Руководство администратора

KRAFTWAY SECURE SHELL

ВЕРСИЯ 2.2

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для администрирования ВПО оболочка безопасности Kraftway Secure Shell версии 2.2 (далее по тексту KSS), которое поставляется в виде предустановленного встроенного программного обеспечения материнских плат.

В настоящем документе содержится информация о назначении ВПО, функциях ВПО, сведения о технических средствах, обеспечивающих выполнение данного ВПО, представлены сведения о настройке ВПО, работе, приводятся информационные сообщения, сообщения об ошибках ВПО и способы их устранения.

Данное руководство ориентировано для персонала системного администрирования, обладающего знаниями о сетях на базе инфраструктуры открытых и закрытых ключей.

Установка ВПО происходит на заводе АО «Крафтвэй корпорэйшн ПЛС» с использованием аппаратных средств для прошивки BIOS.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Термин
BIOS	Basic Input/Output System – базовая система ввода-вывода
EXT	Extended File System – расширенная файловая система
FAT	File Allocation Table – тип файловой системы
KSS	Оболочка Kraftway Secure Shell
NTFS	New Technology File System – файловая система новой технологии
Smart Card	ICC (Integrated Circuit Card) – Смарт-карта – пластиковая карта с интегрированными электронными цепями
SPI Flash	Микросхема памяти для хранения внутреннего ПО материнской платы
TokenID	Уникальный серийный номер ИУ
UEFI	Unified Extensible Firmware Interface – интерфейс между программным обеспечением, управляющим низкоуровневыми функциями оборудования и операционной системой
USB	Universal Serial Bus – универсальная последовательная шина
АО	Аппаратное обеспечение, оборудование компьютера
ВПО	Встроенное программное обеспечение
ИУ	Идентификационное устройство
КД	Конструкторская документация
КЦ	Контроль целостности
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОБ	Оболочка безопасности – интеграционная среда
ОС	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
РД	Руководящий документ
СДЗ	Средство доверенной загрузки

Сокращение	Термин
СЗИ	Средства защиты информации
Токен	Электронное устройство, предназначенное для идентификации его владельца в виде смарт-карты или USB-ключа,
ТУ	Технические условия
УЦ	Удостоверяющий центр
ФС	Файловая система
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЭД	Эксплуатационная документация

1 ОБЩИЕ СВЕДЕНИЯ О ВПО

1.1 Обозначение и наименование ВПО

Наименование ВПО – Оболочка безопасности Kraftway Secure Shell версия 2.2.

Версия ВПО – 2.2.

Обозначение ВПО – 643.18184162.00008-2.2.

1.2 Назначение KSS

Встроенное программное обеспечение *Оболочка безопасности Kraftway Secure Shell («KSS»)* – это программная интеграционная среда на базе UEFI аппаратной платформы технических средств.

Оболочка KSS предназначена для создания среды функционирования efi-модулей безопасности.

Efi-модуль – это ВПО интегрируемое в UEFI.

KSS обеспечивает пользовательский интерфейс для вызова модулей безопасности, таких как средство доверенной загрузки (СДЗ).

1.3 Цели KSS

Оболочка безопасности KSS является интеграционным решением. Благодаря этому становится возможным адаптировать набор модулей безопасности к требованиям конкретного предприятия.

В рамках интеграционного решения в *Оболочке безопасности KSS* заложены средства решения задач управления загрузкой необходимого количества efi-модулей и функционирование efi-модулей сторонних разработчиков.

1.4 Функции KSS

KSS обеспечивает:

1) Корректную работу и управление запуском модулей безопасности (МБ) в соответствии с эксплуатационной документацией;

2) Совместимость МБ с компонентами средств вычислительной техники информационной системы;

3) Физическую защиту компонентов МБ

– Обеспечение физической целостности вычислительной техники;

4) Обеспечение условий безопасного функционирования

– Обеспечение расширенных возможностей по хранению и анализу информации аудита безопасности;

– Обеспечение меток времени для реализации функции аудита безопасности средства доверенной загрузки;

5) Защита от отключения (обхода)

Обеспечение невозможности отключения (обхода) компонентов МБ

1.5 Условия применения

Для функционирования KSS требуется специализированная UEFI версий 3.2.1 и выше

1.5.1 Требования к аппаратному обеспечению

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

В состав KSS входят драйвера для работы модулей (КЦ ФС, KUEFI, логические диски) которые могут работать со следующими файловыми системами:

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

1.6 Основные характеристики

В *Оболочку безопасности KSS* версии 2.2 могут входить следующие программные модули:

1. Электронный замок:
– ПК ЭЗ «Витязь»
– АПМДЗ-И1
2. Управление сертификатами
3. Контроль целостности файловой системы
4. Контроль целостности оборудования (АО)
5. Логические диски
6. Журнал событий
7. Управление обновлениями
8. Настройка сети
9. Сетевой клиент безопасности
10. Синхронизации времени
11. Антивирус для UEFI
12. Контроля целостности модулей безопасности

1.7 Ролевая модель пользователей KSS

Доступ к настройкам модулей KSS зависит от ролевой модели применяемого средства доверенной загрузки.

ПК ЭЗ «Витязь» обеспечивает разделение пользователей на следующие роли:

– *Администратор*;

– *Пользователь*.

Администраторы СДЗ, в свою очередь, различаются между собой правами доступа. Назначение прав доступа администраторам выполняется при создании или изменении профилей пользователей с ролью *Администратор*.

Пользователь зарегистрированный первым *Администратором* является *Суперадминистратором* и его профиль не подлежит изменению.

При выключенном модуле *СДЗ* пользователь наделен правами *Администратора*. При включенном модуле СДЗ действует ролевая модель, применяемая в конкретном изделии (см. документацию на изделие).

1.8 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.

1.8.1 Правила поведения администратора

Администратор должен работать в соответствии с документом «KSS версия 2.2. Руководство администратора» и, прежде всего, ознакомиться с ним.

Администратор обязан соблюдать следующие правила работы с ИУ:

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

1.8.2 Правила поведения пользователя

Администратор должен ознакомить с данными правилами пользователей, работающих за компьютерами, на которых установлен KSS B2.2.

Пользователь обязан соблюдать следующие правила работы с ИУ:

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

2 ЛОГИЧЕСКАЯ СТРУКТУРА KSS

2.1 Описание логической структуры взаимодействия модулей KSS

Структура интерфейсных функций, составных частей и связи между ними.

Логическая структура интерфейсных функций KSS приведена на рисунке 2.1:

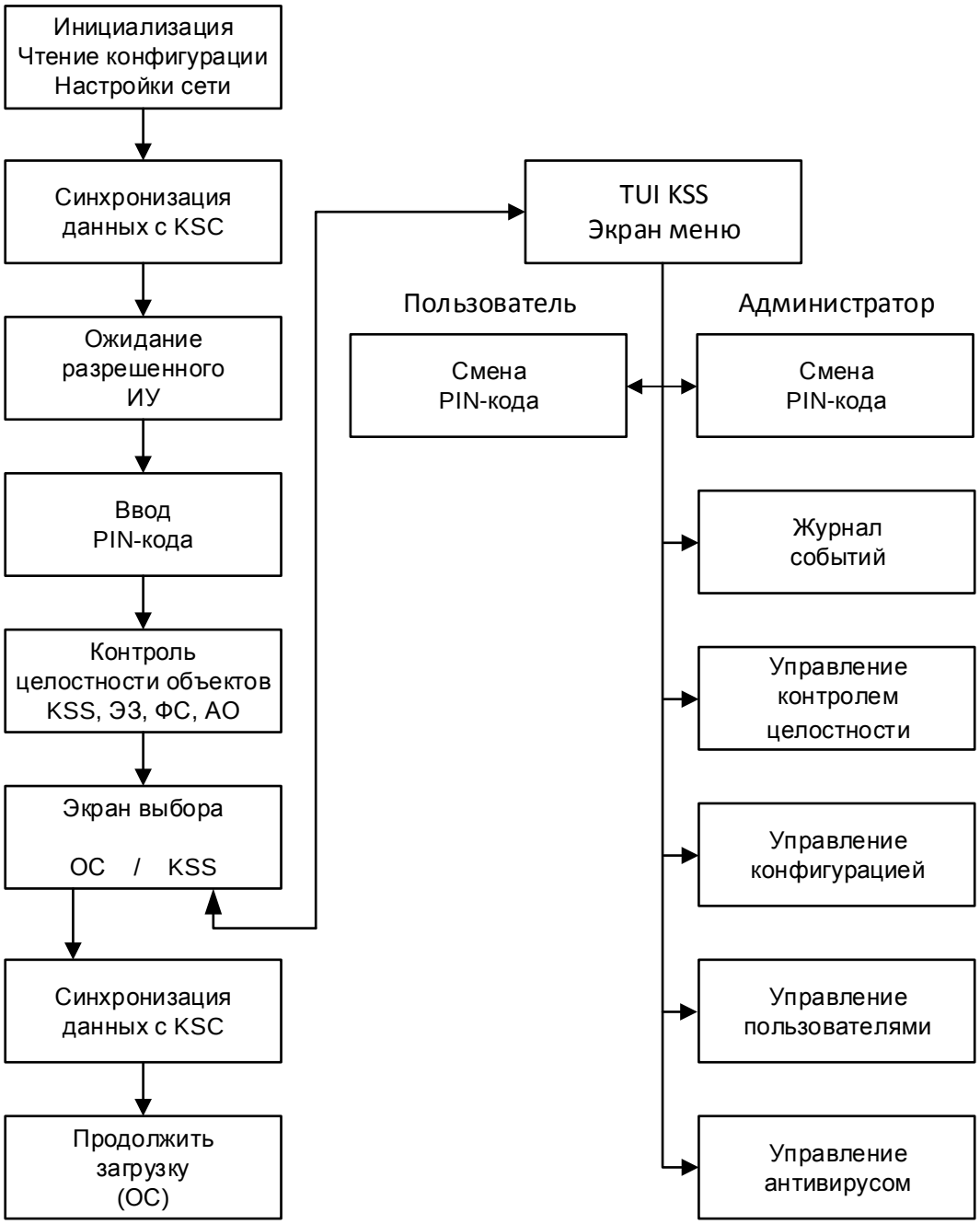

Рисунок 2.1 – Логическая структура интерфейсных функций KSS

При включении питания компьютера происходит инициализация компьютера в сети и подсоединение KSS к серверу безопасности KSC. При этом происходит *Первая синхронизация* настроек KSS с настройками в KSC. Чтение конфигурации всех модулей.

Если модуль СДЗ выключен, то на экран выводится страница выбора действий пользователя: загрузка интерфейса KSS или продолжение загрузки компьютера, ОС.

Если включен модуль *Электронного замка*, то пользователю предлагается пройти процедуру аутентификации.

После аутентификации пользователя в СДЗ, происходит процедура контроля целостности файлов KSS, СДЗ, Файловой системы (ФС), и контроль целостности Аппаратного обеспечения (АО) (оборудования).

После завершения процедуры контроля целостности на экран выводится страница выбора действий пользователя: загрузка интерфейса KSS или продолжение загрузки компьютера, ОС.

При загрузке интерфейса оболочки KSS, пользователь, имеет право выполнять необходимые действия с модулями KSS в зависимости от назначенных прав.

После завершения работы пользователя в KSS и выходе из оболочки, происходит *Вторая синхронизация* настроек KSS с настройками в KSC.

Загружается ОС.

2.2 Используемые методы

При написании *Оболочки безопасности KSS* применялось низкоуровневое, процедурное программирование.

2.3 Алгоритм работы KSS

Алгоритм работы KSS на этапе загрузки компьютера приведен на рисунке 2.2

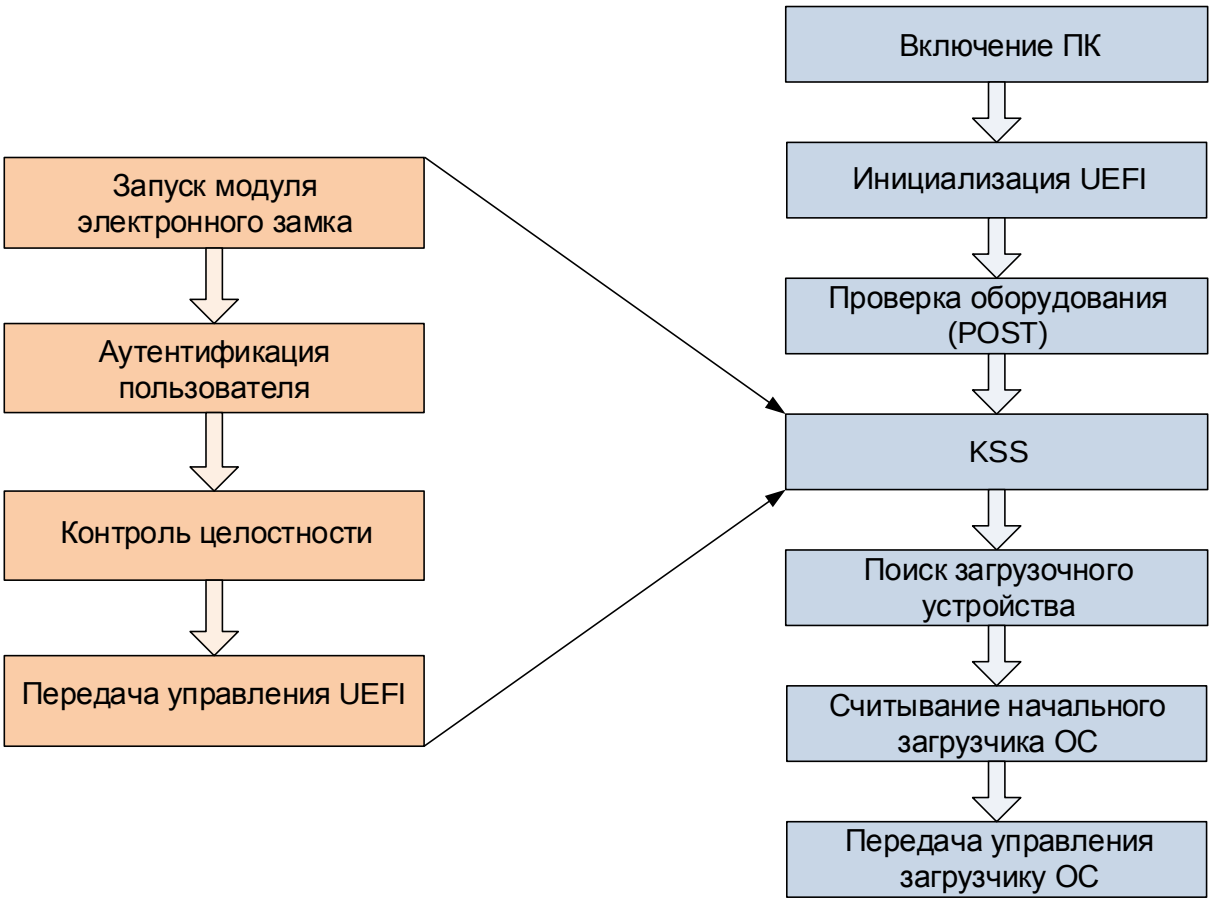

Рисунок 2.2 – Алгоритм работы KSS на этапе загрузки компьютера

Алгоритм работы KSS при использовании в качестве СДЗ - ПК ЭЗ «Витязь».

После включения компьютера производится инициализация UEFI и самотестирование оборудования, после чего управление компьютером перехватывается модулем KSS *Электронным замком*, т.к. по требованиям безопасности согласно руководящих документов, функции включения модулей KSS должны происходить при включённом модуле СДЗ.

Экран меню. Для пользователя и администратора количество пунктов разное:

- Администратору доступны все пункты меню модулей KSS;
- Пользователю доступны только один пункт меню – «Электронный замок “Витязь”» => «Сменить пароль»;

1) при нажатии клавиши [Esc] KSS завершает работу и управление передается в систему.

После завершения работы 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.

Алгоритм работы KSS при использовании в качестве СДЗ – АПМДЗ-И1 см. в документации по АПМДЗ-И1

2.4 Связи программы с другими программами

Выгрузка отчета о состоянии модулей KSS и журнала событий производится при помощи утилиты KSS, после аутентификации пользователя в СДЗ с ролью *администратора*. Выгрузка отчета и журнала из KSS, 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 показаны в кавычках («»), названия различных параметров приводится *курсивом*, значения параметров – в кавычках («»).

3.1 Оболочка Kraftway Secure Shell

3.1.1 Вход в оболочку Kraftway Secure Shell

Для входа в оболочку KSS следует:

Вариант 1. При первом запуске компьютера или при выключенном СДЗ

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.

Рисунок 3.1 – Приглашение на вход в KSS

После выполнения данного действия на экран выводится страница главного меню оболочки «Kraftway Secure Shell» (см. Рисунок 3.2);

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

Вариант 2. При включенном СДЗ.

1) пройти процедуру идентификации в СДЗ;

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 главного меню оболочки «Kraftway Secure Shell» (см. Рисунок 3.2);

Примечания:

1. Если ранее не было выполнено никаких настроек в KSS, то сразу же после отображения Логотипа материнской платы (см. Рисунок 3.1) администратору предлагается дождаться начала загрузки ОС или войти в оболочку KSS.

2. Все дальнейшие операции, связанные с модулями KSS доступны администратору только после включения соответствующих модулей: *Электронный замок*, *Настройка сети* и т.д.

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;

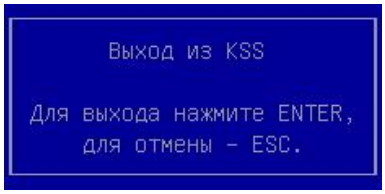

Рисунок 3.3 – Запрос подтверждения на выход из оболочки KSS

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 состоит из следующих элементов (см. Рисунок 3.4):

– область «1» – для отображения названия пункта/подпункта меню;

– область «2» – для отображения пунктов/подпунктов меню, дополнительной или справочной информации;

– область «3» – для отображения подсказок.

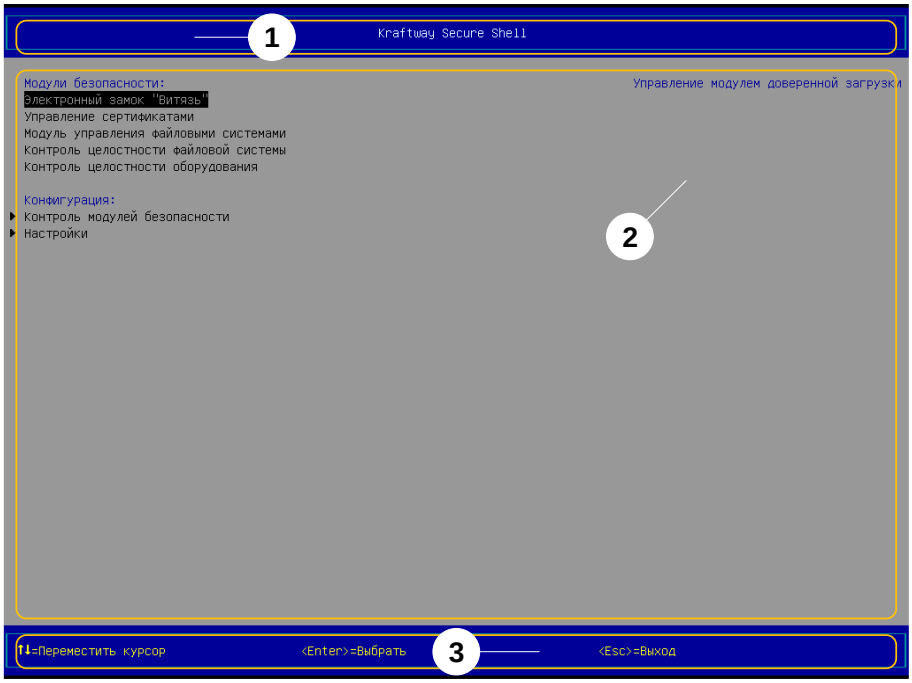

Рисунок 3.4 – Элементы оболочки KSS

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 рисунке 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 KSS (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 KSS:
    – Список модулей KSS;
– Конфигурация:
    – Контроль модулей;
    – Настройки.

3.2 Конфигурация

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.2.1 Установка запрета 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) → [Пробел] на клавиатуре, включить запрет;

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

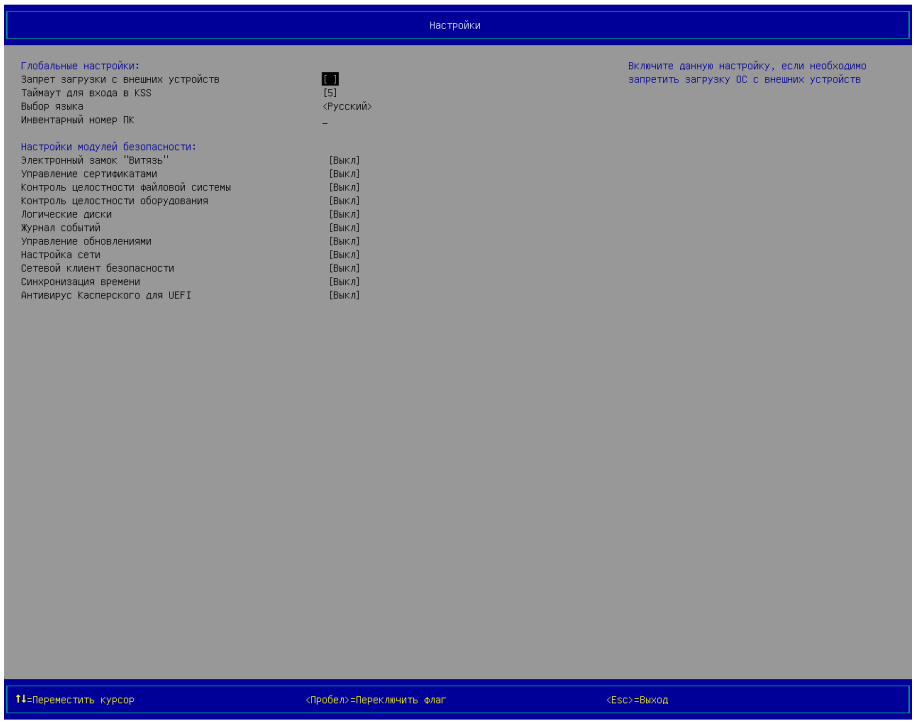

Рисунок 3.5 – Страница *Настройки* (вид 1),
все модули выключены

3.2.2 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);

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.

