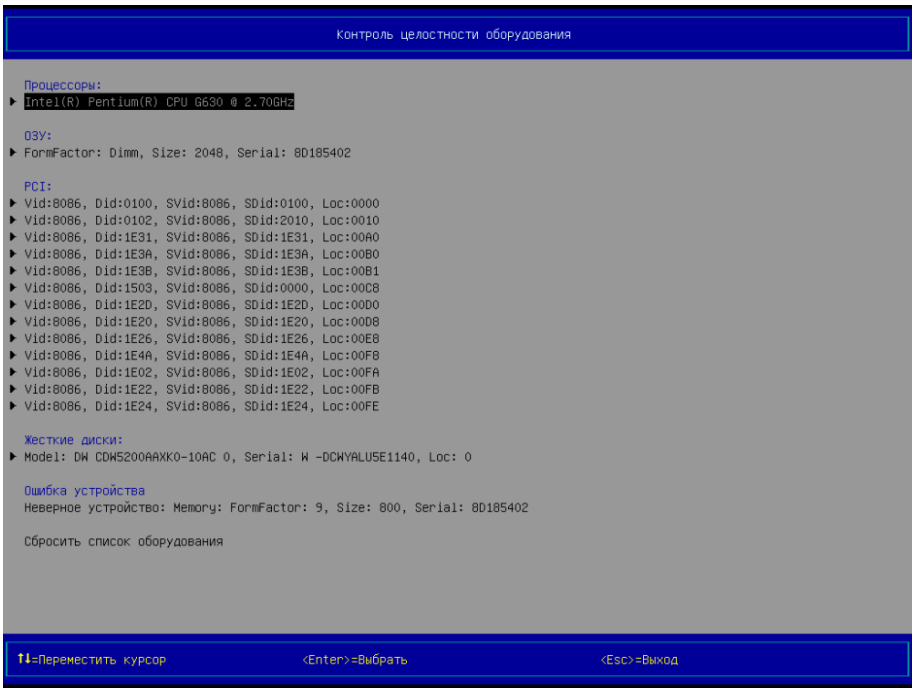


Рисунок 5.3 – Ошибка устройства: Неверное устройств: Memory FormFactor: 9, Size: 800, Serial: 80185402

4. Журнал событий (см. Рисунок 5.4)

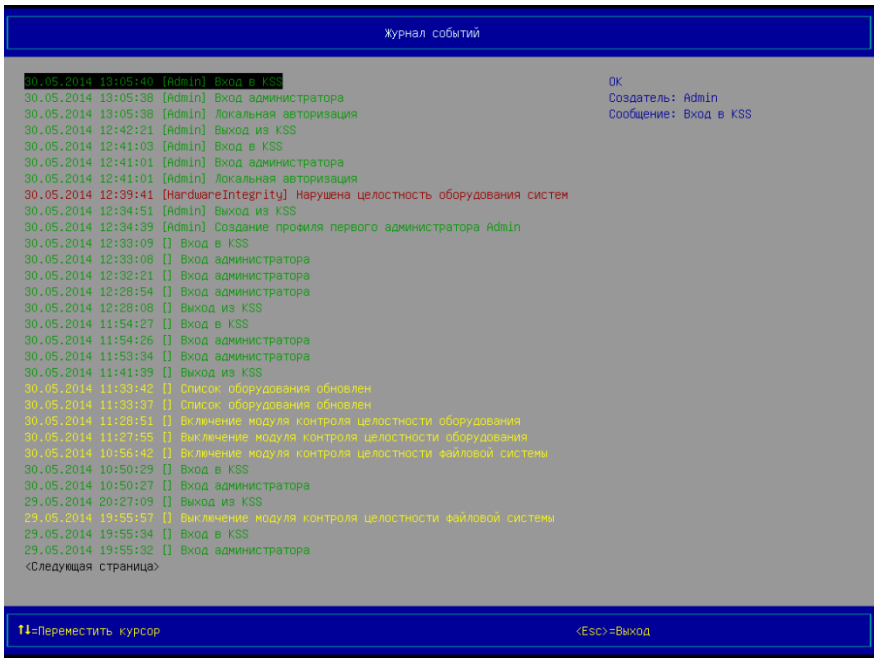


Рисунок 5.4 – Нарушена целостность оборудования системы

5.1.2 Сообщения Администратору в различных ситуациях

Ситуация № 1

Во время выполнения процедуры КЦ для каждого файла, прошедшего проверку, на экран выводится результат данной проверки в виде записи: <Результат проверки>: <путь к файлу, прошедшего проверку> (см. рисунок 5.5). Результат проверки может принимать значения: «Успех», «Не найден», «Ошибка». После завершения процедуры КЦ, ниже всех записей с результатами проверки, выводится итоговая информация о результатах данной процедуры, которая содержит: количество проверенных файлов, количество файлов, которые прошли процедуру КЦ с положительным результатом, количество файлов, которые прошли процедуру КЦ с отрицательным результатом. При отрицательном результате процедуры КЦ, на экран выводятся записи следующего вида (см. рисунок 5.5):

Целостность файловой системы нарушена

Нажмите любую клавишу для продолжения…

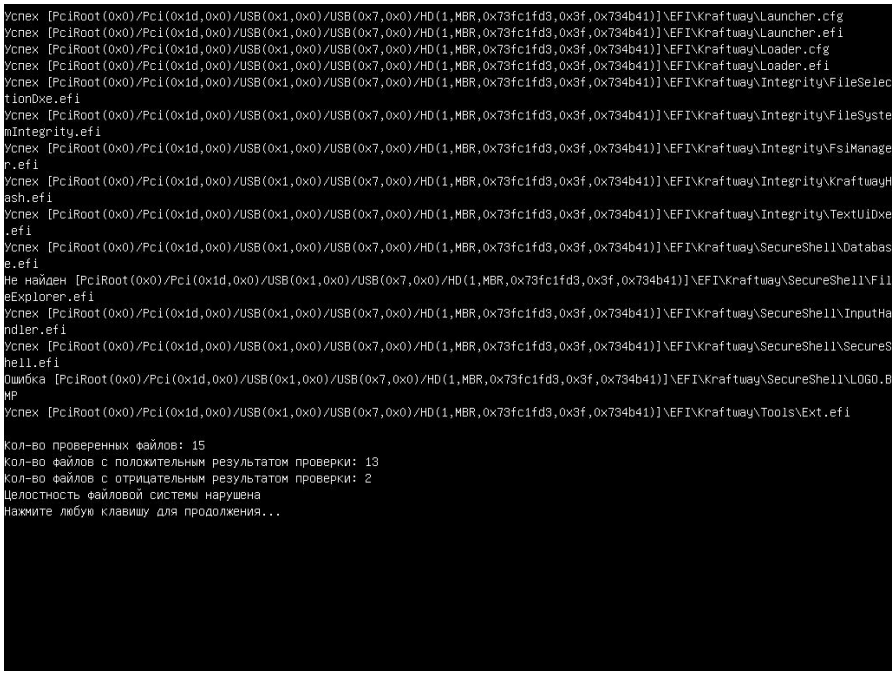


Рисунок 5.5 – Целостность файловой системы нарушена

Решение: при появлении записей такого вида администратору следует: либо обновить контрольные суммы файлов, которые прошли процедуру КЦ с отрицательным результатом, либо удалить эти файлы из списка файлов (данное действие выполняется в том случае, если отрицательный результат КЦ определённых файлов не является критич-

ным). Также администратору следует просмотреть журнал событий ЭЗ и проанализировать данные, хранящиеся в нём, для нахождения причины нарушения целостности файлов.

Ситуация № 2

При отрицательном результате процедуры КЦ, и когда ЭЗ включён, после вывода записей, описанных в ситуации № 1 (см. рисунок 5.5), на экран монитора выводятся записи следующего вида (см. рисунок 5.6):

Ограничение доступа:

Нарушена целостность файловой системы.