3.2.3 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»);

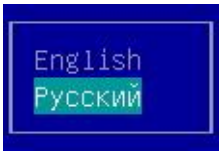

Рисунок 3.6 – Окно для выбора языка интерфейса KSS

5) выбрать требуемый язык интерфейса KSS в окне выбора;

6) → [Enter] на клавиатуре.

Примечание. При вводе данных, для переключения раскладки клавиатуры, воспользуйтесь клавишей [F9].

3.2.4 Ввод инвентарного номера ПК

Для ввода инвентарного номера ПК 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 *Инвентарный номер ПК* в разделе *Глобальные настройки*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.7), для ввода значения;

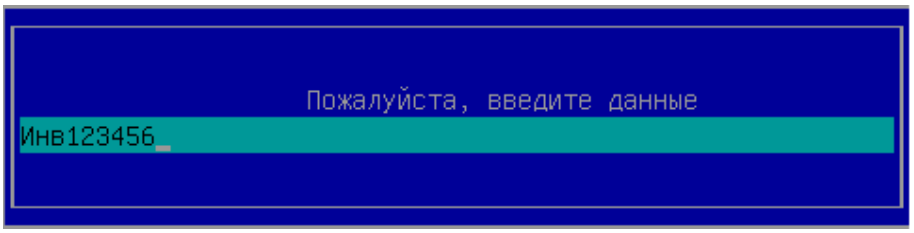

Рисунок 3.7 – Окно для ввода инвентарного номера ПК

5) сменить языковую раскладку клавиатуры → [F9];

6) ввести инвентарный номер ПК;

7) → [Enter] на клавиатуре, для подтверждения введенных данных.

3.3 Контроль целостности модулей KSS

При включении СДЗ происходит процедура контроля целостности модулей и целостности драйверов KSS.

Для вывода результата процедуры контроля целостности модулей и целостности драйверов KSS 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 3.8);

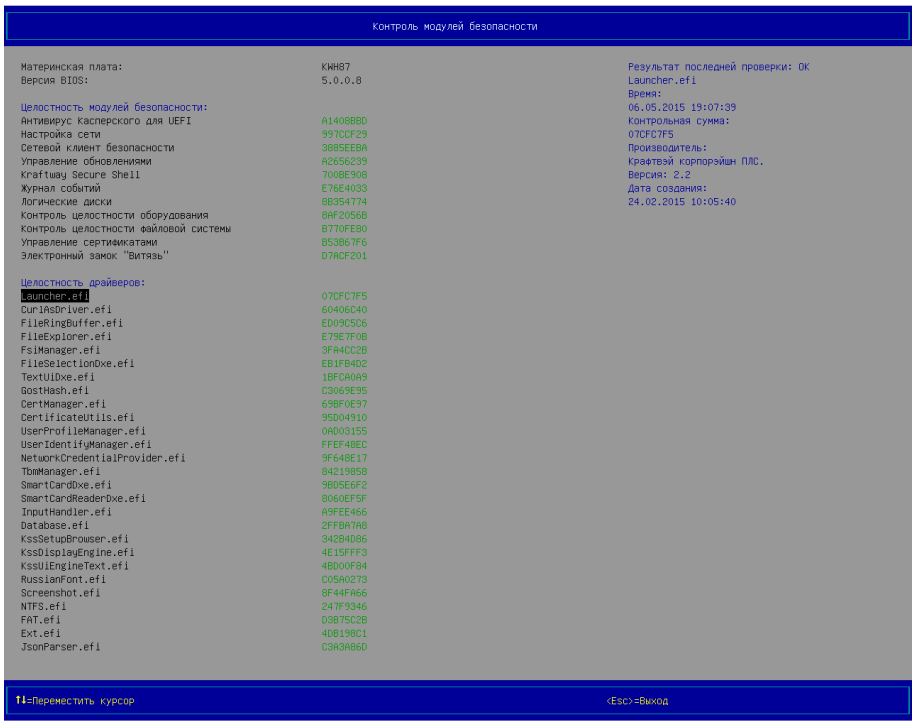

Рисунок 3.8 – Страница «Контроль модулей безопасности»

3) выбрать требуемый модуль 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 KSS происходит при каждом старте компьютера.

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

3. После выбора требуемого модуля или драйвера KSS 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 или драйвер KSS.

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

3.4 Электронный замок “Витязь”

Модуль *Электронный замок* “Витязь” предназначен для защиты компьютера от несанкционированного доступа и обеспечения доверенной загрузки.

Ниже описана процедура включения / выключения модуля ПК ЭЗ «Витязь».

Для получения информации об электронном замке АПМДЗ-И1 смотрите соответствующую документацию.

Внимание! СДЗ начнет выполнять свои функции только после создания профиля первого администратора. Рекомендуется создать профиль первого администратора сразу же после включения СДЗ для дальнейшей работы в нём.

3.4.1 Включение СДЗ. Метод 1

Для включения СДЗ в первый раз или после выключения СДЗ с очисткой всех данных 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 *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 3.9);

Рисунок 3.9 – 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 3.10), запрашивающее подтверждение на включение СДЗ;

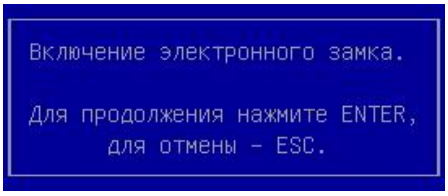

Рисунок 3.10 – Диалоговое окно, запрашивающее подтверждение на включение СДЗ

6) → [Enter] на клавиатуре, после выполнения этого действия на экран выводится страница «Лицензионное соглашение» (см. Рисунок 3.11);

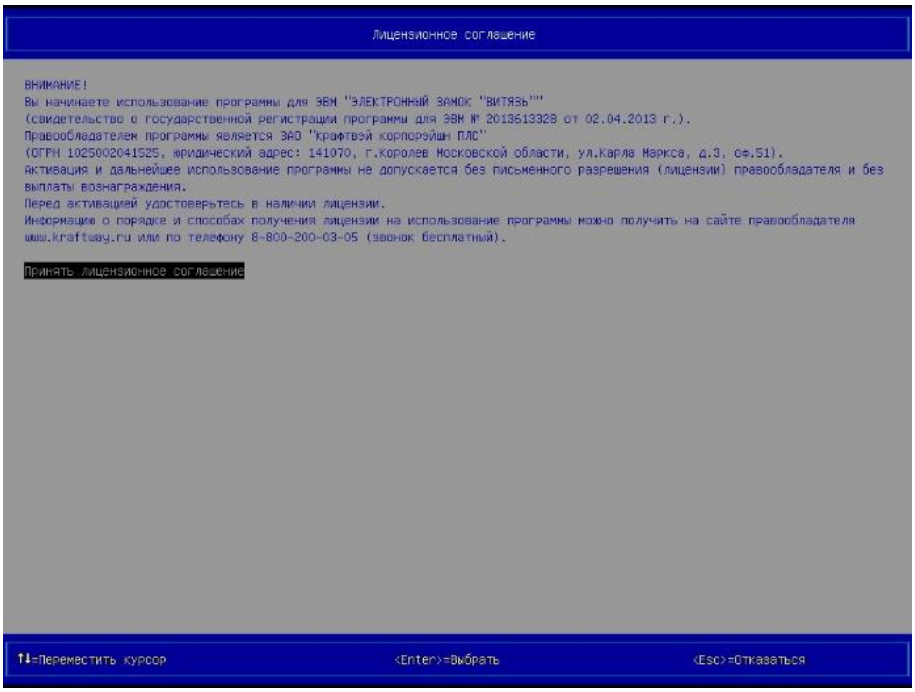

Рисунок 3.11 – Страница «Лицензионное соглашение»,
пункт *Принять лицензионное соглашение* выбран по умолчанию

7) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница «Электронный замок “Витязь”: Настройки» (см. Рисунок 3.12);

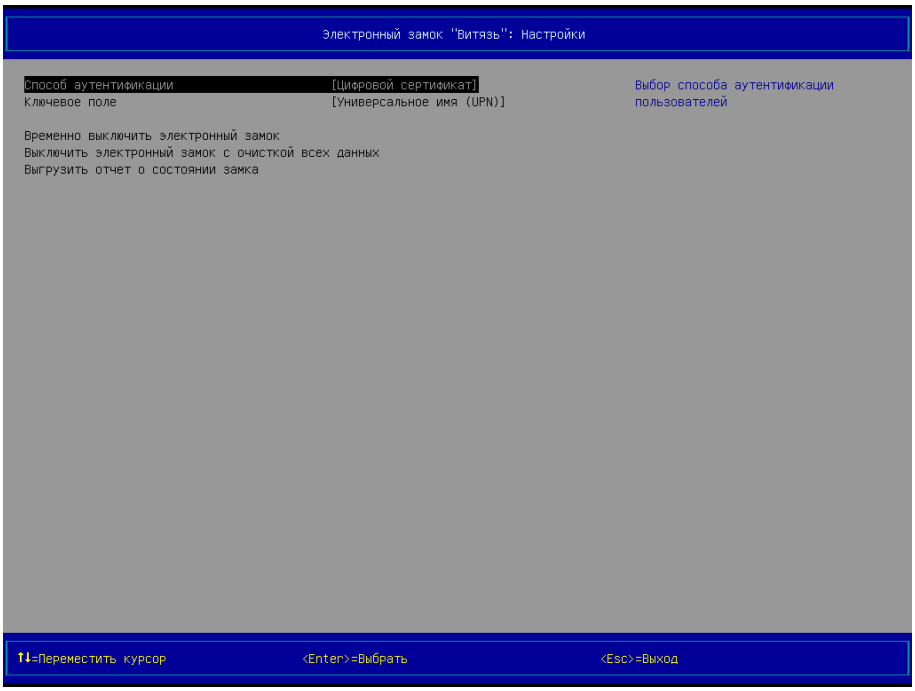

Рисунок 3.12 – Страница «Электронный замок “Витязь”: Настройки» (вид 2), *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)»

8) выбрать пункт *Способ аутентификации*;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.13), предлагающее выбрать способ аутентификации пользователя (доступные значения параметра: «Цифровой сертификат», «Электронный ключ», «Цифровой сертификат и электронный ключ»);

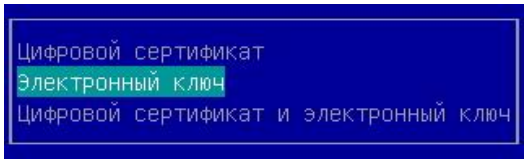

Рисунок 3.13 – Окно для выбора способа аутентификации пользователя

10) выбрать требуемый способ аутентификации в окне выбора;

11) → [Enter] на клавиатуре;

12) выбрать пункт *Ключевое поле* (см. Рисунок 3.12, 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 3.14), 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»);

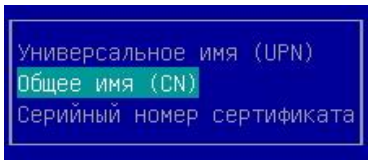

Рисунок 3.14 – Окно для выбора ключевого поля сертификата пользователя

14) → [Enter] на клавиатуре.

Примечания:

1. При попытке назначения параметрам: *Способ аутентификации Ключевое поле* новых значений, на экран выводится окно (см. Рисунок 3.15), запрашивающее подтверждение на внесение изменений.

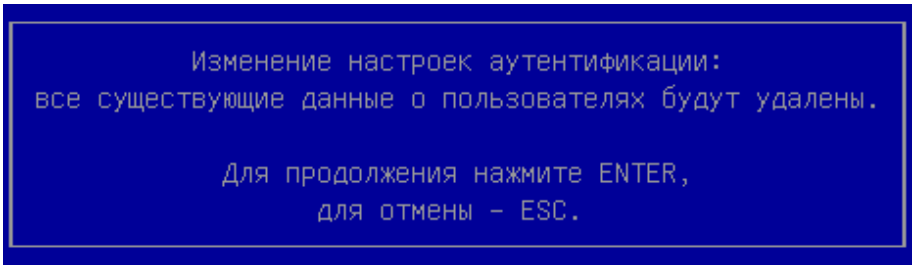

Рисунок 3.15 – Запрос подтверждения на внесение изменений

2. Пункт *Ключевое поле* не выводится на странице «Электронный замок “Витязь”: Настройки» (см. Рисунок 3.16), если параметру *Способ аутентификации* было присвоено значение «Электронный ключ».

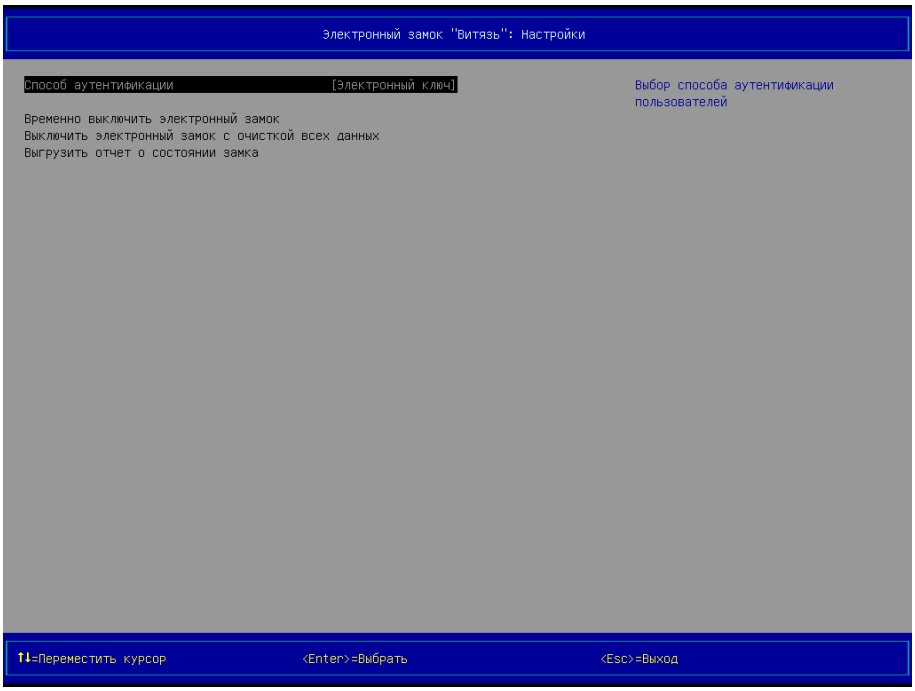

Рисунок 3.16 – Страница «Электронный замок “Витязь”: Настройки» (вид 3), *Способ аутентификации* – «Электронный ключ»

3. После включения СДЗ статус модуля *Электронный замок “Витязь”* меняется с «Выкл» на «Вкл» на странице «Настройки» (см. Рисунок 3.17).

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

3.4.2 Включение СДЗ. Метод 2

Для включения СДЗ после временного его выключения 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 *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 СДЗ (см. Рисунок 3.9);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.10), запрашивающее подтверждение на включение СДЗ;

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

7) для прохождения аутентификации выполнить:

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

б) действия 3-8, если до временного выключения СДЗ 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 3.11);

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница «Электронный замок "Витязь": Настройки» (см. Рисунок 3.12);

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

Примечание. После включения СДЗ статус модуля *Электронный замок "Витязь"* меняется с «Выкл» на «Вкл» на странице «Настройки» (см. Рисунок 3.17).

3.4.3 Выключение СДЗ с очисткой всех данных

Для выключения СДЗ с очисткой всех данных 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 3.17);

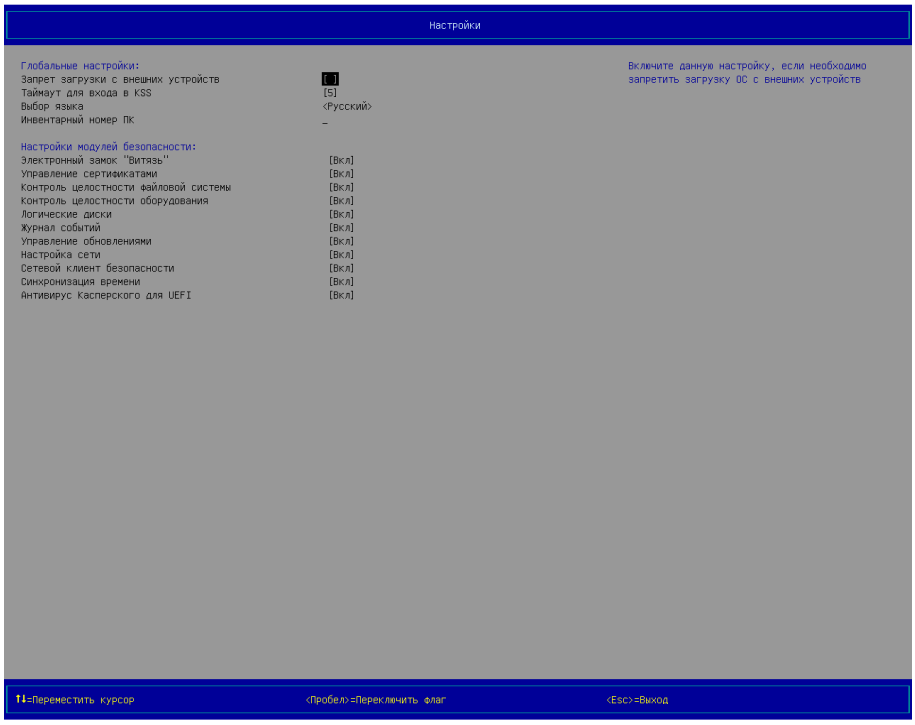

Рисунок 3.17 – Страница «Настройки» (вид 2),
все модули включены

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 3.12, Рисунок 3.16);

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 3.18), запрашивающее подтверждение на выключение СДЗ с очисткой всех данных;

Рисунок 3.18 – Запрос подтверждения на выключение СДЗ
с очисткой всех данных

7) → [Enter] на клавиатуре, после выполнения данного действия происходит выключение СДЗ с удалением ранее введённых данных (информация о пользователях, журнал событий СДЗ), параметрам настроек присваиваются значения по умолчанию, на экран выводится страница *Настройки,* статус модуля меняется с «Вкл» на «Выкл», (см. Рисунок 3.5, Рисунок 3.17).

3.4.4 Временное выключение СДЗ

Для выключения СДЗ без очистки всех данных 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 3.17);

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 3.12, Рисунок 3.16);

5) выбрать пункт *Временно выключить электронный замок*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.19), запрашивающее подтверждение на выключение СДЗ;

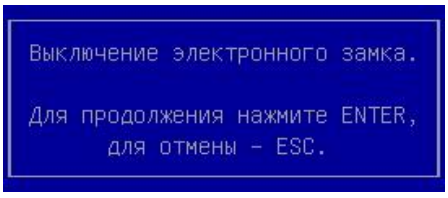

Рисунок 3.19 – Запрос подтверждения на выключение СДЗ

7) → [Enter] на клавиатуре, после выполнения данного действия происходит выключение СДЗ без удаления ранее введённых данных (информация о пользователях, журнал событий СДЗ), значения параметров настроек не изменяются на значения по

умолчанию, статус модуля на странице *Настройки* меняется с «Вкл» на «Выкл», на экран выводится страница «Настройки» (см. Рисунок 3.17).

3.5 Управление сертификатами

Цифровой сертификат – электронный документ, который содержит электронный ключ пользователя, информацию о пользователе, удостоверяющую подпись центра выдачи сертификатов и информацию о сроке действия сертификата.

Сертификаты используются для контроля доступа (авторизации), для подтверждения подлинности пользователей и компьютеров, для получения доступа к файлам обновлений. Цифровые Сертификаты УЦ и компьютера издаются УЦ непосредственно в сети пользователя. Сертификат обновления издается Kraftway.