Доступ разрешён только администратору

Поиск электронного ключа

Подключите электронный ключ

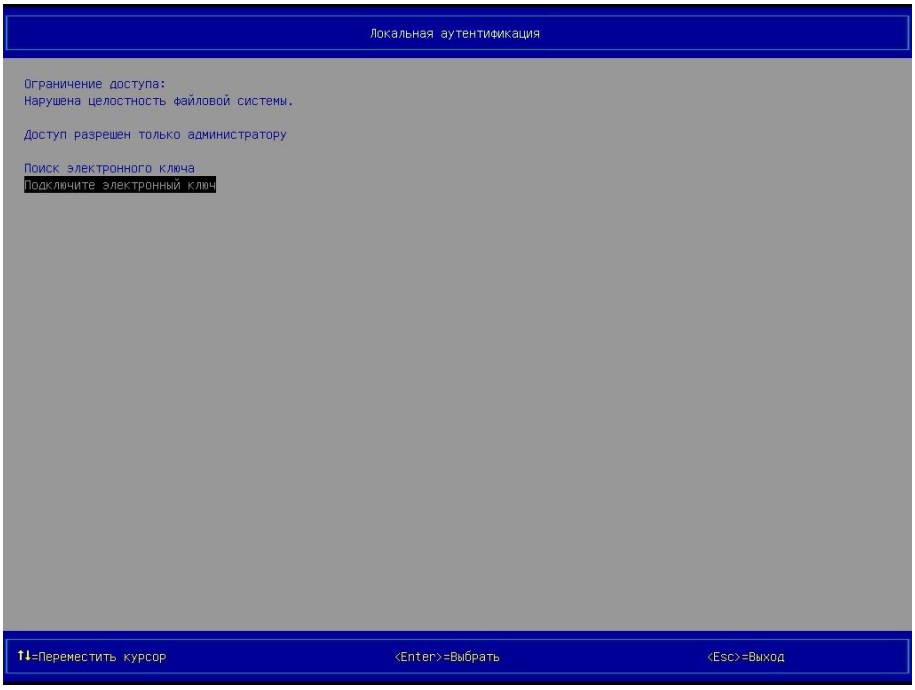


Рисунок 5.6 – Страница *Локальная аутентификация* (вид 5), ЭЗ заблокировал компьютер

Решение: при появлении записей такого вида администратору следует: пройти процедуру аутентификации, далее выполнить действия, приведённые для ситуации № 1.

Ситуация № 3

Если текущий пароль пользователя был введён неправильно во время его аутентификации, то на экран выводится окно (см. рисунок 5.7), информирующее о том, что был введён неверный пароль.

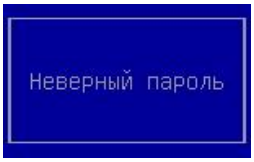


Рисунок 5.7 – Неправильно введён пароль

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

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

Ситуация № 4

Если количество неправильно введённого пароля пользователя во время его аутентификации равно значению параметра *Максимальное количество попыток ввода пароля* (см. п. 3.6), то после нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 5.8), информирующее о превышении количества попыток ввода пароля, после повторного нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 5.7), информирующее о том, что был введён неверный пароль, а после третьего нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 5.9), информирующее о попытке входа заблокированного пользователя.

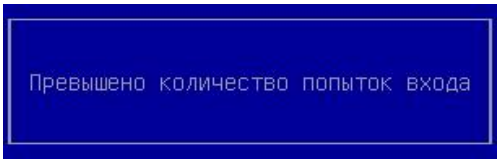


Рисунок 5.8 – Превышено количество попыток ввода пароля

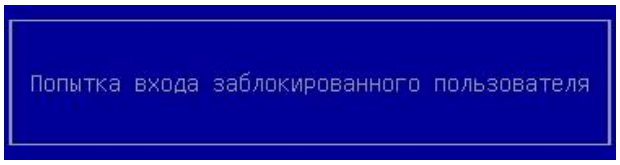


Рисунок 5.9 – Попытка входа заблокированного пользователя

Решение: администратору следует отключить АН пользователя от USB-порта персонального компьютера, профиль которого был заблокирован, пройти процедуру аутентификации в ЭЗ с помощью АН администратора, войти в оболочку KSS, разблокировать профиль пользователя, профиль которого был заблокирован.

Ситуация № 5

Если после включения персонального компьютера, во время процедуры аутентификации, подключить АН пользователя, профиль которого ранее был заблокирован ЭЗ, то на экран будет выведено окно (см. рисунок 5.9), информирующее о попытке входа заблокированного пользователя).

Решение: администратору следует отключить АН пользователя от USB-порта персонального компьютера, профиль которого был заблокирован, пройти процедуру аутентификации в ЭЗ с помощью АН администратора, войти в оболочку KSS, разблокировать профиль пользователя, профиль которого был заблокирован.