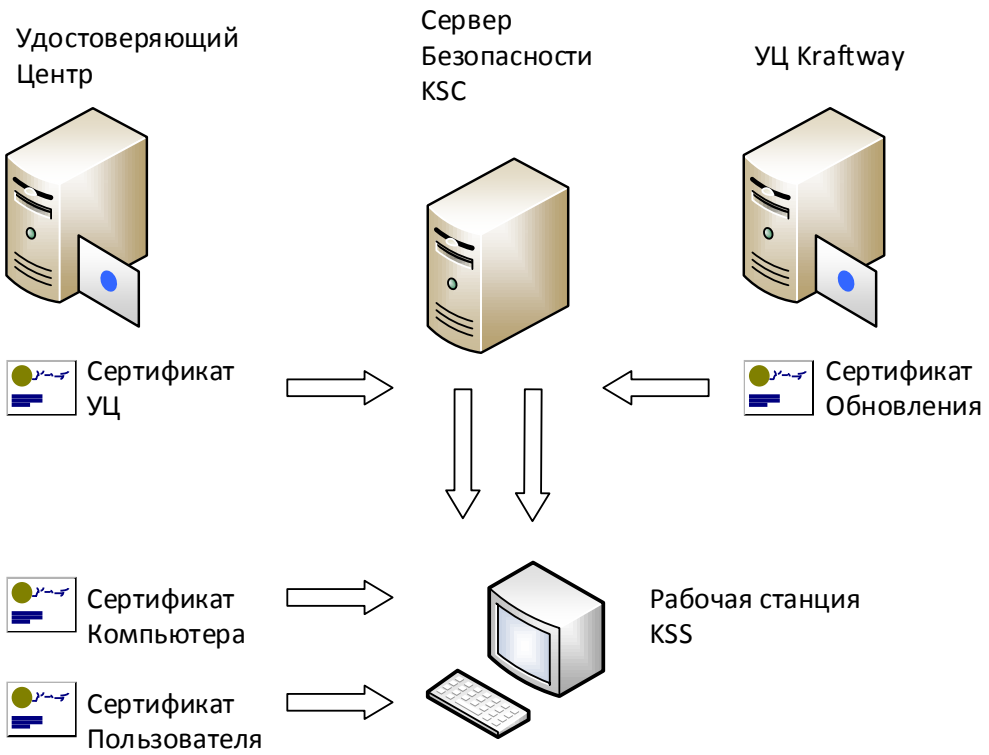

Рисунок 3.20 – Сертификаты, используемые в KSS

В KSS используются сертификаты следующих типов:

– Сертификат удостоверяющего центра – электронный документ, выданный УЦ (корневой сертификат);

– Сертификат компьютера – электронный документ, установленный на компьютер (вручную), выданный УЦ (пользовательский – защита от подмены клиента);

– Сертификат пользователя – электронный документ, присутствующий на ИУ и выданный УЦ;

– Сертификат обновления – электронный документ, выданный Kraftway, для обновления модулей KSS.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.5.1 Включение модуля *Управление сертификатами*

Для включения модуля *Управление сертификатами* следует:

1) выберите 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) выберите в разделе *Настройки модулей безопасности* пункт *Управление сертификатами* со статусом «Выкл»;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами: Настройки* (см. Рисунок 3.21);

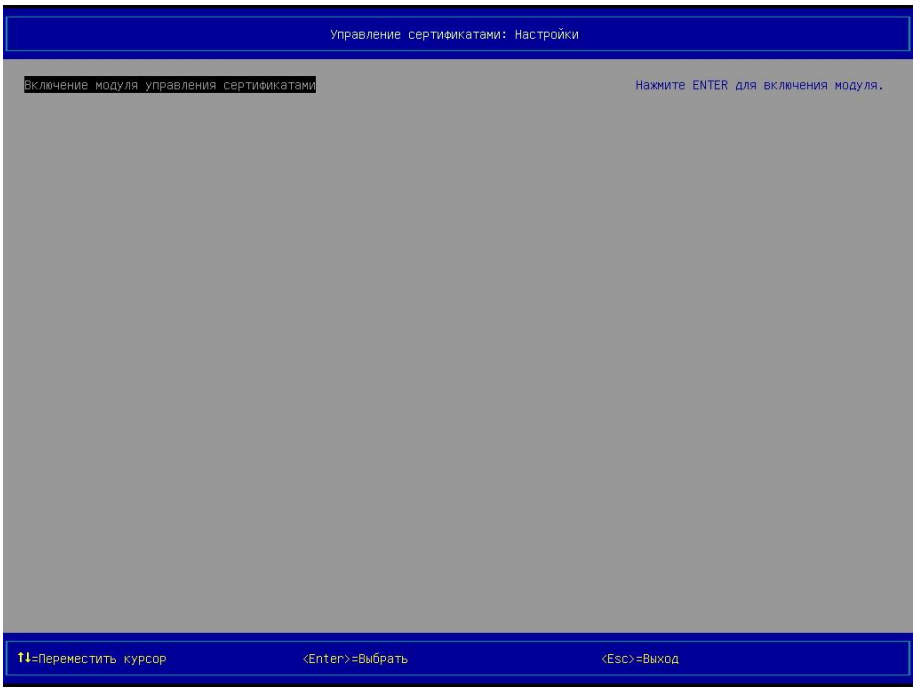

Рисунок 3.21 – Страница *Управление сертификатами: Настройки* (вид 1), пункт для включения модуля

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

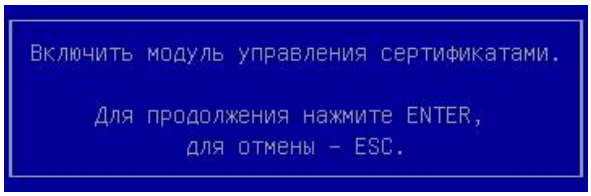

Рисунок 3.22 – Запрос подтверждения на включение модуля *Управление сертификатами*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля *Управление сертификатами*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.17).

3.5.2 Выключение модуля *Управление сертификатами*

Для выключения модуля *Управление сертификатами* следует:

1) выберите 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 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Управление сертификатами* со статусом «Вкл»;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Управление сертификатами: Настройки* (см. Рисунок 3.23) с пунктом для выключения модуля;

Рисунок 3.23 – 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 3.24), запрашивающее подтверждение на выключение модуля;

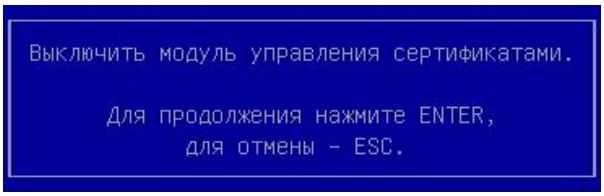

Рисунок 3.24 – Запрос подтверждения на выключение модуля *Управление сертификатами*

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

3.5.3 Настройка оповещения о сроке действия сертификата

Для настройки оповещения об окончании срока действия сертификата за заданное количество дней следует:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Управление сертификатами* (см. Рисунок 3.25);

3) выберите пункт *Оповещать об истечении срока действия сертификата*;

4) → [Enter] на клавиатуре, окно ввода значения количества дней станет активным;

5) введите цифровое значение оповещения об окончании срока действия сертификата за заданное количество дней (по умолчанию 14 дней);

6) → [Enter] на клавиатуре, значение будет сохранено;

7) → [Esc] на клавиатуре, для выхода в Главное меню.

Примечание. Проверка срока действия осуществляется у следующих типов сертификатов:

1. Сертификат удостоверяющего центра;
2. Сертификат компьютера;
3. Сертификат электронного ключа;
4. Сертификат обновления.

3.5.4 Добавление *Сертификата УЦ* вручную

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

Для добавления *Сертификата удостоверяющего центра* (УЦ) в KSS вручную следует:

1) выберите 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 3.25);

Рисунок 3.25 – Страница *Управление сертификатами* (вид 1), сертификаты УЦ отсутствуют

3) подключите USB-диск с файлом *Сертификата УЦ* к свободному порту персонального компьютера (при добавлении файла сертификата с разделов жёстких дисков персонального компьютера данный пункт следует пропустить);

4) выберите пункт *Добавить сертификат УЦ* (см. Рисунок 3.25);

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница «Файловый менеджер» (см. рисунок 3.26);

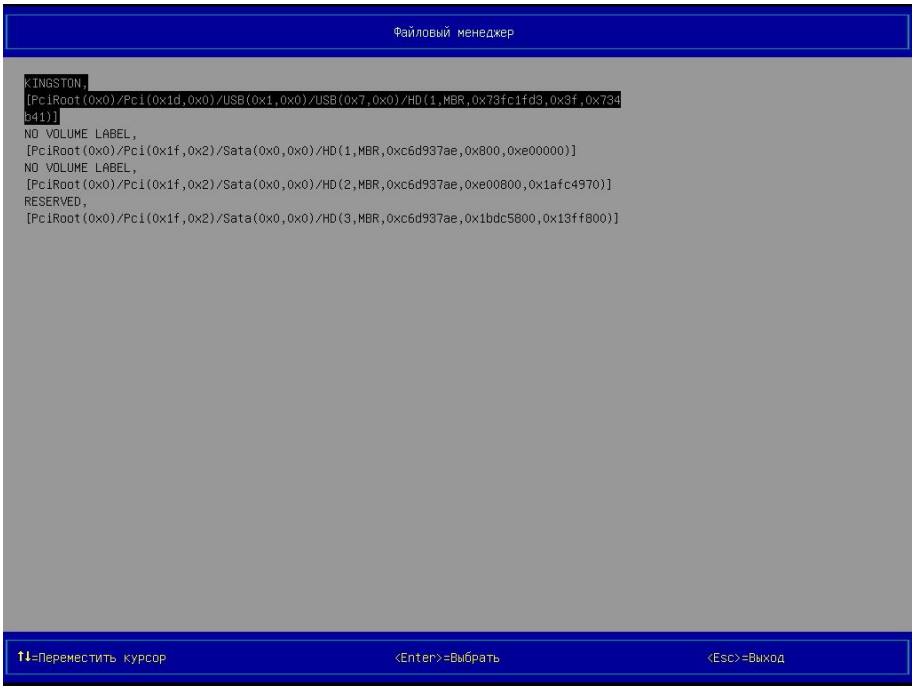

Рисунок 3.26 – Страница «Файловый менеджер»

6) выберите диск, на котором расположен файл *Сертификата УЦ*;

7) → [Enter] на клавиатуре;

8) откройте папку (подпапку), в которой расположен файл *Сертификата УЦ*;

9) выделите требуемый файл *Сертификата УЦ*;

10) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.27), информирующее о добавлении *Сертификата УЦ* в KSS;

Рисунок 3.27 – Сертификат УЦ добавлен

11) → [Enter] на клавиатуре, на странице «Управление сертификатами» в пункте *Сертификаты УЦ* появятся имена добавленных сертификатов.

Примечания:

1. Добавление *Сертификата УЦ* в KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1).

2. Действия на странице «Файловый менеджер» (см. Рисунок 3.26): 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.

3.5.5 Добавление *Сертификата УЦ* автоматически

В KSS предусмотрено автоматическое добавление *Сертификата УЦ* при синхронизации KSS и KSC. Для этого необходимо произвести настройки соединения с KSC, описанные в разделе «3.12.1 Сетевой клиент безопасности».

3.5.6 Просмотр информации о *Сертификате УЦ*

Для просмотра информации о *Сертификате УЦ* следует:

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

2) → [Enter] на клавиатуре, на экран выводится страница «Управление сертификатами» (см. Рисунок 3.28);

Рисунок 3.28 – Страница *Управление сертификатами* (вид 2), два *Сертификата УЦ* добавлены

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

4) просмотрите и проанализируйте данную информацию.

Примечание. Просмотр информации о *Сертификате УЦ* возможен только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления хотя бы одного *Сертификата УЦ* в KSS.

3.5.7 Удаление всех *Сертификатов УЦ*

Для удаления всех сертификатов УЦ из KSS следует:

1) выберите 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 3.28);

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

4) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.29), запрашивающее подтверждение на удаление всех *Сертификатов УЦ*, ранее добавленных в KSS;

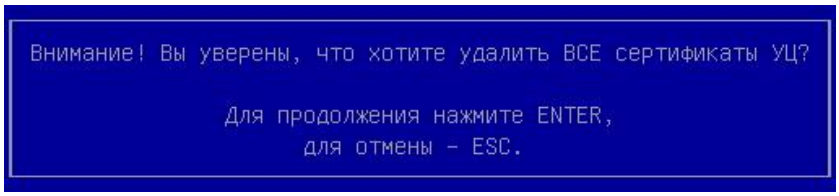

Рисунок 3.29 – Запрос подтверждения на удаление всех сертификатов УЦ

5) → [Enter] на клавиатуре, все *Сертификаты УЦ*, ранее добавленные в KSS, удаляются из KSS, а на экран выводится окно (см. Рисунок 3.30), информирующее об удалении всех Сертификатов УЦ;

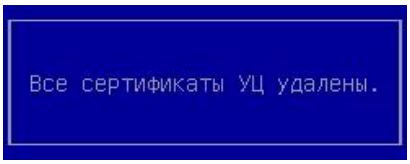

Рисунок 3.30 – Все *Сертификаты УЦ* удалены

6) → [Enter] на клавиатуре.

Примечание. Удаление всех *Сертификатов УЦ* из KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления хотя бы одного *Сертификата УЦ* в KSS.

3.5.8 Добавление *Сертификата компьютера*

Для добавления сертификата компьютера в KSS следует:

1) выберите 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 3.25);

3) подключите USB-диск с файлом *Сертификата компьютера* к свободному порту персонального компьютера (при добавлении файла сертификата с разделов жёстких дисков персонального компьютера данный пункт следует пропустить);

4) выберите пункт *Добавить сертификат компьютера* в разделе *Сертификат компьютера* (см. Рисунок 3.25);

5) → [Enter] на клавиатуре, на экран выводится страница *Файловый менеджер* (см. Рисунок 3.26);

6) выберите диск, на котором расположен файл *Сертификата компьютера*;

7) → [Enter] на клавиатуре;

8) откройте папку (подпапку), в которой расположен файл *Сертификата компьютера*;

9) выделите требуемый файл *Сертификата компьютера*;

10) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.31), предлагающее ввести пароль для выбранного файла сертификата;

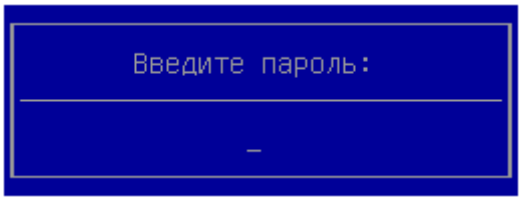

Рисунок 3.31 – Ввод пароля сертификата

11) выведите пароль выбранного файла *Сертификата компьютера*;

12) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.32), информирующее о добавлении *Сертификата компьютера* в KSS;

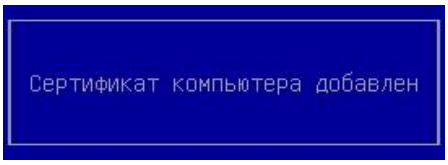

Рисунок 3.32 – Сертификат компьютера добавлен

13) → [Enter] на клавиатуре.

Примечания:

1. Добавление *Сертификата компьютера* в KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1).

2. Действия на странице «Файловый менеджер» (см. Рисунок 3.26): 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 KSS.

3.5.9 Просмотр информации о *Сертификате компьютера*

Для просмотра *Сертификата компьютера* следует:

1) выберите 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 3.33);

Рисунок 3.33 – Страница *Управление сертификатами* (вид 3), сертификат компьютера добавлен

3) выберите *Сертификат компьютера*, информацию о котором требуется просмотреть, - 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;

4) просмотрите и проанализируйте данную информацию.

Примечание. Просмотр информации о *Сертификате компьютера* возможен только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления *Сертификата компьютера* в KSS.

3.5.10 Удаление *Сертификата компьютера*

Для удаления *Сертификата компьютера* из KSS следует:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Управление сертификатами* (см. Рисунок 3.33);

3) выбрать пункт *Удалить сертификат компьютера* в разделе *Сертификат компьютера*;

4) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.34), запрашивающее подтверждение на удаление *Сертификата компьютера*, ранее добавленного в KSS;

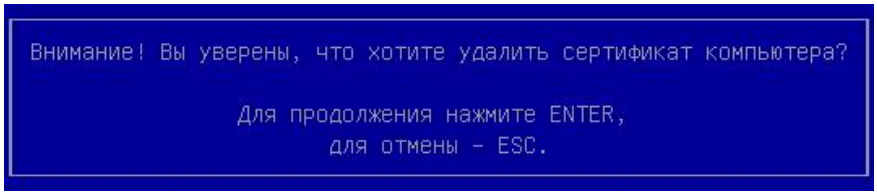

Рисунок 3.34 – Запрос подтверждения на удаление *Сертификата компьютера*

5) → [Enter] на клавиатуре, после выполнения данного действия *Сертификат компьютера*, ранее добавленный в KSS, удаляется из KSS, а на экран выводится окно (см. Рисунок 3.35), информирующее об удалении *Сертификата компьютера*;

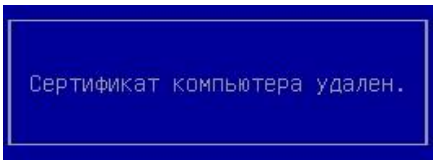

Рисунок 3.35 – *Сертификат компьютера* удалён

6) → [Enter] на клавиатуре.

Примечание. Удаление *Сертификата компьютера* из KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления *Сертификата компьютера* в KSS.

3.5.11 Добавление *Сертификата обновления*

Для добавления *Сертификата обновления* в KSS следует:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Управление сертификатами* (см. Рисунок 3.36);

Рисунок 3.36 – Страница «Управление сертификатами»

3) подключите USB-диск с файлом *Сертификата обновления* к свободному порту персонального компьютера (при добавлении файла сертификата с разделов жёстких дисков персонального компьютера данный пункт следует пропустить);

4) выберите пункт *Добавить сертификат обновления* в разделе *Сертификат обновления* (см. Рисунок 3.36);

5) → [Enter] на клавиатуре, на экран выводится страница «Файловый менеджер» (см. Рисунок 3.26);

6) выберите диск, на котором расположен файл *Сертификата обновления*;

7) → [Enter] на клавиатуре, откройте папку, подпапку, в которой расположен файл *Сертификата обновления*;

8) выберите требуемый файл *Сертификата обновления*;

9) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.37), информирующее о добавлении *Сертификата обновления* в KSS;

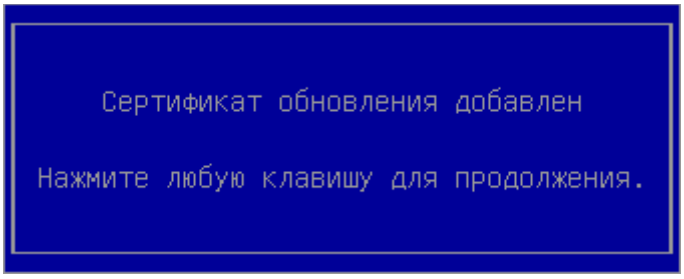

Рисунок 3.37 – Сертификат обновления добавлен

10) → [Enter] на клавиатуре.

Примечания:

1. Добавление сертификата компьютера в KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1).

2. Действия на странице «Файловый менеджер» (см. Рисунок 3.26): 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 обновления* можно добавить в KSS.

3.5.12 Просмотр информации о *Сертификате обновления*

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 3.38);

Рисунок 3.38 – Страница *Управление сертификатами* (вид 3), информация о *Сертификате обновления*

3) выберите пункт с названием *Сертификата обновления*, после выполнения данного действия в правой части области № 2 оболочки KSS выводится информация о сертификате: серийный номер сертификата, кем выдан, кому выдан, даты и время начала срока действия сертификата, даты и время окончания срока действия сертификата (см. Рисунок 3.38);

4) просмотрите и проанализируйте данную информацию.

Примечание. Просмотр информации о *Сертификате обновления* возможен только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления *Сертификата обновления* в KSS.

3.5.13 Удаление *Сертификата обновления*

Для удаления *Сертификате обновления* из KSS следует:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Управление сертификатами* (см. Рисунок 3.36);

3) выбрать пункт *Удалить сертификат обновления* в разделе *Сертификат обновления* (см. Рисунок 3.36);

4) → [Enter] на клавиатуре, на экран выводится окно (см. Рисунок 3.39), запрашивающее подтверждение на удаление *Сертификата обновления*, ранее добавленного в KSS;

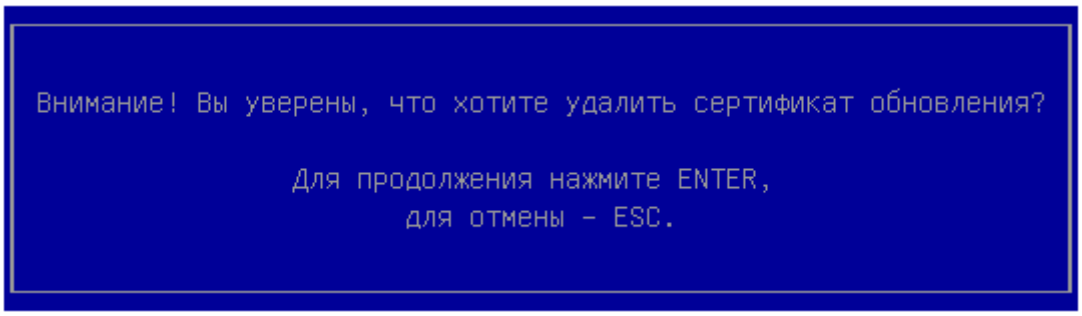

Рисунок 3.39 – Запрос подтверждения на удаление *Сертификата обновления*

5) → [Enter] на клавиатуре, *Сертификат обновления*, ранее добавленный в KSS, удаляется из KSS, а на экран выводится окно (см. Рисунок 3.40), информирующее об удалении сертификата;

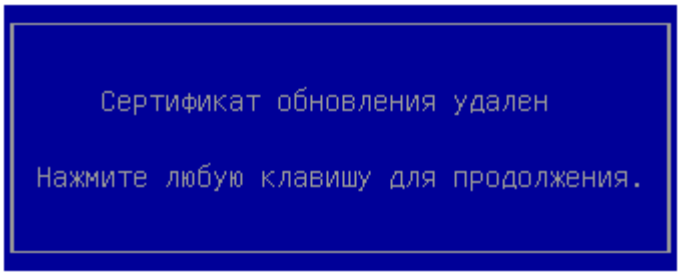

Рисунок 3.40 – *Сертификат обновления* удалён

6) → [Enter] на клавиатуре.

Примечание. Удаление *Сертификата обновления* из KSS возможно только после включения модуля *Управление сертификатами* (см. п. 3.5.1) и добавления *Сертификат обновления* в KSS.

3.6 *Контроль целостности файловой системы*

Модуль *Контроля целостности файловой системы* входит в состав модулей СДЗ.