Ситуация № 6

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

при следующих условиях:

- если во время прохождения пользователем процедуры аутентификации было превышено максимальное количество попыток аутентификации, т.е. количество подключений АН пользователя к USB-порту персонального компьютера, которое было задано администратором ранее в настройках ЭЗ (см. п. 3.3.1);
- если во время прохождения пользователем процедуры аутентификации количество попыток ввода пароля пользователя превысило максимальное количество попыток аутентификации, которое было задано администратором ранее в

настройках ЭЗ (см. п. 3.6.2), т.е. если после вывода окна (см. рисунок 5.9) пользователем было выполнено последовательное нажатие на клавишу [Enter] такое количество раз, которое привело к превышению максимального количества попыток аутентификации.

Решение: администратору следует отключить АН пользователя от USB-порта персонального компьютера, профиль которого был заблокирован, нажать на любую клавишу клавиатуры, пройти процедуру аутентификации в ЭЗ с помощью АН администратора, войти в оболочку KSS, разблокировать профиль пользователя, профиль которого был заблокирован.

Ситуация № 7

Если при прохождении процедуры аутентификации подключить АН пользователя, незарегистрированное в БД ЭЗ, к свободному USB-порту компьютера, то на экран будет выведено окно (см. рисунок 5.10), информирующее о попытке использования незарегистрированного ключа.

Рисунок 5.10 – Попытка использования незарегистрированного ключа

Примечание. Окно (см. рисунок 5.10) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Решения:

1. Отключить АН пользователя от USB-порта персонального компьютера, которое не было ранее зарегистрировано в ЭЗ, подключить АН пользователя, зарегистрированное в БД ЭЗ.

2. Отключить АН пользователя от USB-порта персонального компьютера, которое не было ранее зарегистрировано в ЭЗ, подключить АН администратора к USB-порту персонального компьютера, 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. 3.5.3), которое отсутствует в БД ЭЗ, то после нажатия на клавишу [Enter] клавиатуры на экран будет выведено окно (см. рисунок 5.11), информирующее о том, что пользователь, проходящий в данный момент процедуру аутентификации, не зарегистрирован в ЭЗ.

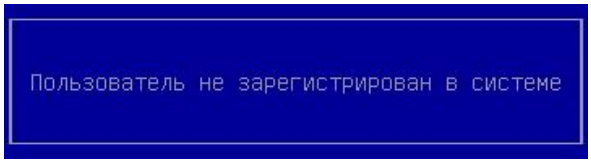


Рисунок 5.11 – Пользователь не зарегистрирован в ЭЗ

Примечание. Окно (см. рисунок 5.11) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Цифровой сертификат».

Решение: администратору следует нажать на любую клавишу клавиатуры, отключить АН пользователя от USB-порта персонального компьютера, подключить АН администратора к USB-порту персонального компьютера, пройти процедуру аутентификации, войти в оболочку KSS, создать профиль нового пользователя с применением АН, с помощью которого ранее была невозможна аутентификация пользователя.

Примечание. Т.к. в настройках ЭЗ 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 пользователей на АН, то на странице *Локальная аутентификация* (см. Рисунок 5.12) выводится запись следующего вида:

Сертификатов не обнаружено

Рисунок 5.12 – Страница *Локальная аутентификация* (вид 6), сертификаты не были найдены на АН

Примечание. Запись, представленная на странице *Локальная аутентификация* (см. Рисунок 5.12), может быть выведена тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: администратору следует сохранить сертификат пользователя на АН.

Ситуация № 10

Если во время прохождения пользователем процедуры аутентификации результат проверки сертификата пользователя на подлинность отрицательный (см. п. 3.5.5), то на экран выводится окно (см. рисунок 5.13), информирующее об ошибке аутентификации.

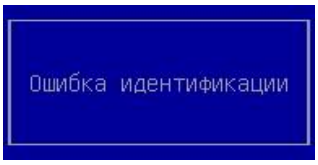


Рисунок 5.13 – Ошибка аутентификации

Примечание. Окно (см. рисунок 5.13) выводится на экран только тогда, когда пользователь проходит процедуру аутентификации при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решения:

1. Администратору следует сохранить сертификат пользователя на АН, который был подписан с помощью сертификата УЦ, добавленного ранее в ЭЗ.

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. Администратору следует обратиться в Единый центр поддержки пользователей компании Kraftway (см. раздел 6), т.к. дальнейшая аутентификация в ЭЗ невозможна (см. предупреждение п. 3.8.3).

Ситуация № 11

Если модуль безопасности *Электронный замок "Витязь"* выключен, то операции, выполняемые в нём, недоступны для администратора, т.е. после выбора пункта *Электронный замок "Витязь"* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2), и нажатия на клавишу [Enter] на экран выводится страница *Электронный замок "Витязь"* с записью (см. рисунок 5.14):

Электронный замок выключен

Рисунок 5.14 – Страница *Электронный замок “Витязь”* (вид 3),
пункты для выполнения операций отсутствуют

Решение: администратору следует включить модуль безопасности *Электронный замок “Витязь”* (см. п. 3.4).

Ситуация № 12

Если модуль безопасности *Контроль целостности файловой системы* выключен, то операции, выполняемые в нём, недоступны для администратора, т.е. после выбора пункта *Контроль целостности файловой системы* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2), и нажатия на клавишу [Enter] на экран выводится страница *Контроль целостности файловой системы* с записью (см. рисунок 5.5):

Модуль контроля целостности файловой системы выключен

Рисунок 5.15 – Страница *Контроль целостности файловой системы* (вид 3), пункты для выполнения операций отсутствуют

Решение: администратору следует включить модуль безопасности *Контроль целостности файловой системы* (см. п. 3.9).

Ситуация № 13

Если модуль безопасности *Управление сертификатами* выключен, то операции, выполняемые в нём, недоступны для администратора, т.е. после выбора пункта *Управление сертификатами* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2, и нажатия на клавишу [Enter] на экран выводится страница *Управление сертификатами* (см. рисунок 5.16) с записью:

Модуль управления сертификатами выключен

Рисунок 5.16 – Страница *Управление сертификатами* (вид 5),
пункты для выполнения операций отсутствуют

Решение: администратору следует включить модуль безопасности *Управление сертификатами* (см. п. 3.8.1).

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] клавиатуры после соответствующего запроса (см. рисунок 3.27), то в этом случае на экран выводится окно (см. рисунок 5.17), информирующее о том, что АН не найден.

Рисунок 5.17 – АН (электронный ключ) не найден

Решение: администратору следует нажать любую клавишу на клавиатуре, после чего повторить процедуру создания профиля нового пользователя, подключить АН пользователя при соответствующем запросе (см. рисунок 3.27), закончить создание профиля нового пользователя.

Ситуация № 15

Если при создании профиля нового пользователя с применением его АН поле окна для ввода пароля (см. рисунок 3.29) оставить пустым или ввести пароль неправильно, то после нажатия на клавишу [Enter] клавиатуры на экран будет выведено окно (см. рисунок 5.18), информирующее о том, что был введён неверный пароль.

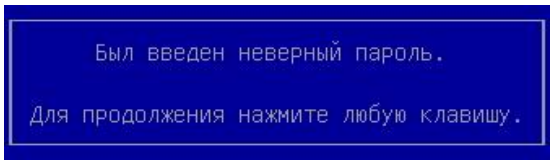


Рисунок 5.18 – Был введён неверный пароль

Решение: администратору следует нажать на любую клавишу, расположенную 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 (см. рисунок 3.29) нажать на клавишу [Esc], то на экран будет выведено окно (см. рисунок 5.19), информирующее о том, что операция прервана.

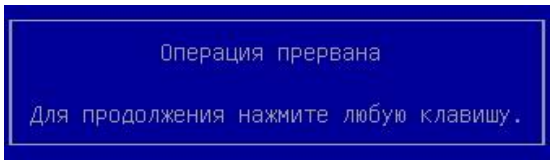


Рисунок 5.19 – Операция прервана

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

Ситуация № 17

Если при создании профиля нового пользователя поля в окнах для ввода данных пользователя (см. рисунки 3.32, 3.33) оставить пустыми, и нажать на клавишу [Enter]

клавиатуры, то на экран будет выведено окно (см. рисунок 5.20), информирующее о том, что были введены неверные данные.

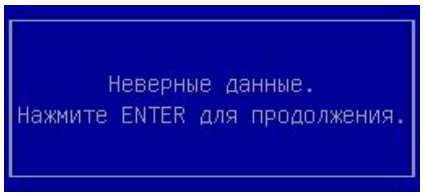


Рисунок 5.20 – Были введены неверные данные

Решение: администратору следует ввести данные в поля окон для ввода данных пользователя (см. рисунки 3.32, 3.33).

Ситуация № 18

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] клавиатуры после соответствующего запроса (см. рисунок 3.27), то в этом случае на экран выводится окно (см. рисунок 5.21), информирующее о том, что АН был зарегистрирован ранее в ЭЗ.