Модуль *Контроля целостности файловой системы* предназначен для проверки целостности критичных файлов на изменения путем сравнения контрольных сумм и сигнализации при обнаружении изменений. При нарушении целостности осуществлять управление KSS сможет только пользователь с правами Администратора.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.6.1 Включение модуля КЦ файловой системы

Для включения модуля 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 3.41);

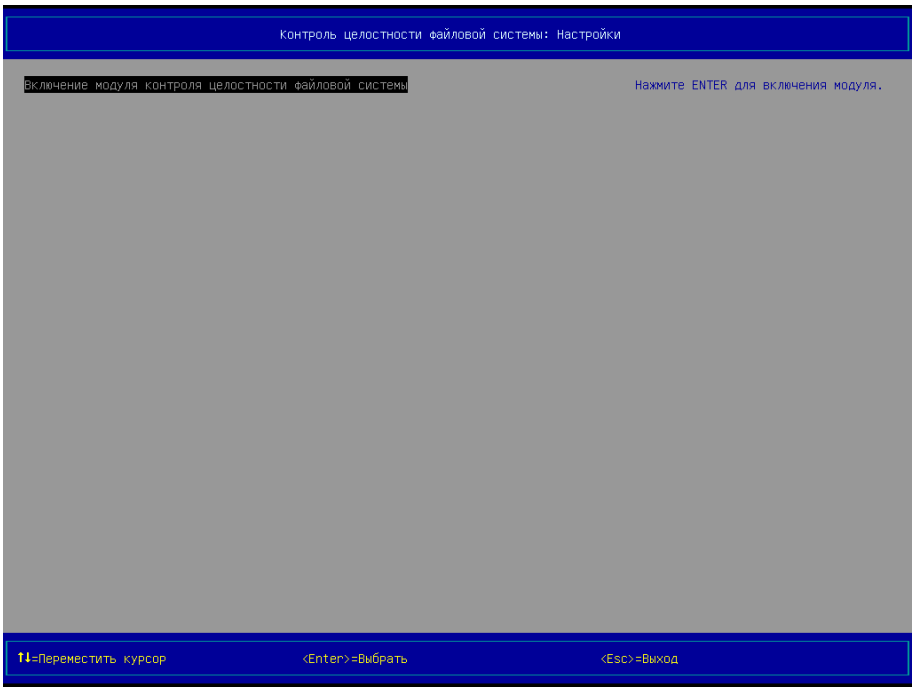

Рисунок 3.41 – Страница *Контроль целостности файловой системы: Настройки* (вид 1), пункт для включения модуля КЦ ФС

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.42), запрашивающее подтверждение на включение модуля;

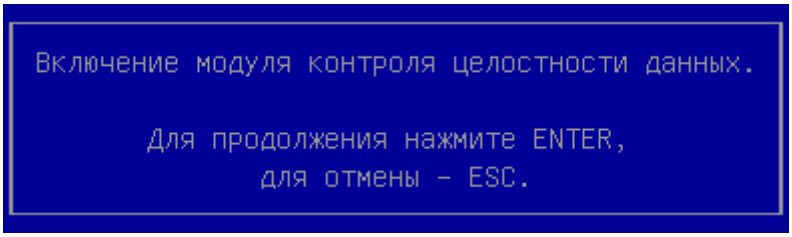

Рисунок 3.42 – Запрос подтверждения на включение модуля *Контроль целостности файловой системы*

6) → [Enter] на клавиатуре, на экран выводится страница *Контроль целостности файловой системы: Настройки* (вид 2), с возможностью выбора хеш-функции (см. Рисунок 3.43);

Рисунок 3.43 – 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 3.44), предлагающее выбрать хеш-функцию из списка;

Рисунок 3.44 – 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 ;

11) → [Esc] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17), статус модуля *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».

3.6.2 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 3.17);

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 3.43) 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 3.44), 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 ;

9) → [Esc] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17).

3.6.3 Выключение модуля КЦ файловой системы

Для выключения модуля КЦ файловой системы следует:

1) выберите 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 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Контроль целостности файловой системы* со статусом «Вкл»;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности файловой системы: Настройки* (см. Рисунок 3.45) с пунктом для выключения модуля и удаления всех списков контроля целостности;

Рисунок 3.45 – 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 3.46), запрашивающее подтверждение на выключение модуля и удаления всех списков контроля целостности;

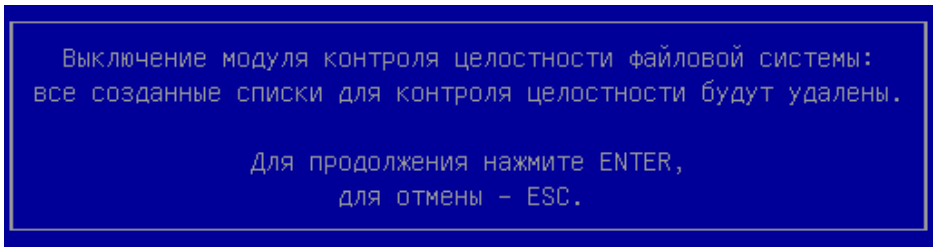

Рисунок 3.46 – Диалоговое окно, запрашивающее подтверждение на выключение модуля КЦ ФС и удаление всех списков контроля целостности

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется выключение модуля *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).

3.6.4 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 3.47);

Рисунок 3.47 – 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 3.48);

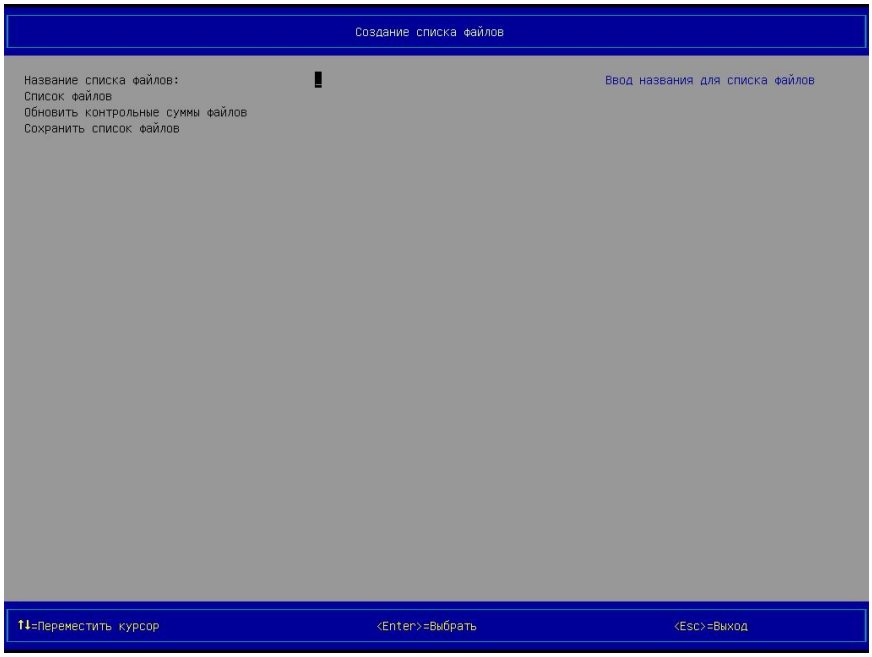

Рисунок 3.48 – Страница *Создание списка файлов*

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 3.49);

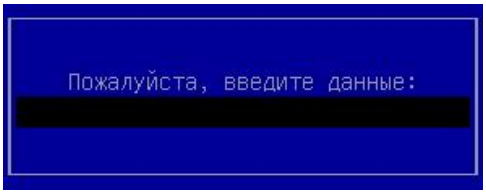

Рисунок 3.49 – Окно для ввода названия списка файлов

7) ввести название списка файлов;

8) → [Enter] на клавиатуре;

9) выбрать пункт С*писок файлов* (см. Рисунок 3.48);

10) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно файлового менеджера (см. Рисунок 3.50), в котором предлагается выбрать объекты (файлы, папки), подлежащие КЦ;

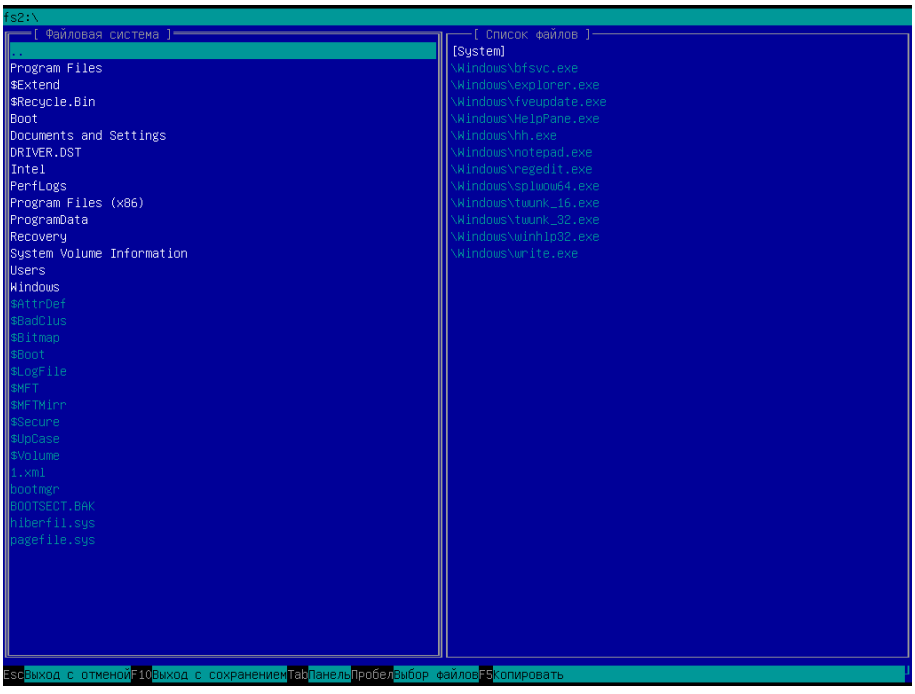

Рисунок 3.50 – Окно файлового менеджера

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 3.48);

20) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.51), информирующее об успешном обновлении (создании) контрольных сумм (КС) файлов;

Рисунок 3.51 – Окно, информирующее об успешном обновлении КС файлов

21) → [Enter] на клавиатуре;

22) выбрать пункт *Сохранить список файлов* (см. Рисунок 3.48);

23) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.52), информирующее о выполнении сохранения списка файлов.

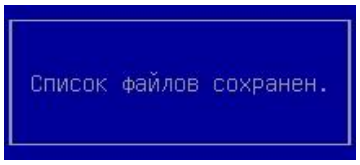

Рисунок 3.52 – Окно, информирующее о сохранении списка файлов

– → [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 3.53). 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 *Контроль целостности файловой системы* (см. п. 0).
2. Выбор требуемых объектов в панелях *Файловая система* и *Список файлов* выполняется с помощью клавиш [↑], [↓], расположенных на клавиатуре (см. Рисунок 3.50).
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.

3.6.5 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 3.53);

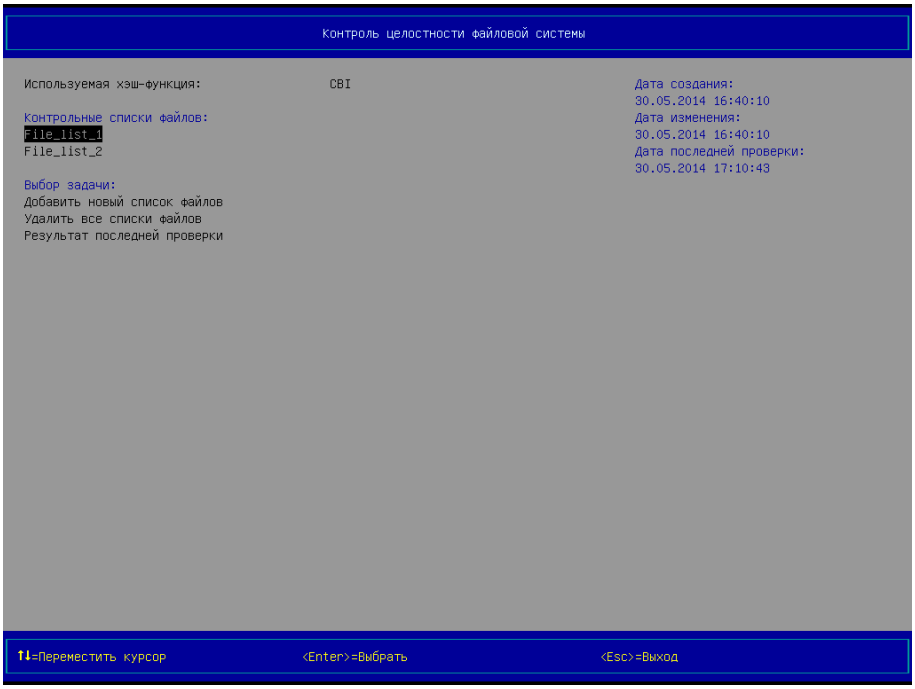

Рисунок 3.53 – Страница *Контроль целостности файловой системы* (вид 2), созданы два списка файлов, подлежащих КЦ

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 3.54), предлагающее выбрать действие, которое необходимо выполнить над выбранным списком файлов;

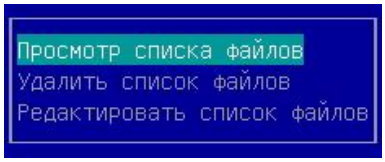

Рисунок 3.54 – Окно для выбора действия над выбранным списком файлов

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 3.55);

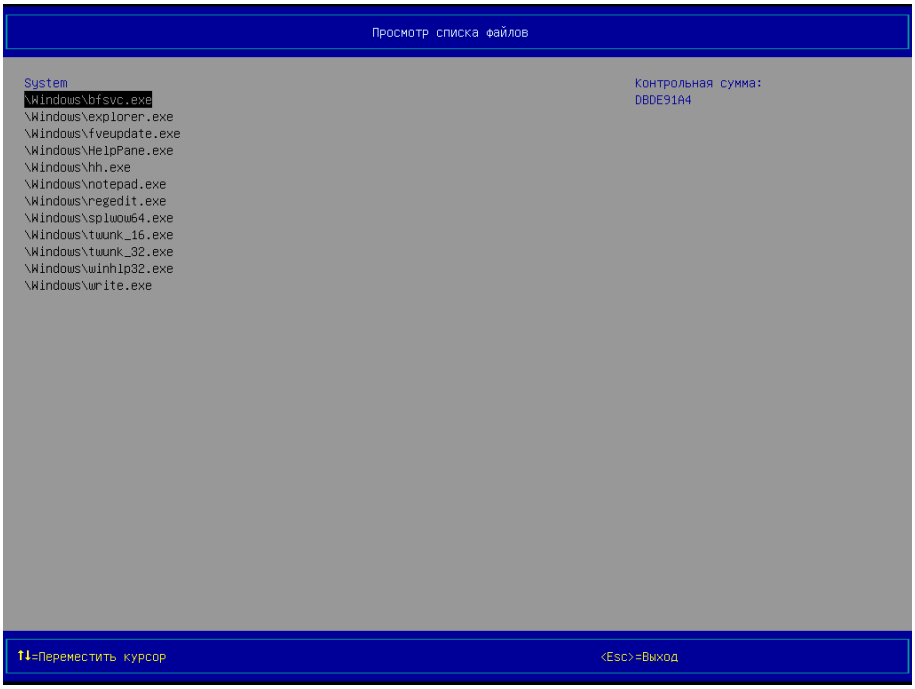

Рисунок 3.55 – Страница *Просмотр списка файлов*

Примечания:

1. Просмотр списка файлов, подлежащих КЦ, возможен только после включения модуля *Контроль целостности файловой системы* (см. п. 0), 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.

3.6.6 Редактирование списка файлов, подлежащих КЦ

Для редактирования списка файлов, подлежащих КЦ, следует:

1) выполнить действия 1-4 п. 3.6.5,

2) выбрать пункт *Редактировать список файлов* в окне (см. Рисунок 3.54);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Редактировать список файлов* (см. Рисунок 3.56);

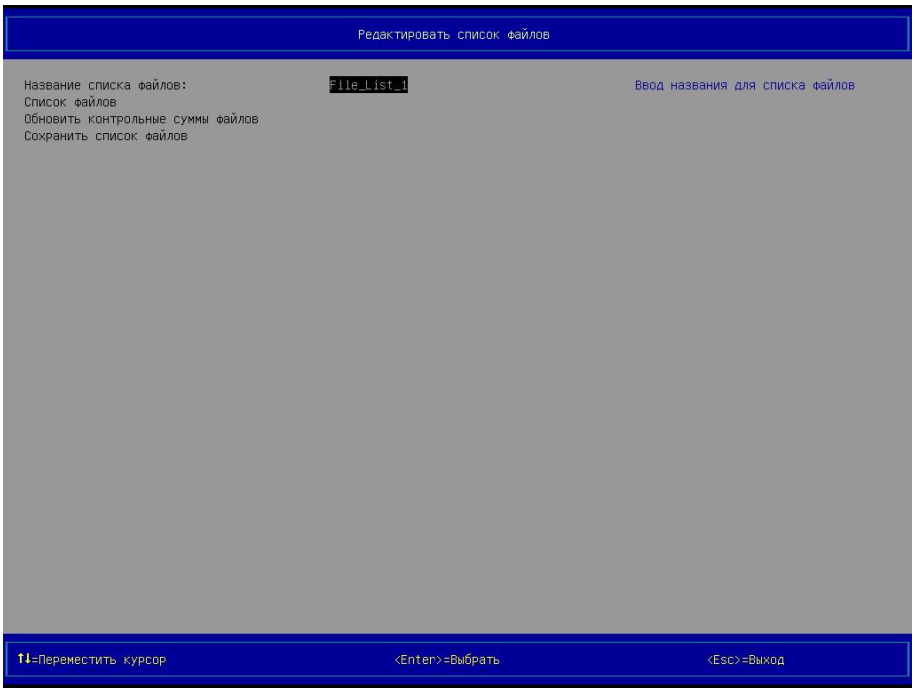

Рисунок 3.56 – Страница *Редактировать список файлов*

4) выполнить изменение названия списка файлов при необходимости (см. действия 5-8 п. 3.6.4);

5) изменить состав списка файлов при необходимости (см. действия 9-18 п. 3.6.4);

6) обновить контрольные суммы файлов (см. действия 19-21 п. 3.6.4), если состав списка файлов был изменён;

7) сохранить список файлов (см. действия 22-24 п. 3.6.4), если состав списка файлов был изменён.

Примечание. Редактирование списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. п. 0), создания хотя бы одного списка файлов, подлежащих КЦ.

3.6.7 Удаление списка файлов, подлежащих КЦ

Для удаления списка файлов, подлежащих КЦ, следует:

1) выполнить действия 1-4 п. 3.6.5,

2) выбрать пункт *Удалить список файлов* в окне (см. Рисунок 3.54);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.57), запрашивающее подтверждение на удаление выбранного списка файлов;

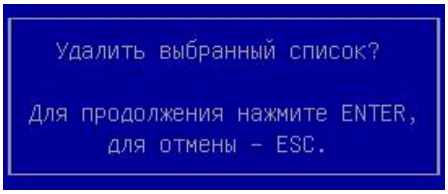

Рисунок 3.57 – Запрос подтверждения на удаление выбранного списка файлов

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

Примечание. Удаление списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы* (см. п. 0), создания хотя бы одного списка файлов, подлежащих КЦ.

3.6.8 Вывод результата последнего выполнения процедуры КЦ файлов

Для вывода результата последнего выполнения процедуры КЦ файлов следует:

1) выполнить действия 1, 2 п. 3.6.4;

2) выбрать пункт *Результат последней проверки* (см. Рисунок 3.53);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Результат последней проверки* (см. рисунки 3.58, 3.59);

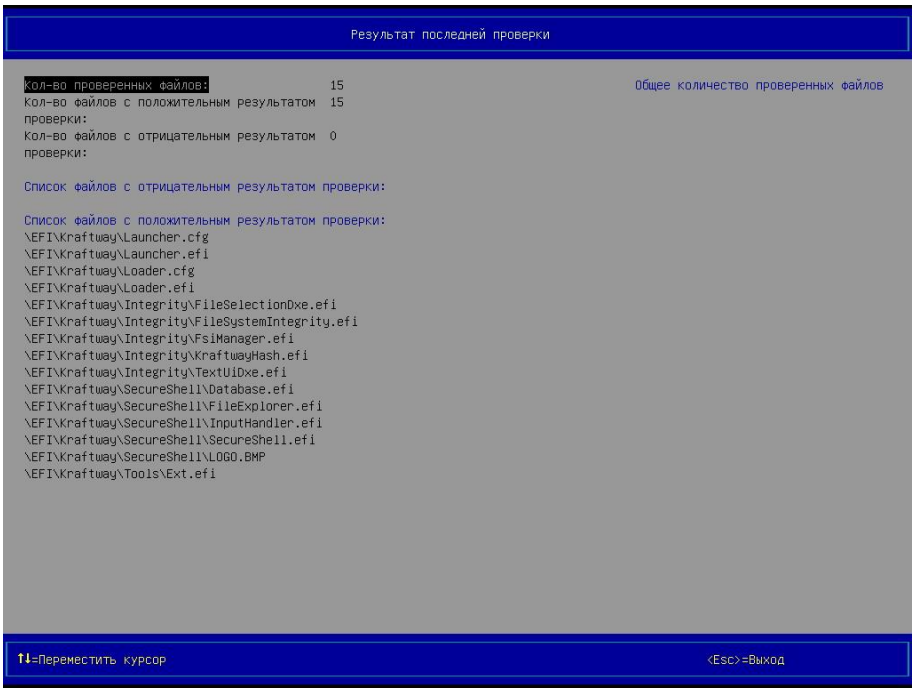

Рисунок 3.58 – Страница *Результат последней проверки* (вид 1), файлы с отрицательным результатом проверки отсутствуют

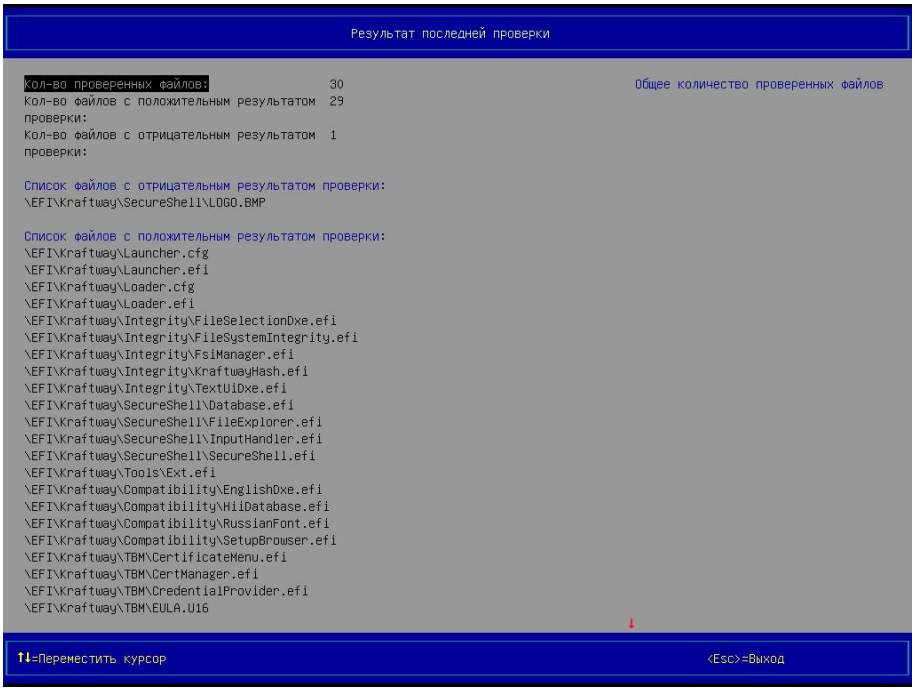

Рисунок 3.59 – Страница *Результат последней проверки* (вид 2), выведен файл с отрицательным результатом проверки

4) выбрать требуемый файл в разделе *Список файлов с отрицательным результатом проверки* с помощью клавиш [↑], [↓], расположенных на клавиатуре, для вы-

вода 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 *Контроль целостности файловой системы* (см. п. 0), 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.