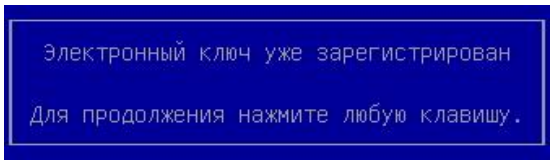


Рисунок 5.21 – АН (электронный ключ) уже зарегистрирован

Примечание. Окно (см. рисунок 5.21) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках ЭЗ: *Электронный замок “Витязь”* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

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

Ситуация № 19

Если при создании профиля нового пользователя с применением АН попытаться создать данный профиль, подключив АН, на котором отсутствует сертификат пользователя, то после выполнения поиска сертификатов на АН на экран выводится окно (см. рисунок 5.22), информирующее о том, что сертификат недоступен.

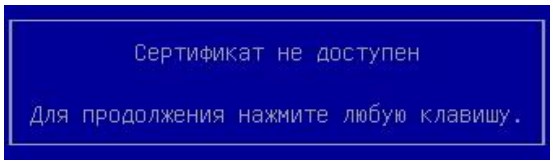


Рисунок 5.22 – Сертификат недоступен

Примечание. Окно (см. рисунок 5.22) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках ЭЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решения:

1. Администратору следует нажать на любую клавишу, расположенную на клавиатуре, и повторить создание профиля нового пользователя с применением АН, на котором размещён сертификат пользователя, специально созданный для данного пользователя.

2. Администратору следует нажать на любую клавишу, расположенную на клавиатуре. Сгенерировать сертификат для пользователя, для которого ранее нельзя было создать профиль пользователя в ЭЗ, сохранить этот сертификат пользователя на АН пользователя, повторить создание профиля нового пользователя с применением данного АН.

Ситуация № 20

Если не подключить АН пользователя перед сменой его пароля или подключить АН другого пользователя, для которого смена пароля в данный момент не выполняется, то на экран буден выведено окно (см. рисунок 5.23), информирующее о том, что АН не был подключён, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 5.24), информирующее о том, что произошла ошибка при смене пароля.

Рисунок 5.23 – АН не был подключен

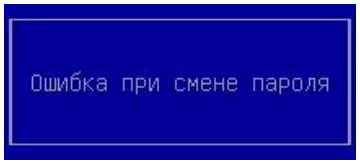


Рисунок 5.24 – Произошла ошибка при смене пароля

Решение: администратору следует нажать на любую клавишу клавиатуры, далее подключить АН пользователя, пароль которого подлежит изменению, повторить процедуру изменения пароля пользователя.

Ситуация № 21

Если текущий пароль пользователя был введён неправильно во время изменения пароля пользователя, то на экран выводится окно (см. рисунок 5.25), информирующее о том, что пароль был введён неправильно, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 5.24), информирующее о том, что произошла ошибка при смене пароля.

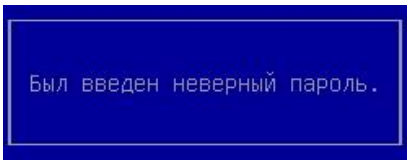


Рисунок 5.25 – Неправильно введён пароль

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

Ситуация № 22

Если новый пароль пользователя был введен неправильно во время изменения пароля, то на экран выводится окно (см. рисунок 5.26), информирующее о несовпадении

паролей, а после нажатия на любую клавишу клавиатуры выводится окно следующего вида (см. рисунок 5.24), информирующее о том, что произошла ошибка при смене пароля.

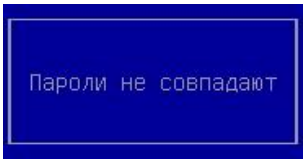


Рисунок 5.26 – Пароли не совпадают

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

Ситуация № 23

Если при добавлении списка файлов, подлежащих КЦ, поле в окне для ввода названия списка файлов (см. рисунок 3.101) оставить пустым и нажать на клавишу [Enter] клавиатуры, то на экран будет выведено окно (см. рисунок 5.20), информирующее о том, что были введены неверные данные.

Решение: администратору следует ввести данные в поле окна для ввода названия списка файлов (см. рисунок 3.101).

Ситуация № 24

Если при добавлении списка файлов, подлежащих КЦ, ввести название списка файлов с использованием специальных символов в соответствующем окне (см. рисунок 3.101) и нажать на клавишу [Enter] клавиатуры, то на экран будет выведено окно (см. рисунок 5.27), информирующее о том, что название списка файлов содержит недопустимые символы.

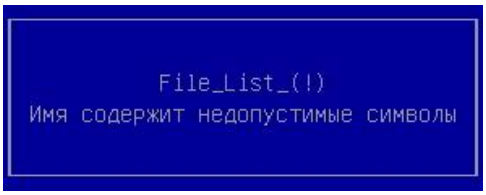


Рисунок 5.27 – Название списка файлов содержит недопустимые символы

Решение: администратору следует повторно выполнить добавление списка файлов, подлежащих КЦ. 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 № 25

Если при добавлении нового списка файлов, подлежащих КЦ, ввести название, которое было присвоено ранее уже добавленному списку файлов в соответствующем окне (см. рисунок 3.101) и нажать на клавишу [Enter] клавиатуры, то на экран будет выведено окно (см. рисунок 5.28), состоящее из записей следующего вида: <присваиваемое название списка файлов>
Такое имя уже используется, информирующее о том, что введённое название списка файлов уже присвоено добавленному списку.

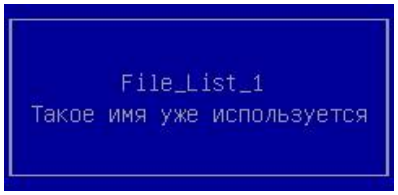


Рисунок 5.28 – Название списка файлов уже присвоено добавленному списку

Решение: администратору следует повторно выполнить добавление нового списка файлов, подлежащих КЦ. Выполняя данную операцию, при присвоении названия новому списку файлов, администратору следует ввести название, отличное от названий списков файлов, которые ранее были добавлены в ЭЗ.

Ситуация № 26

При попытке сохранить список файлов, подлежащих КЦ, которому не было присвоено название, на экран выводится окно (см. рисунок 5.29), информирующее о том, что список файлов невозможно сохранить по причине отсутствия названия у сохраняемого списка файлов.

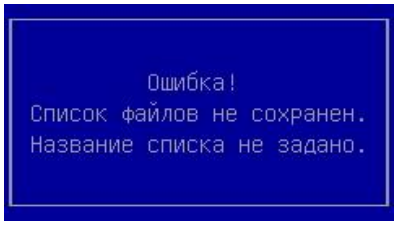


Рисунок 5.29 – Требуется задать название списку файлов

Решение: для сохранения списка файлов, подлежащих КЦ, администратору следует присвоить название добавляемому списку файлов.

Ситуация № 27

Если во время добавления сертификата УЦ в ЭЗ на странице *Файловый менеджер* (см. п. 3.8.3) отменить данную операцию, то на экран будет выведено окно (см. рисунок 5.30), информирующее о том, что не удалось импортировать сертификат УЦ.

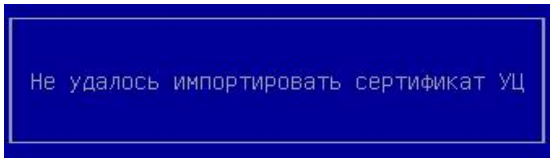


Рисунок 5.30 – Ошибка добавления сертификата УЦ

Ситуация № 28

При попытке добавления сертификата УЦ, который ранее был добавлен в ЭЗ, на экран выводится окно (см. рисунок 5.31), информирующее о наличии данного сертификата УЦ в ЭЗ.

Рисунок 5.31 – Добавляемый сертификат УЦ был добавлен в ЭЗ ранее

Решение: администратору следует добавить другой сертификат УЦ при необходимости.

Ситуация № 29

Если во время добавления сертификата компьютера в ЭЗ на странице *Файловый менеджер* (см. п. 3.8.6) отменить данную операцию, то на экран будет выведено окно (см. рисунок 5.32), информирующее о том, что не удалось импортировать сертификат компьютера.

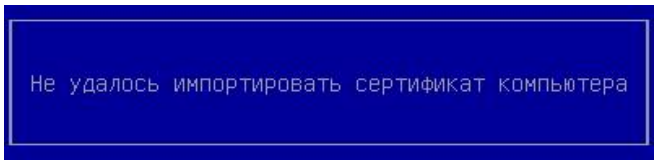


Рисунок 5.32 – Ошибка добавления сертификата компьютера

Ситуация № 30

Если во время добавления сертификата компьютера в ЭЗ на странице *Файловый менеджер* (см. п. 3.8.6), а именно после вывода окна (см. рисунок 3.41), предлагающего ввести пароль для выделенного файла сертификата, отменить данную операцию, то на экран будет выведено окно (см. рисунок 5.32), информирующее о том, что не удалось импортировать сертификат компьютера.