3.6.9 Удаление всех списков файлов, подлежащих КЦ

Для удаления всех списков файлов, подлежащих КЦ, следует:

1) выполнить действия 1, 2 п. 3.6.4;

2) выбрать пункт *Удалить все списки файлов* (см. Рисунок 3.53);

3) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.60), запрашивающее подтверждение на удаление всех списков файлов;

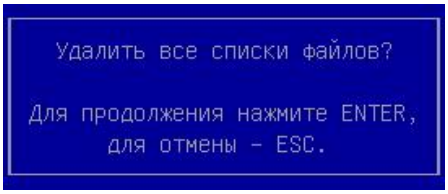

Рисунок 3.60 – Запрос подтверждения на удаление всех списков файлов

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 *Контроль целостности файловой системы* (см. п. 3.6.1) и создания хотя бы одного списка файлов, подлежащих КЦ.

3.7 Модуль *Контроль целостности оборудования*

Модуль *Контроля целостности оборудования* входит в состав модулей СДЗ.

Модуль *Контроля целостности оборудования* предназначен для проверки целостности аппаратного обеспечения компьютера путем сравнения контрольных сумм и сигнализации при обнаружении изменений. При нарушении целостности осуществлять управление KSS сможет только пользователь с правами Администратора.

3.7.1 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 3.61);

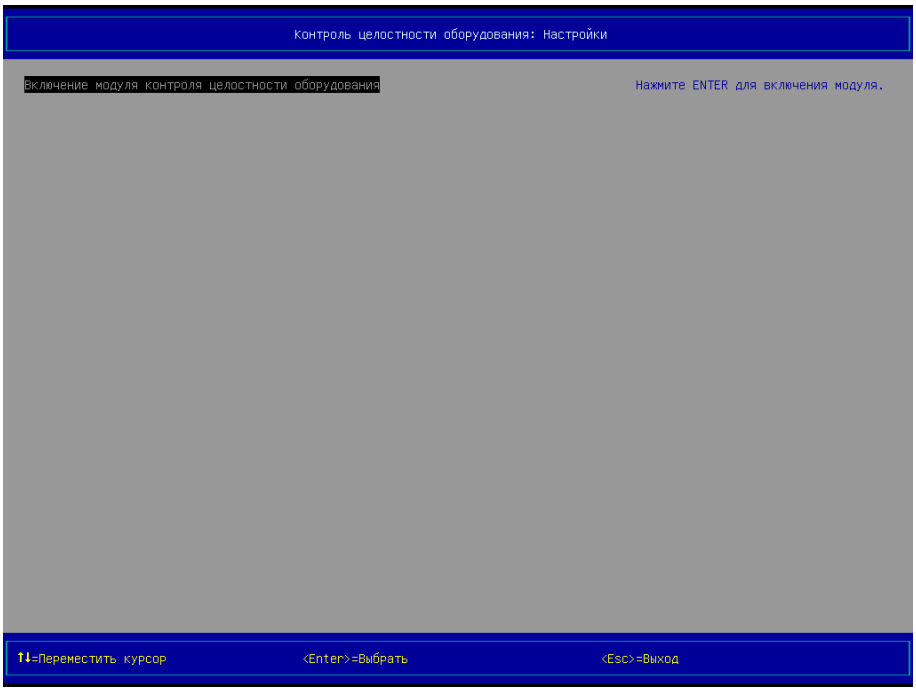

Рисунок 3.61 – Страница *Контроль целостности оборудования: Настройки* (вид 1), пункт для включения модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.62), запрашивающее подтверждение на включение модуля;

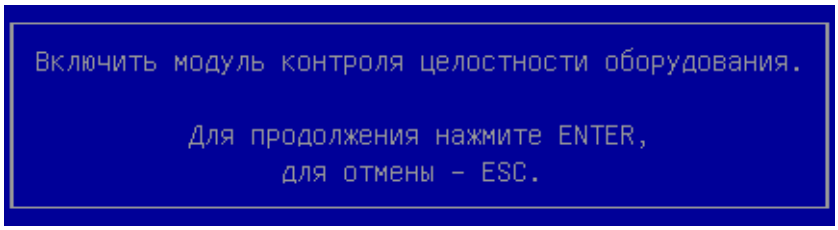

Рисунок 3.62 – Запрос подтверждения на включение *Модуля контроль целостности оборудования*

6) → [Enter] на клавиатуре, после выполнения данного действия выполняется включение модуля *Контроль целостности оборудования*, на экран выводится страница *Настройки*, статус модуля изменяется с «Выкл» на «Вкл» (см. Рисунок 3.17).

3.7.2 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 3.17);

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 3.63) с пунктом *Выключение модуля контроля целостности оборудования*;

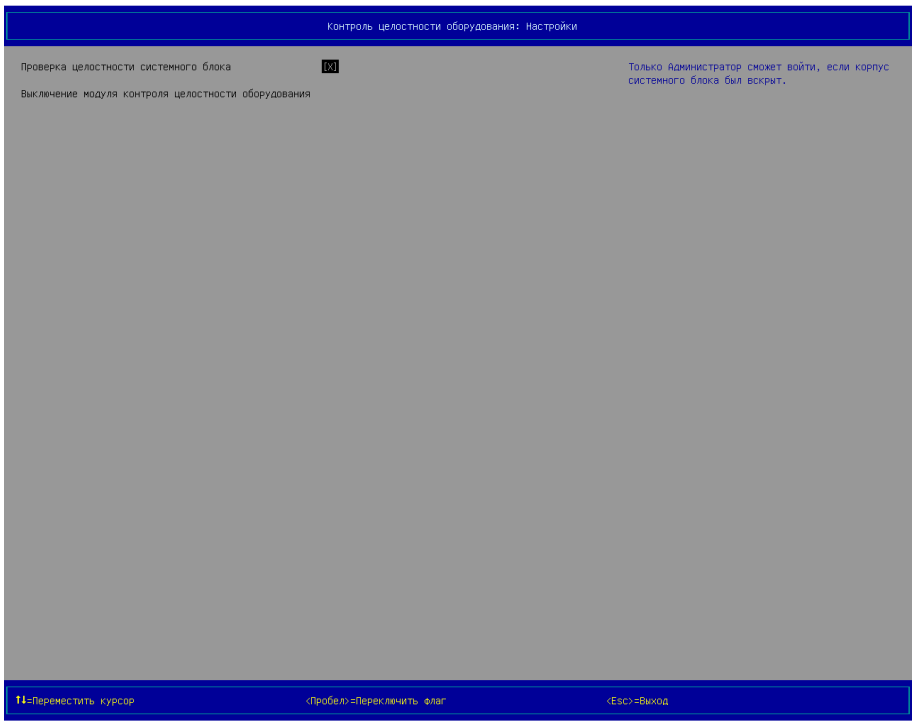

Рисунок 3.63 – Страница *Контроль целостности оборудования: Настройки* (вид 2), пункт выключение модуля

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.64), запрашивающее подтверждение на выключение модуля;

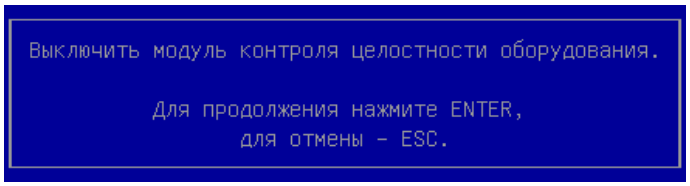

Рисунок 3.64 – Диалоговое окно, запрашивающее подтверждение на выключение модуля *Контроль целостности оборудования*

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

3.7.3 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 3.65, Рисунок 3.66);

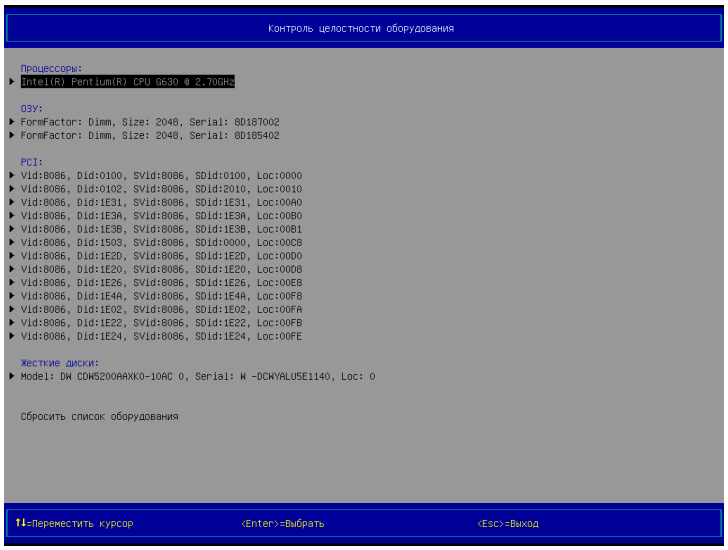

Рисунок 3.65 – Страница *Контроль целостности оборудования* (вид 1), с положительным результатом проверки

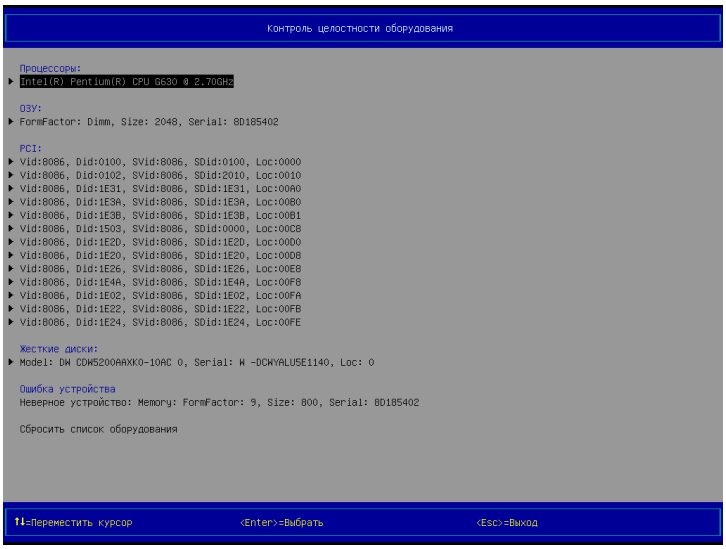

Рисунок 3.66 – Страница *Контроль целостности оборудования* (вид 2), с отрицательным результатом проверки

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

Примечания:

1. Вывод результата последнего выполнения процедуры КЦ оборудования возможен только после включения модуля *Контроль целостности оборудования* (см. п. 3.7.1) 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 3.7.4).

3. Информация от *Модуля контроля целостности оборудования* сохраняется в *Журнале событий* (см. пункт 0).

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.

3.7.4 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 3.65, Рисунок 3.66);

3) выбрать пункт *Сбросить список оборудования*;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.67), запрашивающее подтверждение на сброс списка оборудования;

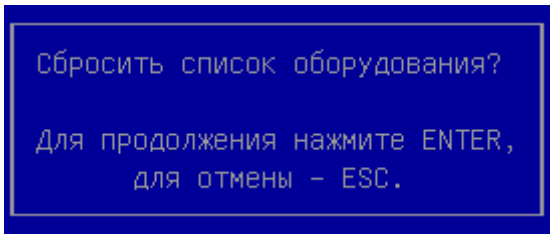

Рисунок 3.67 – Запрос подтверждения на сброс списка оборудования

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 *Контроль целостности оборудования* (см. п. 3.7.1).

3.7.5 Проверка 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) выберите 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) выберите в разделе *Настройки модулей безопасности* пункт *Контроль целостности оборудования* со статусом «Вкл»;

4) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится страница *Контроль целостности оборудования: Настройки* с пунктом *Проверка целостности системного блока* (см. Рисунок 3.63);

5) выберите пункт *Проверка целостности системного блока*;

6) активируйте 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 *Контроль целостности оборудования* (см. п. 3.7.1).

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

3. Информация о работе *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).

3.8 Логические диски

Модуль Логические диски предназначен для переименования названия 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».

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

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.8.1 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 3.68) с пунктом *Включение модуля управления логическими дисками*;

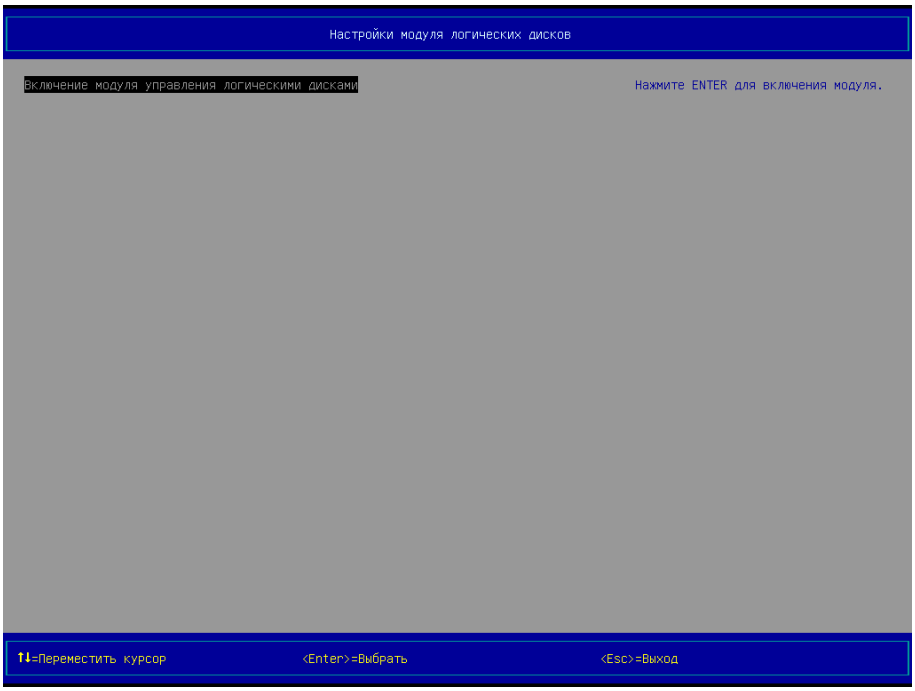

Рисунок 3.68 – Страница *Настройки модуля логических дисков* (вид 1), пункт *Включение модуля управления логическими дисками*

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.69), запрашивающее подтверждение на включение модуля;

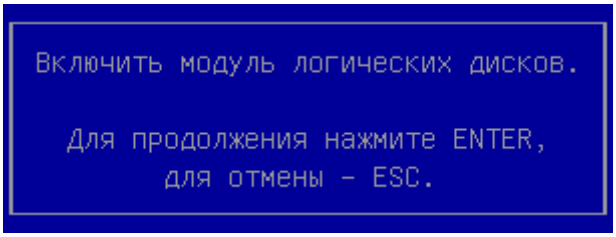

Рисунок 3.69 – Запрос подтверждения на *включение модуля управления логическими дисками*

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 3.17).

3.8.2 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 3.17);

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 3.70) с пунктом *Выключение модуля управления логическими дисками*;

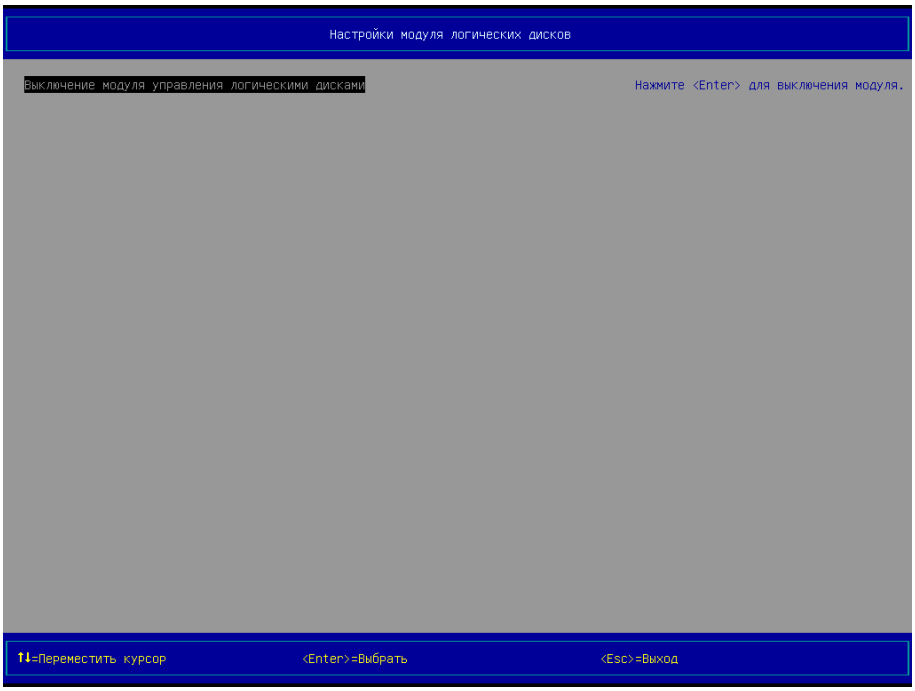

Рисунок 3.70 – Страница *Настройки модуля логических дисков* (вид 2), пункт *Выключение модуля управления логическими дисками*

5) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.71), запрашивающее подтверждение на выключение модуля;

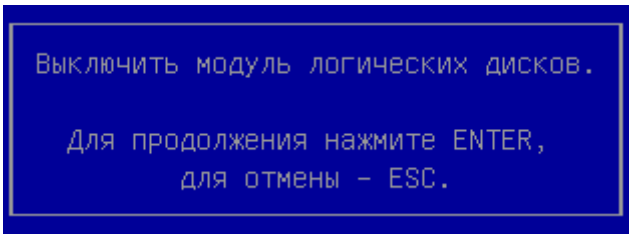

Рисунок 3.71 – Запрос подтверждения на
Выключение модуля управления логическими дисками

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).

3.8.3 Редактирование имен логических дисков

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 3.72).

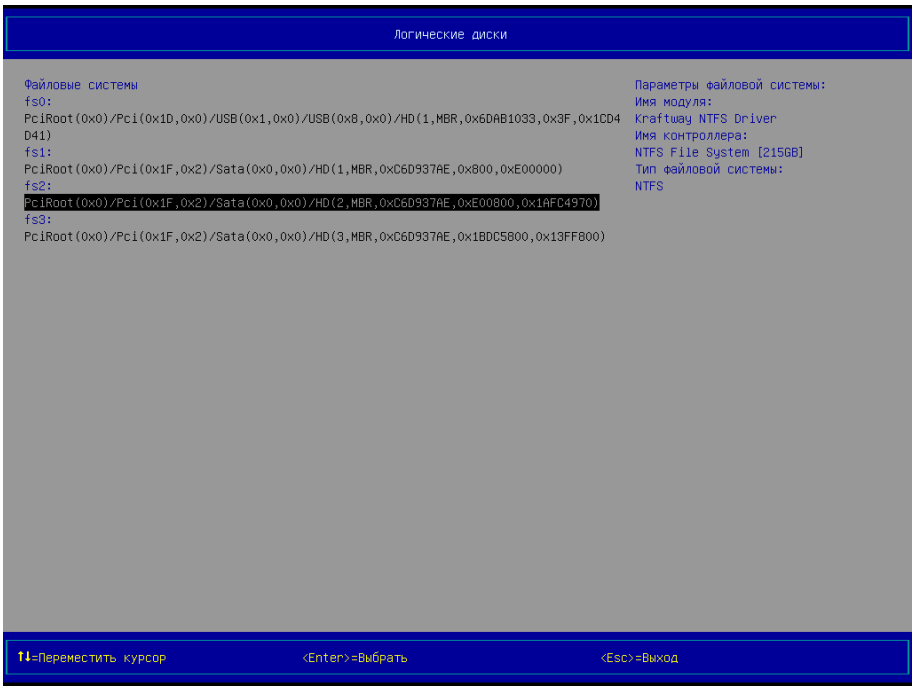

Рисунок 3.72 – Логические диски (вид 1)

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 3.73), с предложением ввести новое имя для выбранного диска;

Рисунок 3.73 – 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 3.74);

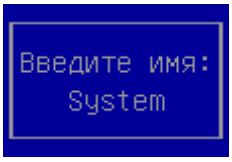

Рисунок 3.74 – Окно *Введите имя* (вид 2),
имя диска, присвоенное пользователем

→ [Enter] на клавиатуре, новое имя диска сохранится в KSS (см.