Ситуация № 31

Если во время добавления сертификата компьютера в ЭЗ на странице *Файловый менеджер* (см. п. 3.8.6) ввести неправильно пароль для сертификата компьютера в соответствующем окне (см. рисунок 3.41), то после нажатия на клавишу [Enter] клавиатуры на экран выводится окно (см. рисунок 5.32), информирующее о том, что не удалось импортировать сертификат компьютера.

Решение: администратору следует повторно выполнить добавление сертификата компьютера.

5.1.3 Отображение информации при работе модуля антивируса

Ситуация № 1

Если во время проверки компьютера на наличие вредоносных объектов антивирусом будет обнаружено заражение, то на экран выводится сообщение (см. рисунок 5.323).

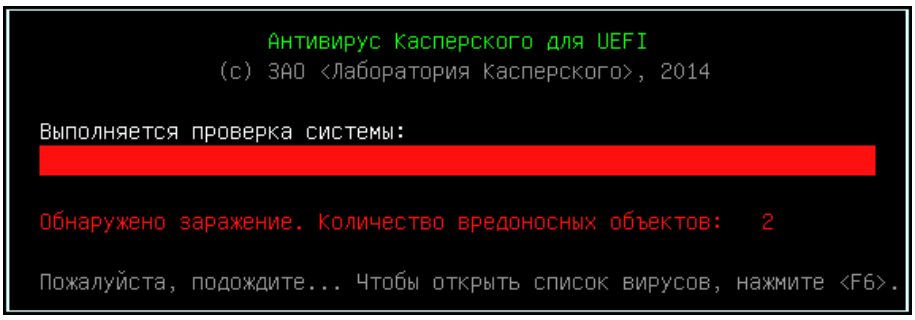


Рисунок 5.33 – Антивирус. Обнаружено заражение

Решение: При получении пользователем сигнала тревоги об обнаружении вредоносных компьютерных программ (вирусов) администратором должны быть выполнены следующие мероприятия:

– изолировать СВТ от локальной сети и доступа в Интернет;
– выполнить вход на СВТ с правами администратора;
– отменить запрет загрузки СВТ с внешних носителей;
– загрузить ОС с доверенного внешнего носителя в режиме «только чтение»;
– выполнить процедуру удаления, лечения или восстановления зараженных файлов;
– установить запрет загрузки СВТ с внешних носителей;
– подключить СВТ к локальной сети;

6 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

При возникновении различных проблем, связанных с работой ПК ЭЗ «Витязь» В2.2, а также для получения консультации, администратор может обратиться в *Центр поддержки пользователей* компании Kraftway.

Перед обращением в *Центр поддержки пользователей* администратору предлагается подготовить следующую информацию:

– версию ЭЗ;

– аппаратные характеристики персонального компьютера;

– журнал событий;

– подробное описание неисправностей или ошибок;

– «скриншоты» ошибок ЭЗ.

Консультацию *Центра поддержки пользователей* компании Kraftway можно получить:

1) по телефонам (круглосуточно):

– 8 (495) 969-24-04 – для Москвы;

– 8 (800) 200-03-55 – для регионов;

2) через веб-форму (круглосуточно).

– www.kraftway.ru/support/support.php.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Термин
BIOS	Basic Input/Output System – базовая система ввода-вывода
EXT	Extended File System – расширенная файловая система
FAT	File Allocation Table – тип файловой системы
KSS	Оболочка Kraftway Secure Shell
NTFS	New Technology File System – файловая система новой технологии
Smart Card	ICC (Integrated Circuit Card) – Смарт-карта – пластиковая карта с интегрированными электронными цепями
SPI Flash	Микросхема памяти для хранения внутреннего ПО материнской платы
UEFI	Unified Extensible Firmware Interface – интерфейс между программным обеспечением, управляющим низкоуровневыми функциями оборудования и операционной системой
USB	Universal Serial Bus – универсальная последовательная шина
АН	Аутентифицирующий носитель
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
Пароль	PIN-код
ПК ЭЗ «Витязь» В2.2	Программный комплекс электронный замок Витязь В2.2
ПО	Программное обеспечение
СДЗ	Средство доверенной загрузки
УЦ	Удостоверяющий центр
ФС	Файловая система