7) Рисунок 3.75);

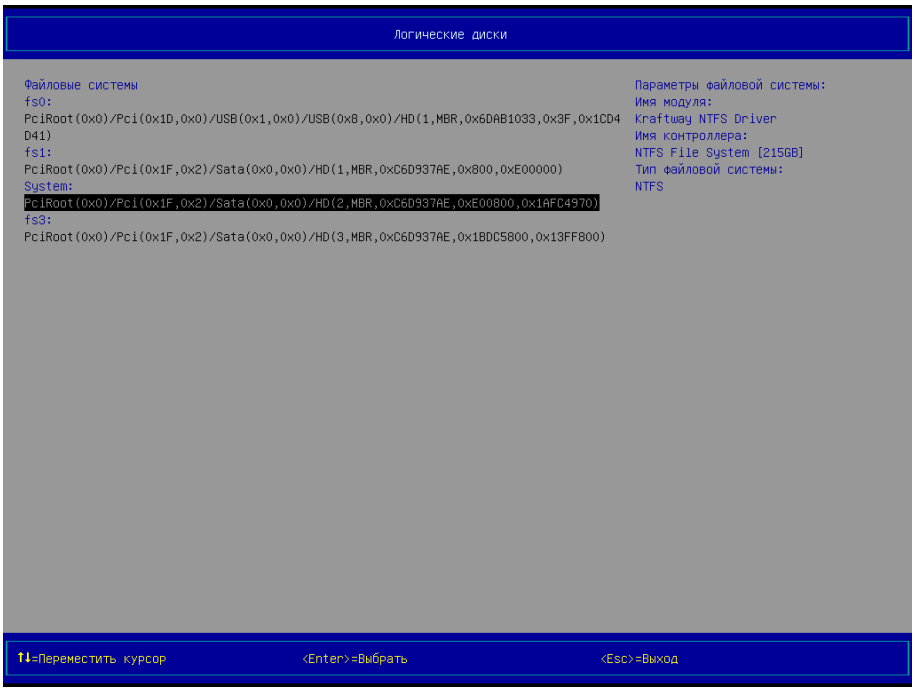

Рисунок 3.75 – Логические диски (вид 2)

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

3.9 Журнал событий

Модуль *Журнал событий* предназначен для записи событий всех включенных модулей KSS. Записи заносятся в общий журнал событий.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.9.1 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 3.76) с пунктом *Включение модуля управления журналом событий*;

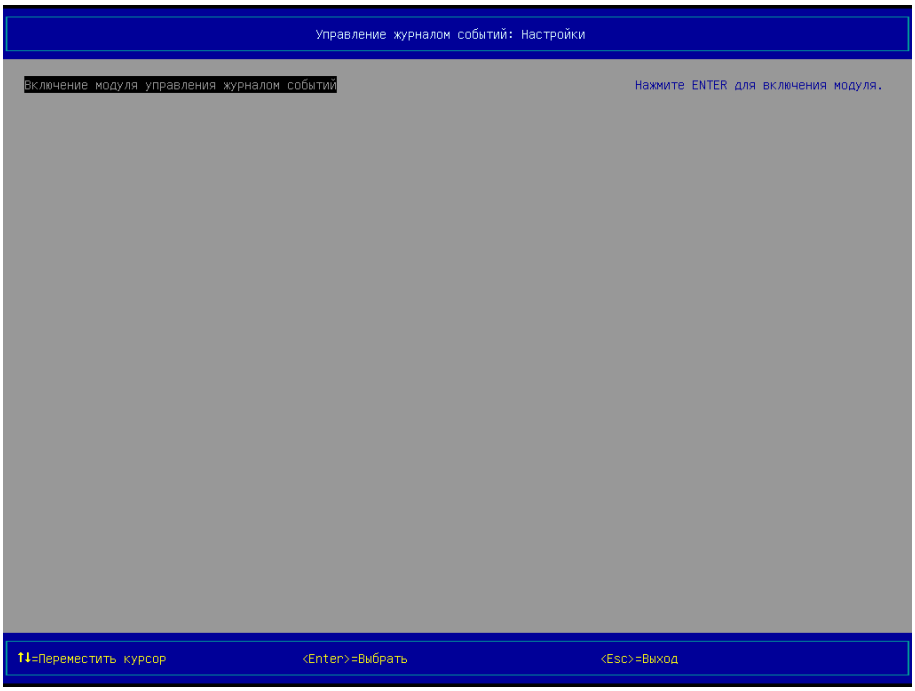

Рисунок 3.76 – Страница *Управление журналом событий: Настройки* (вид 1), пункт *Включение модуля управления журналом событий*

11) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится диалоговое окно (см. Рисунок 3.77), запрашивающее подтверждение на включение модуля;

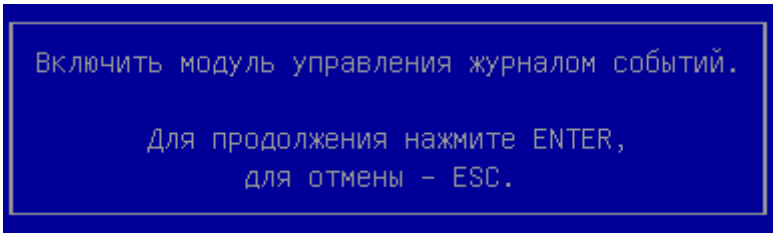

Рисунок 3.77 – Запрос подтверждения на *включение модуля управления журналом событий*

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 3.17).

3.9.2 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 3.17);

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 3.78) с пунктом *Выключение модуля управления журналом событий*;

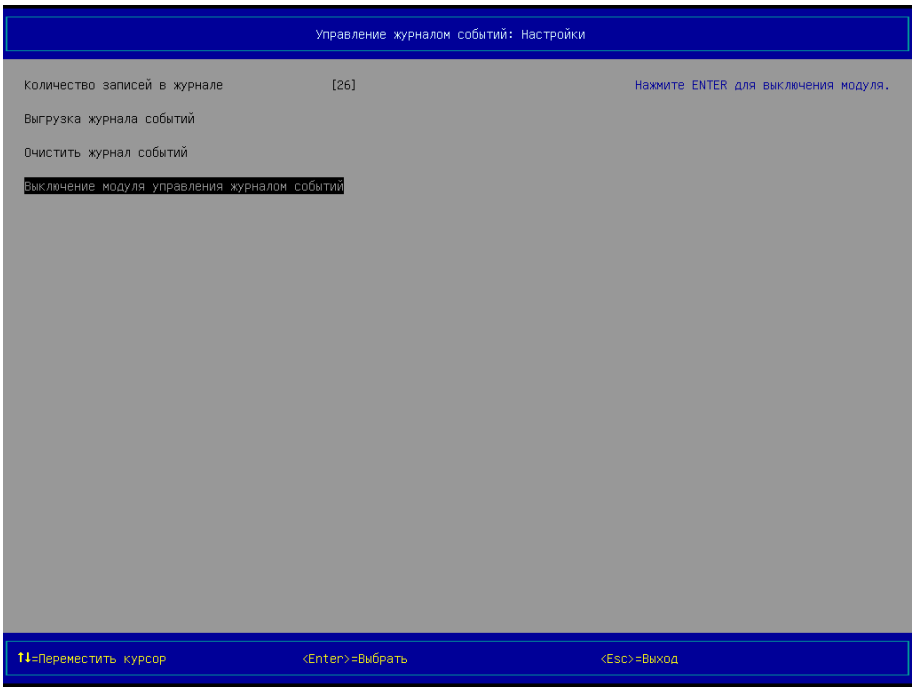

Рисунок 3.78 – Страница *Управление журналом событий: Настройки* (вид 2), пункт *Выключение модуля управления журналом событий*

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

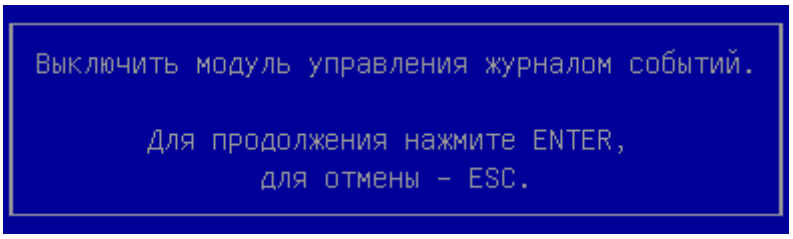

Рисунок 3.79 – Запрос подтверждения на
Выключение модуля управления журналом событий

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).

3.9.3 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 3.80).

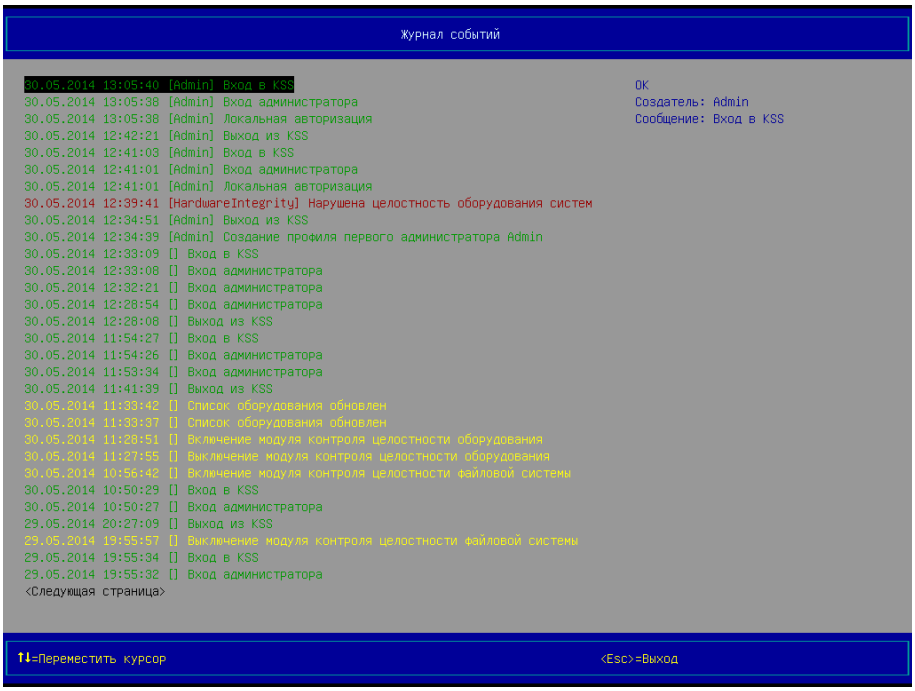

Рисунок 3.80 – Страница *Журнал событий*

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 KSS возможен только после включения модуля *Электронный замок “Витязь”* (см. п. 3.4).

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

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

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

5. В KSS 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.

3.9.4 Сохранение журнала событий в файл

Для сохранения журнала событий KSS 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 3.17);

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 3.81) с пунктом *Выгрузка журнала событий*;

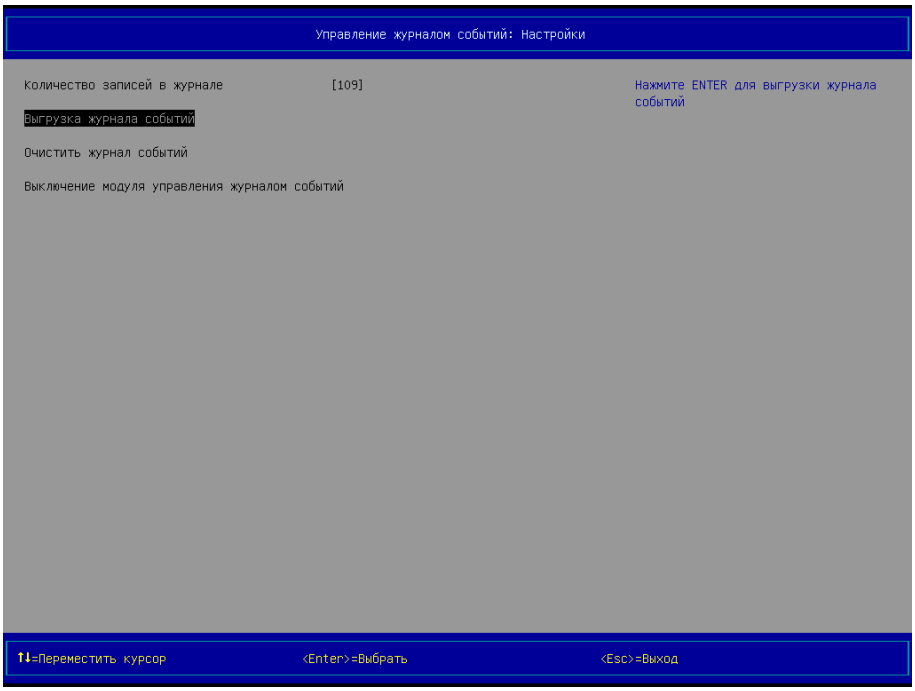

Рисунок 3.81 – *Управление журналом событий: Настройки*, *Выгрузка журнала событий*

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 3.82), информирующее администратора об успешном сохранении журнала событий;

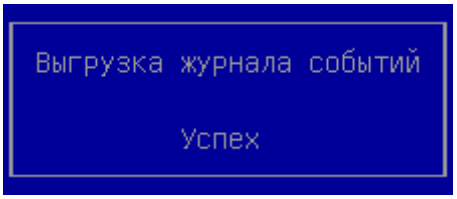

Рисунок 3.82 – Успешное сохранение журнала событий

8) нажать любую клавишу на клавиатуре.

Примечания:

1. Сохранение журнала событий KSS в файл возможно только после включения модуля *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 3.83), информирующее об отсутствии устройства памяти.

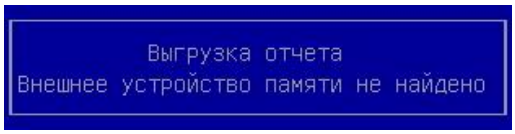

Рисунок 3.83 – Окно, информирующее об отсутствии устройства памяти

5. Если сохранить журнал событий в файл невозможно, то на экран выводится окно (см. Рисунок 3.84).

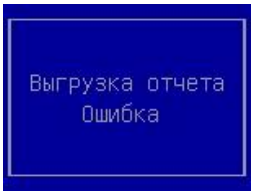

Рисунок 3.84 – Сохранить журнал в файл невозможно

3.9.5 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 3.17);

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 3.85) с пунктом *Очистить журнал событий*;

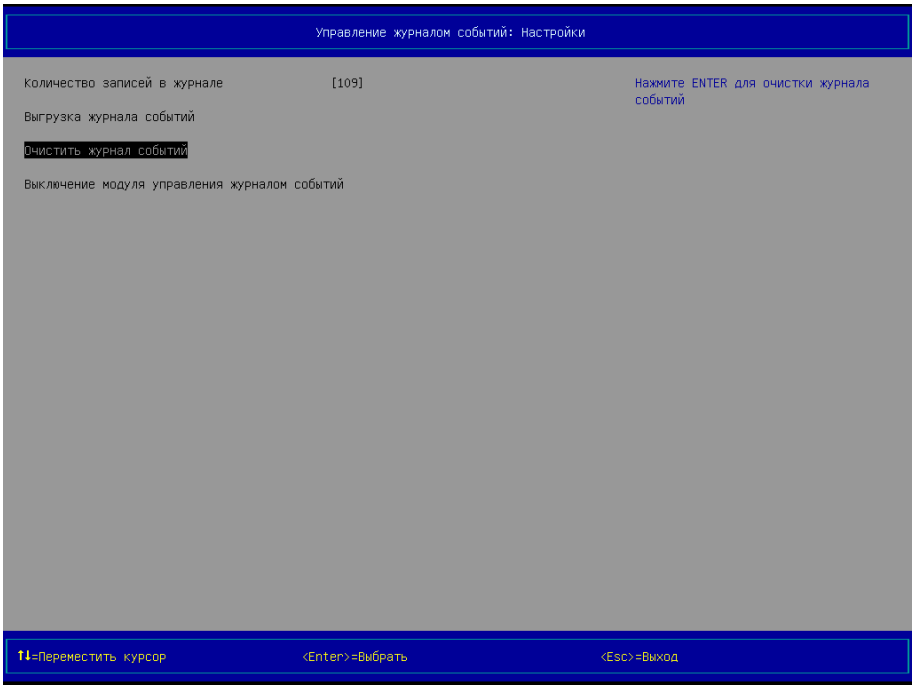

Рисунок 3.85 – *Управление журналом событий: Настройки*, *Очистить журнал событий*

5) выбрать пункт *Очистить журнал событий*;

6) → [Enter] на клавиатуре, после выполнения данного действия на экран выводится окно (см. Рисунок 3.86), запрашивающее подтверждение на очистку журнала событий;

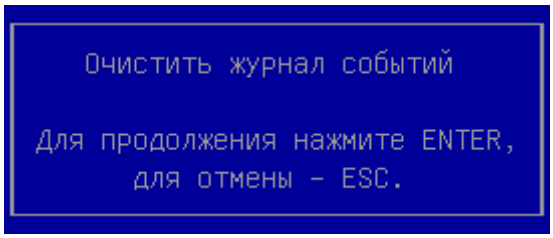

Рисунок 3.86 – Запрос подтверждения на очистку журнала событий

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

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

3.10 Управление обновлениями

Модуль *Управление обновлениями* предназначен для выбора и установки доступных обновлений модулей и драйверов KSS как в ручном, так и в автоматическом режимах. Для управления резервными копиями и для просмотра истории обновлений.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.10.1 Включение модуля *Управления обновлениями*

Для включения модуля *Управления обновлениями* оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

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

3) выберите в разделе *Настройки модулей безопасности* пункт *Управление обновлениями* со статусом [Выкл];

4) → [Enter] на клавиатуре, на экран выводится страница «Настройка сети: Настройки» (см. Рисунок 3.87);

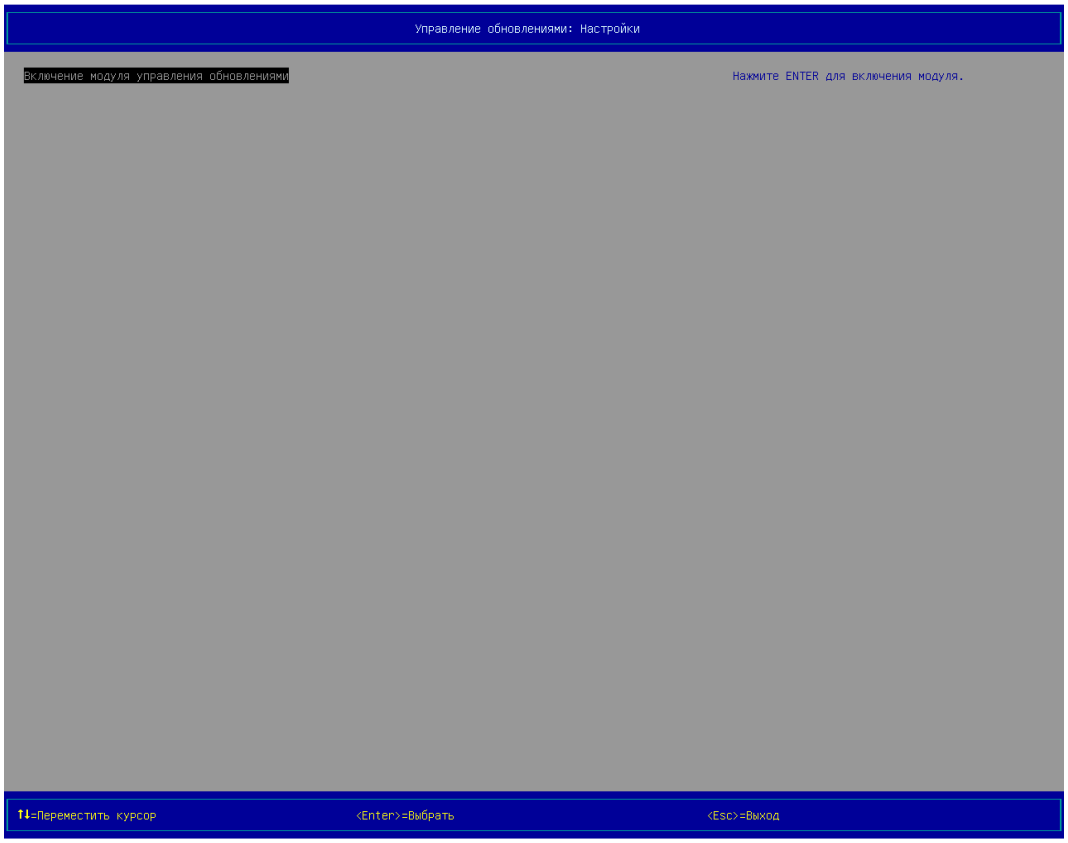

Рисунок 3.87 - Пункт *Включение модуля управления обновлениями*

5) выберите пункт *Включение модуля управления обновлениями* для включения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на включение модуля *Управления обновлениями* (см. Рисунок 3.88);

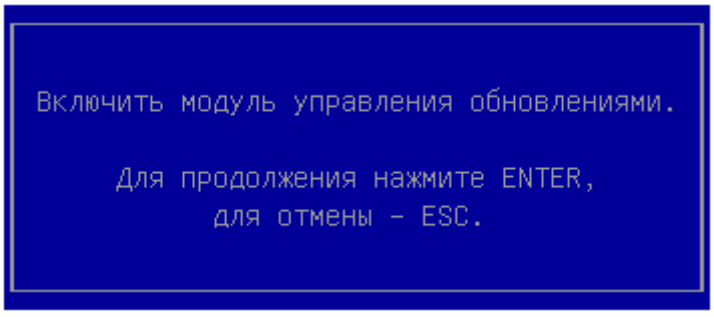

Рисунок 3.88 - Окно подтверждения на включение модуля *Управления обновлениями*

7) подтвердите команду по включению модуля *Управления обновлениями* → [Enter], для отмены включения – нажмите клавишу "Esc". На экран выводится окно

«Настройки» (см. Рисунок 3.17). Статус пункта *Управление обновлениями* изменится с [Выкл] на [Вкл];

3.10.2 Выключение модуля *Управление обновлениями*

Для выключения модуля *Управление обновлениями* оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Управление обновлениями* со статусом [Вкл];

4) → [Enter] на клавиатуре, на экран выводится страница «Управление обновлениями: Настройки» (см. Рисунок 3.89);

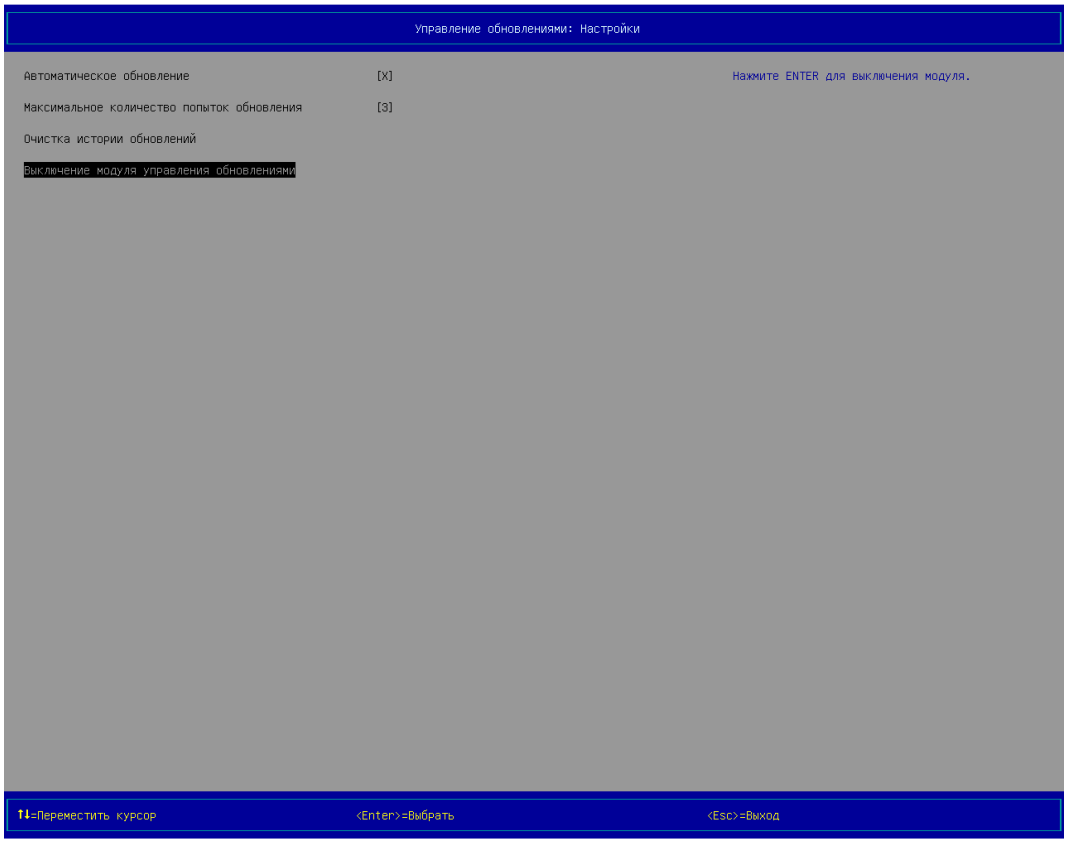

Рисунок 3.89 – Пункт *Выключение модуля управления обновлениями*

5) выберите пункт *Выключение модуля управления обновлениями* для выключения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на выключение модуля *Управления обновлениями* (см. Рисунок 3.90);

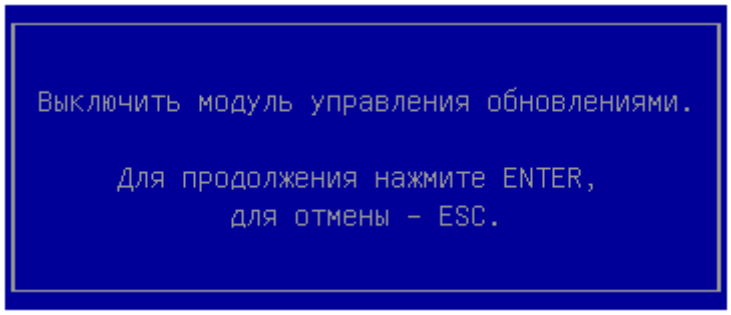

Рисунок 3.90 – Окно подтверждения на выключение модуля *Управления обновлениями*

7) подтвердите команду по выключению модуля *Управления обновлениями* → [Enter], для отмены выключения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.5). Статус пункта *Настройки сети* изменится с [Вкл] на [Выкл];

3.10.3 Настройка модуля *Управления обновлениями*

Для настройки модуля *Управления обновлениями* оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Управление обновлениями* со статусом [Вкл];

4) → [Enter] на клавиатуре, на экран выводится страница «Управление обновлениями: Настройки» (см. Рисунок 3.89);

Пользователю доступны следующие пункты для настройки модуля *Управления обновлениями*:

5) выберите пункт *Автоматическое обновление*, поставьте метку – для обновления модулей в автоматическом режиме без подтверждения от пользователя;

6) выберите пункт *Максимальное количество попыток обновления*, введите числовое значение – количество попыток автоматического обновления модулей на новую версию. При превышении этого количества, новая версия больше не будет устанавливаться.

7) выберите пункт *Очистка истории обновления* – нажмите клавишу [Enter] для очистки истории обновлений.

3.10.4 Управление обновлениями

Для управления обновлениями оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница «Управление обновлениями» (см. Рисунок 3.91);

Рисунок 3.91 – Страница «Управление обновлениями»

Пользователю доступны следующие пункты для настройки *управления обновлениями*:

3) выберите пункт *Загрузка обновлений* – нажмите [Enter] для загрузки обновления из файла. Откроется страница «Файловый менеджер» (см. Рисунок 3.92). Выберите требуемый файл обновления;

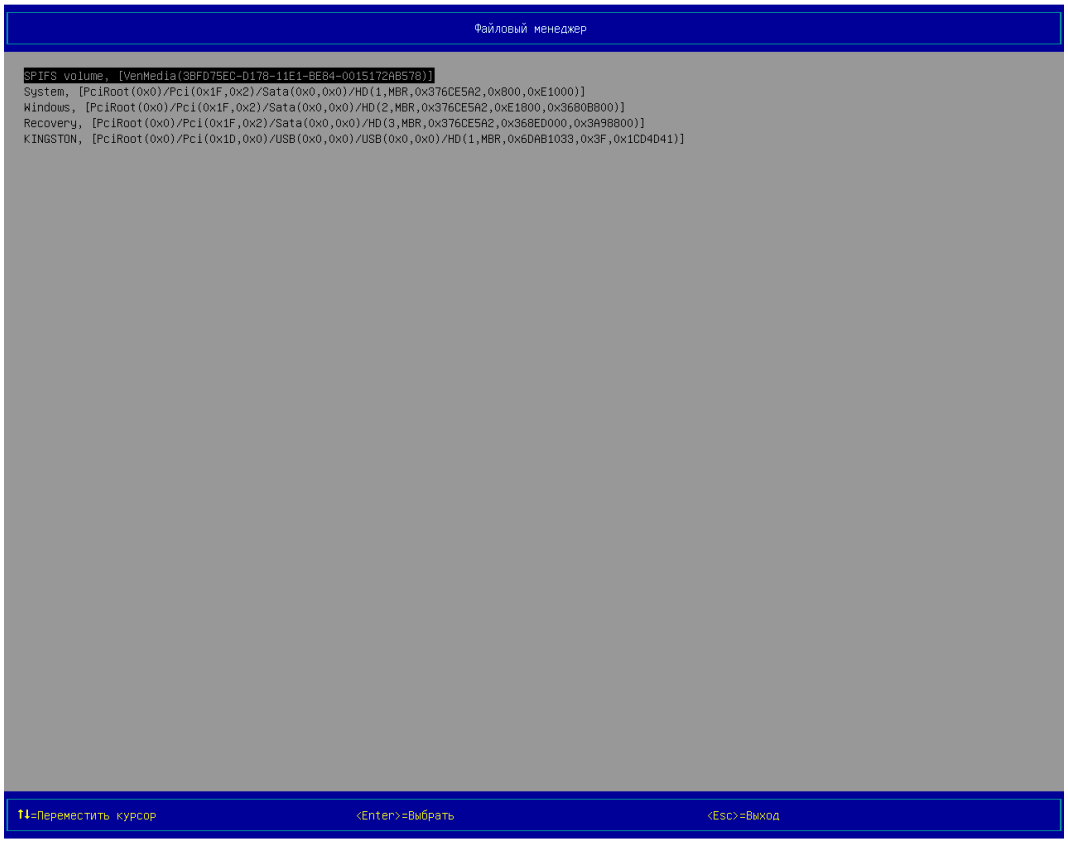

Рисунок 3.92 – Страница «Файловый менеджер»

4) выберите пункт *Доступные обновления* – для выбора доступных обновлений;

5) выберите пункт *Доступные резервные копии* – для выбора резервной копии;

6) выберите пункт *История обновлений* – для просмотра истории обновлений.

3.11 Настройка сети

Модуль *Настройка сети* позволяет настроить параметры сетевого интерфейса. Настройки сети позволяют установить соединение KSS с сервером безопасности KSC для удаленного управления и синхронизации параметров.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

Внимание! Предварительно должна быть включена поддержка протокола IP в UEFI материнской платы.

3.11.1 Включение сетевого модуля

Для включения сетевого модуля оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

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

3) выберите в разделе *Настройки модулей безопасности* пункт *Настройка сети* со статусом [Выкл];

4) → [Enter] на клавиатуре, на экран выводится страница *Настройка сети: Настройки* (см. Рисунок 3.93);

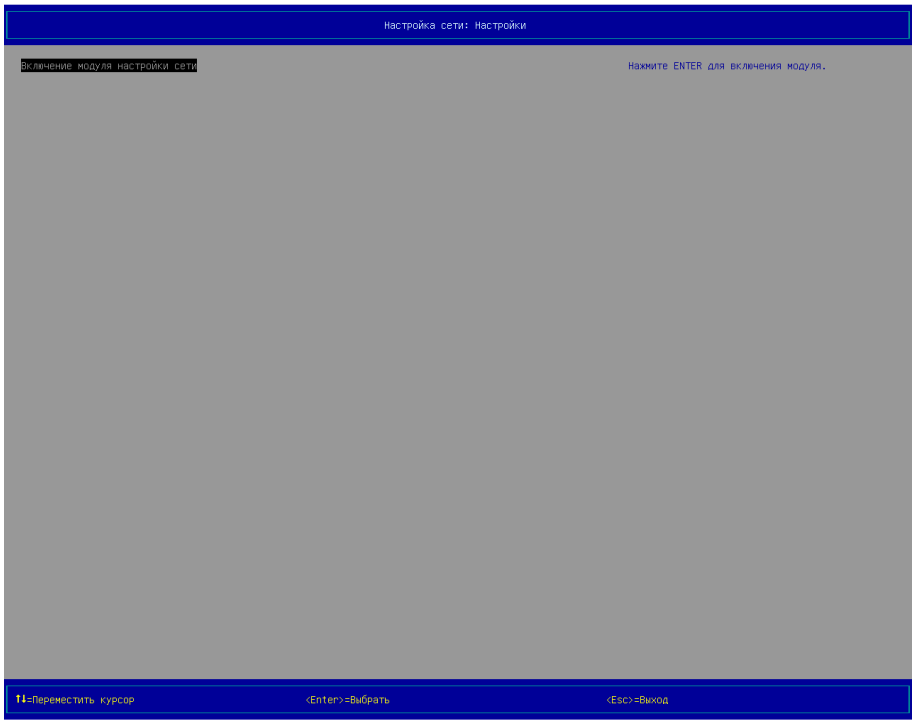

Рисунок 3.93 – Пункт *Включение модуля настройки сети*

5) выберите пункт *Включение модуля настройки сети* для включения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на включение *модуля настройки сети* (см. Рисунок 3.94);

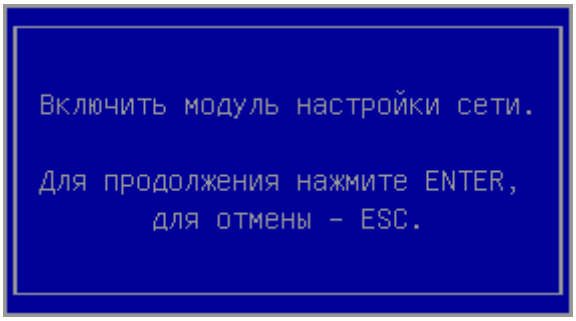

Рисунок 3.94 – Окно подтверждения на включение *модуля настройки сети*

7) подтвердите команду по включению *модуля настройки сети* → [Enter], для отмены включения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.17). Статус пункта *Настройки сети* изменится с [Выкл] на [Вкл];

3.11.2 Выключение модуля *Настройка сети*

Для выключения сетевого модуля оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

9) → [Enter] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17);

10) выберите в разделе *Настройки модулей безопасности* пункт *Настройка сети* со статусом [Вкл];

11) → [Enter] на клавиатуре, на экран выводится страница *Настройка сети: Настройки* (см. Рисунок 3.95);

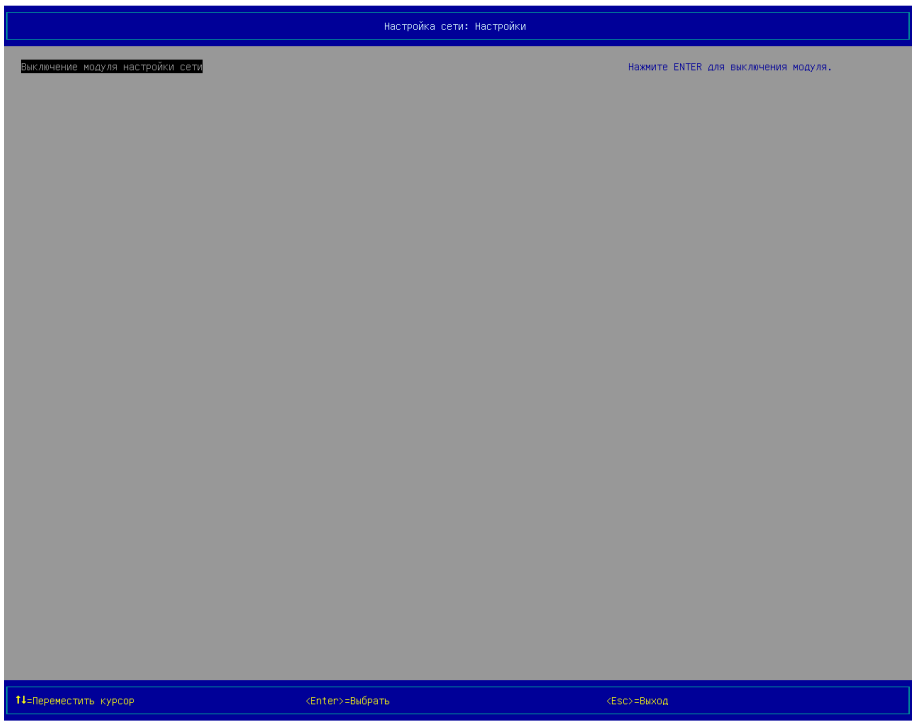

Рисунок 3.95 – Пункт *Выключение модуля настройки сети*

12) выберите пункт *Выключение модуля настройки сети* для выключения модуля;

13) → [Enter] на клавиатуре, на экран выводится окно подтверждения на выключение *Модуля настройки сети* (см. Рисунок 3.96);

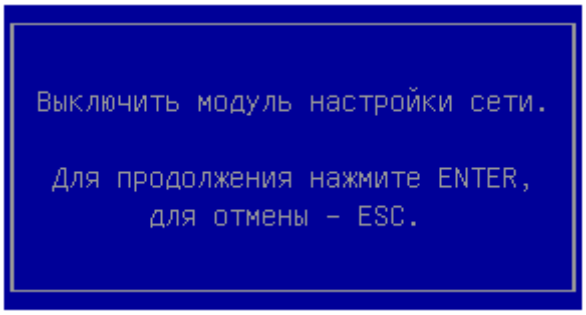

Рисунок 3.96 – Окно подтверждения на выключение *Модуля настройки сети*

14) подтвердите команду по выключению *Модуля настройки сети* → [Enter], для отмены выключения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.5). Статус пункта *Настройки сети* изменится с [Вкл] на [Выкл];

3.11.3 Настройка сетевых параметров

Для настройки сетевого модуля оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

1. выберите пункт *Настройка сети* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2. → [Enter] на клавиатуре, на экран выводится страница «Настройка сети» (см. Рисунок 3.97);

Рисунок 3.97 – Страница «Настройка сети»

3. выберите пункт *Интерфейс*, → [Enter], на экран выводится окно для ввода имени сетевого интерфейса (см. Рисунок 3.98), введите имя сетевого интерфейса (выберите необходимый если их несколько);

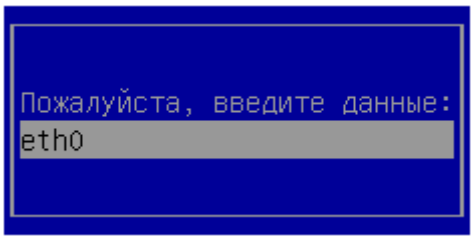

Рисунок 3.98 – Ввод имени сетевого интерфейса

4. → [Enter] для подтверждения;

5. выберите пункт *Тип конфигурации*, → [Enter], на экран выводится окно выбора способа ввода значений параметров (см. Рисунок 3.99);

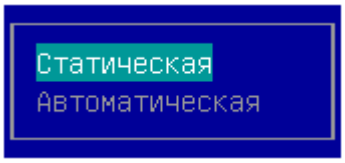

Рисунок 3.99 – Выбор способа ввода значений

6. выберите способ ввода значений параметров сети:

a) Статическая – введите значения параметров вручную:

- *IP Адрес* (назначенный IP адрес этого компьютера);
- *Маска сети* (для протокола IP);
- *Маршрутизатор* (IP адрес маршрутизатора);
- *Первичный сервер DNS* (IP адрес);
- *Вторичный сервер DNS* (IP адрес);
- *Имя домена*.

Выберите пункт с соответствующим параметром, → [Enter], на экран выводится окно ввода значений (см. Рисунок 3.100), → [Enter] для подтверждения;

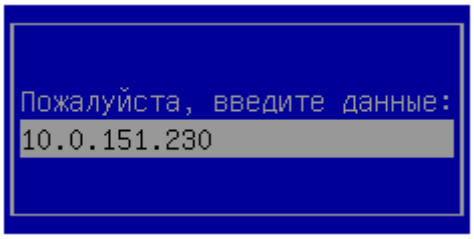

Рисунок 3.100 – Ввод значений параметров сети

b) Автоматическая – значения параметров: *IP Адрес*, *Маска сети*, *Маршрутизатор*, *Первичный сервер DNS*, *Вторичный сервер DNS*, *Имя домена* – присваиваются автоматически сервером DHCP.

7. После настройки и сохранения сетевых параметров необходимо перезагрузить компьютер. При следующем старте компьютера, до окна выбора загрузки KSS, появятся сообщения, подтверждающие включение сетевого модуля (см. Рисунок 3.101).

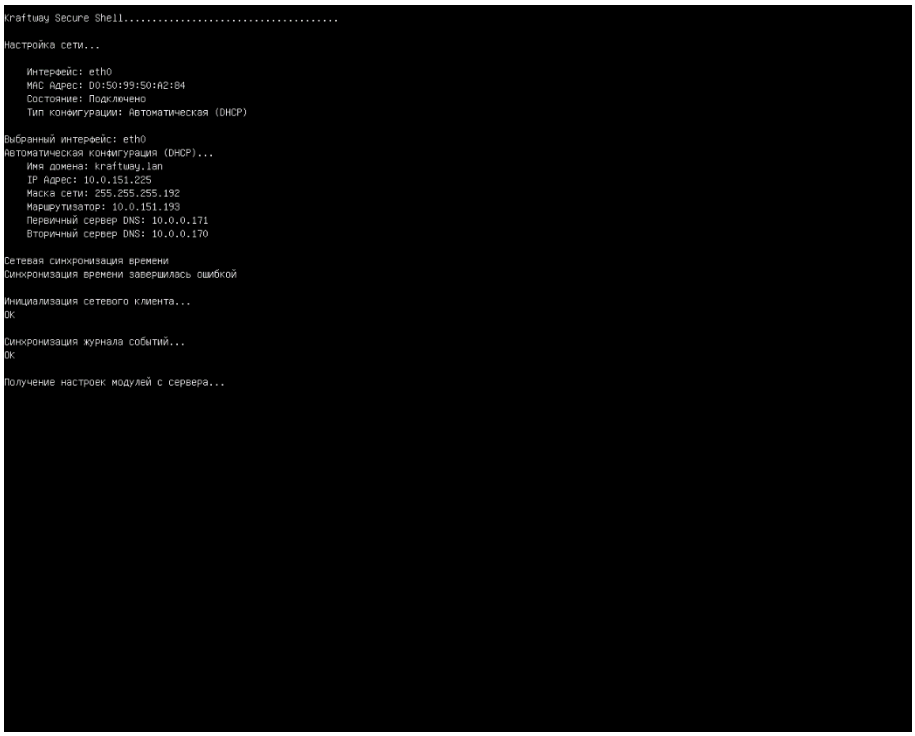

Рисунок 3.101 – Сообщения о работе сетевого модуля

3.12 Сетевой клиент сервера безопасности

Модуль *Сетевой клиент сервера безопасности* позволяет синхронизировать работу модулей оболочки KSS с сервером безопасности KSC. Для синхронизации необходимо настроить сеть, создать соединение с сервером безопасности и выбрать необходимые для синхронизации параметры.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.12.1 Включение модуля *Сетевой клиент безопасности*

Для включения модуля KSS *Сетевой клиент сервера безопасности* необходимо выполнить следующие действия:

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

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

3) выберите в разделе *Настройки модулей безопасности* пункт *Сетевой клиент безопасности* со статусом [Выкл];

4) → [Enter] на клавиатуре, на экран выводится страница *Сетевой клиент безопасности: Настройки* (см. Рисунок 3.102);

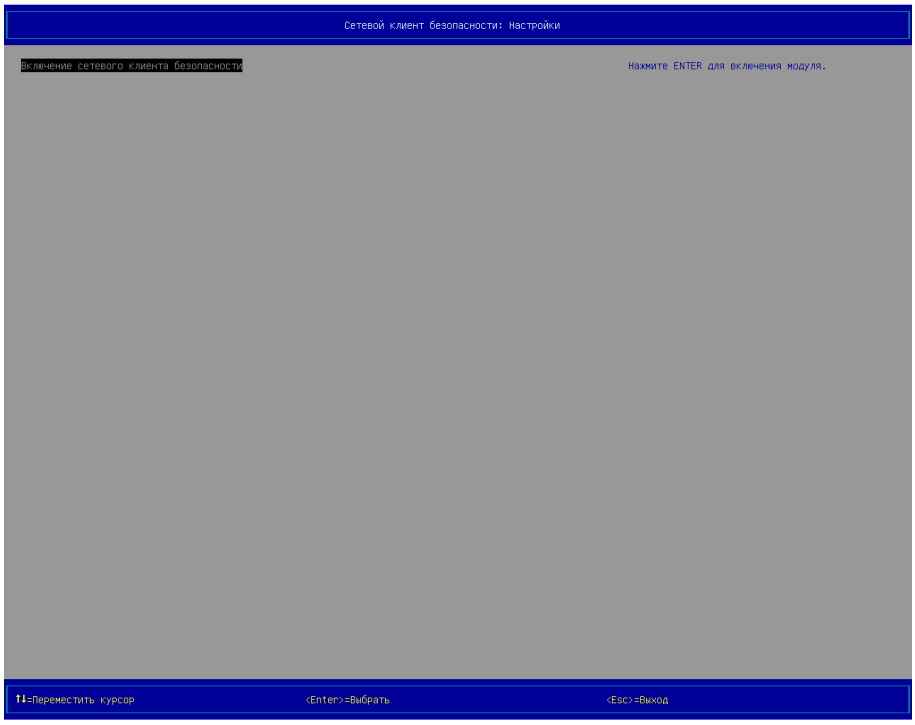

Рисунок 3.102 – Пункт *Включение сетевого клиента безопасности*

5) выберите пункт *Включение сетевого клиента безопасности* для включения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на включение *модуля Сетевого клиента безопасности* (см. Рисунок 3.103);

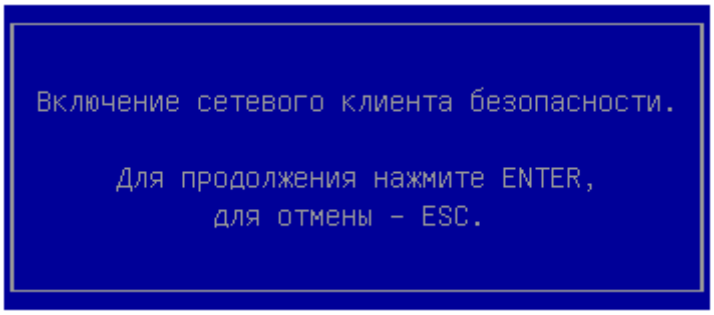

Рисунок 3.103 – Окно подтверждения на включение *модуля Сетевого клиента безопасности*

7) подтвердите команду по включению *модуля Сетевого клиента безопасности*, → [Enter], для отмены включения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.17). Статус пункта *Настройки сети* изменится с [Выкл] на [Вкл];

3.12.2 Выключение модуля *Сетевого клиента безопасности*

Для выключения *Сетевого клиента безопасности* оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Сетевой клиент безопасности* со статусом [Вкл];

4) → [Enter] на клавиатуре, на экран выводится страница *Сетевой клиент безопасности: Настройки* (см. Рисунок 3.104);

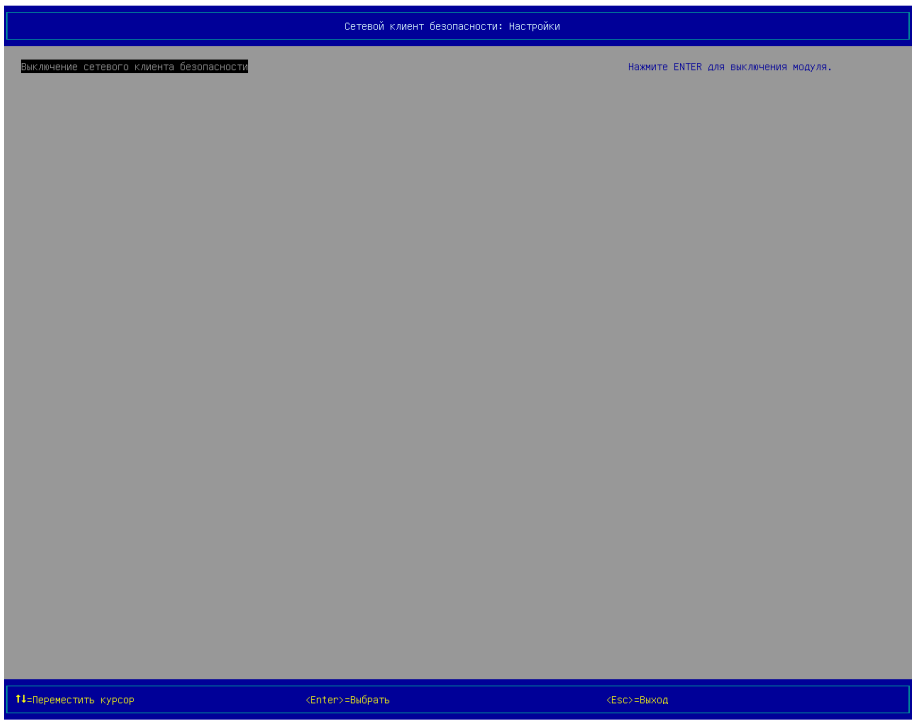

Рисунок 3.104 – Пункт *Выключение сетевого клиента безопасности*

5) выберите пункт *Выключение сетевого клиента безопасности* для выключения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на выключение *Сетевого клиента безопасности* (см. Рисунок 3.105);

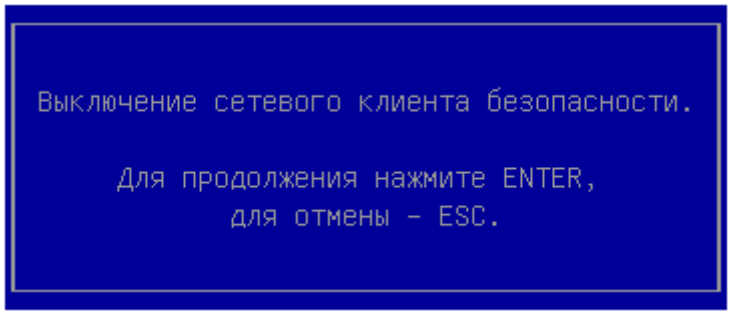

Рисунок 3.105 – Окно подтверждения на выключение *Сетевого клиента безопасности*

7) подтвердите команду по выключению *Сетевого клиента безопасности* → [Enter], для отмены выключения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.5). Статус пункта *Сетевого клиента безопасности* изменится с [Вкл] на [Выкл];

3.12.3 Настройки модуля *Сетевого клиента безопасности*

Для настройки модуля *Сетевого клиента безопасности* оболочки Kraftway Security Shell необходимо выполнить следующие действия:

1) выберите пункт *Сетевой клиент безопасности* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница *Сетевой клиент безопасности* (см. Рисунок 3.106);

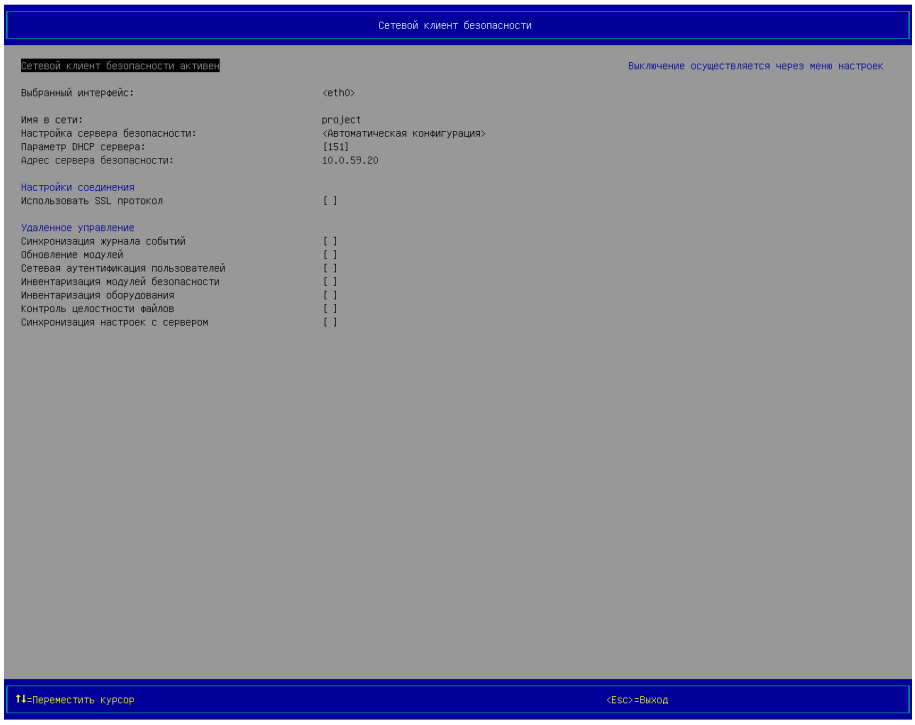

Рисунок 3.106 – Страница «Сетевой клиент безопасности» (Вид 1), все пункты настроек неактивны

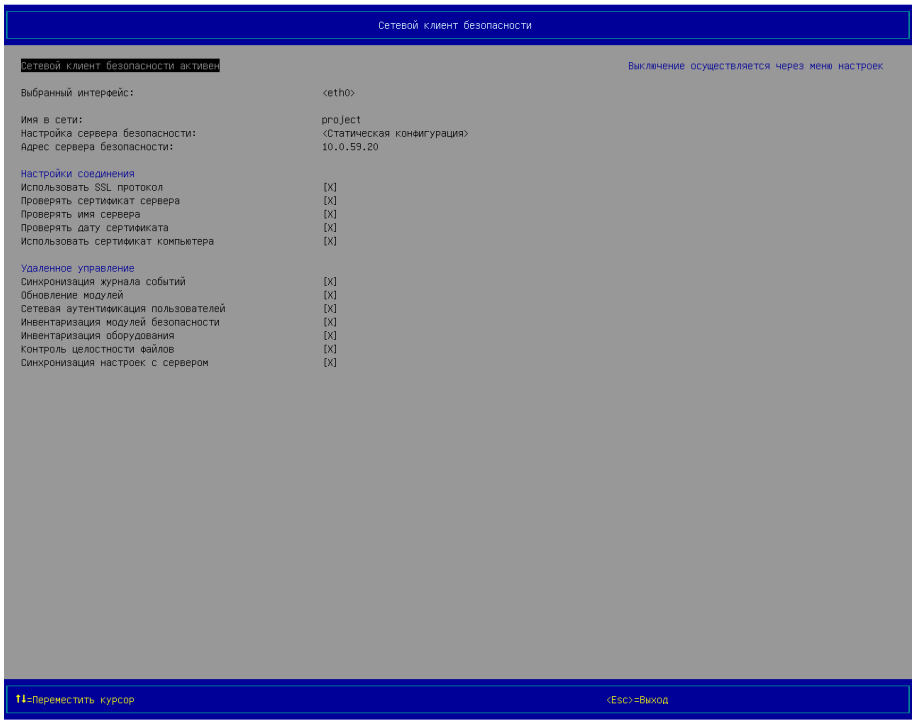

Рисунок 3.107 – Страница «Сетевой клиент безопасности» (Вид 2), все пункты настроек активны

1) Настройки параметров сервера безопасности

1. выберите пункт *Имя в сети*, → [Enter], на экран выводится окно для ввода имени (см. Рисунок 3.108), введите *Имя* компьютера *в сети*;

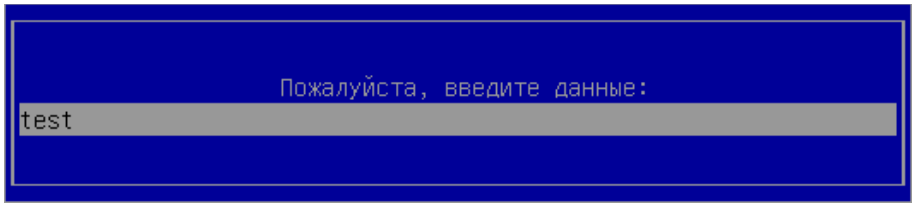

Рисунок 3.108 – Ввод имени компьютера в сети

2. выберите пункт *Настройка сервера безопасности*, → [Enter], на экран выводится окно выбора способа ввода значений параметров (см. Рисунок 3.109);

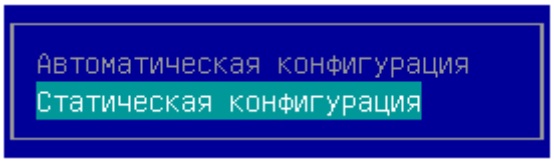

Рисунок 3.109 – Выбор способа настройки

3. выберите способ *Настройки* параметров *сервера безопасности*:

– *Автоматическая конфигурация*

Выберите пункт *Параметр DHCP сервера*, → [Enter], поле ввода данных становится активным (см. Рисунок 3.110), введите значение *Параметра DHCP сервера* (по умолчанию 151). Значение параметра *IP Адрес сервера безопасности* будет установлено автоматически сервером DHCP;

– *Статическая конфигурация*

Выберите пункт *Адрес сервера безопасности*, → [Enter], на экран выводится окно ввода данных (см. Рисунок 3.110), введите значение параметра *IP Адрес сервера безопасности*;

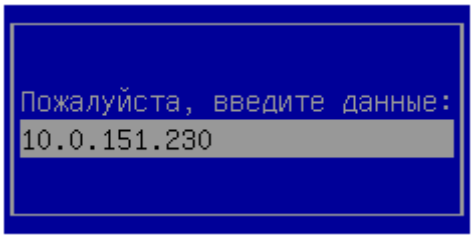

Рисунок 3.110 – Ввод значений параметров сети

2) Настройка соединения с сервером безопасности

1. выберите пункт *Использовать SSL протокол*, при использовании криптографического протокола для соединения с сервером безопасности, → [Enter], параметр будет активирован, на экран выводятся дополнительные параметры:

– активируйте пункт *Проверять сертификат сервера* – для проверки подлинности сертификата сервера безопасности;

– активируйте пункт *Проверять имя сервера* – для проверки имени сервера безопасности в сертификате сервера безопасности;

– активируйте пункт *Проверять дату сертификата* – для проверки срока действия сертификата сервера безопасности;

2. активируйте пункт *Использовать сертификат компьютера* – для проверки сертификата компьютера при соединении с сервером безопасности.

3) Настройка параметров удаленного управления KSS

1. активируйте пункт *Синхронизация журнала событий* – для отправки локального *Журнала событий* на сервер безопасности;

2. активируйте пункт *Обновление модулей* – для обновления модулей KSS с сервера безопасности (необходим *Сертификат обновлений*);

3. активируйте пункт *Сетевая аутентификация пользователей* – для аутентификации локальных пользователей (необходима регистрация ИУ на сервере безопасности;

4. активируйте пункт *Инвентаризация модулей безопасности* – для пересылки списка модулей безопасности установленных в KSS на сервер безопасности;

5. активируйте пункт *Инвентаризация оборудования* – для пересылки списка оборудования компьютера на сервер безопасности;

6. активируйте пункт *Контроль целостности файлов* – для получения с сервера безопасности *Списка* для контроля целостности файлов (список файлов, созданный на

сервере безопасности в добавление к локальным спискам файлов) и отправки контрольных сумм файлов на сервер;

7. активируйте пункт *Синхронизация настроек с сервером* – для удаленной настройки конфигурации и параметров модулей KSS с сервера безопасности.

3.13 Синхронизация времени

Модуль *Синхронизации времени* предназначен для синхронизации времени рабочей станции через сеть Интернет или через локальную сеть с сервера безопасности KSC. Настройка времени происходит при инициализации рабочей станции в сети.

Примечание. Список параметров для удаленного администрирования с сервера безопасности смотри в Главе 4 Передача значений параметров модулей KSS с сервера KSC

3.13.1 Включение синхронизации времени

Для включения модуля KSS *Синхронизация времени* необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница «Настройки» (см. Рисунок 3.5);

3) выберите в разделе *Настройки модулей безопасности* пункт *Синхронизация времени* со статусом [Выкл];

4) → [Enter] на клавиатуре, на экран выводится страница «Синхронизация времени» (см. Рисунок 3.111);

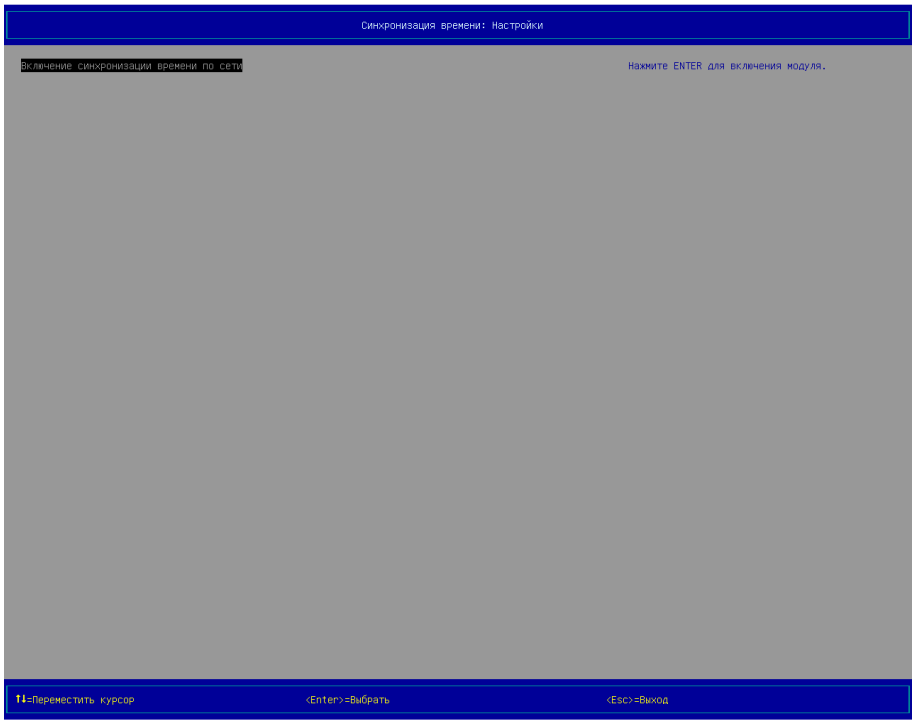

Рисунок 3.111 – Пункт *Включение синхронизации времени*

5) выберите пункт *Включение синхронизации времени* для включения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на включение модуля *Синхронизации времени* (см. Рисунок 3.112);

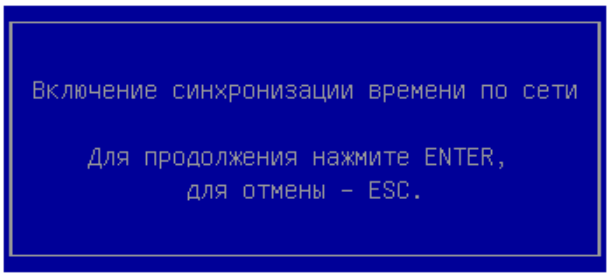

Рисунок 3.112 – Окно подтверждения на включение модуля *Синхронизации времени*

7) подтвердите команду по включению модуля *Синхронизации времени*, → [Enter], для отмены включения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.17). Статус пункта *Синхронизации времени* с [Выкл] на [Вкл];

3.13.2 Выключение модуля Синхронизации времени

Для выключения модуля *Синхронизации времени* оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница «Настройки» (см. Рисунок 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Синхронизации времени* со статусом [Вкл];

4) → [Enter] на клавиатуре, на экран выводится страница «Синхронизации времени» (см. Рисунок 3.113);

5) выберите пункт *Выключение синхронизации времени* для выключения модуля;

6) → [Enter] на клавиатуре, на экран выводится окно подтверждения на выключение *Синхронизации времени* (см. Рисунок 3.114);

7) подтвердите команду по выключению *Синхронизации времени* → [Enter], для отмены выключения – нажмите клавишу "Esc". На экран выводится окно «Настройки» (см. Рисунок 3.5). Статус пункта *Синхронизация времени* изменится с [Вкл] на [Выкл];

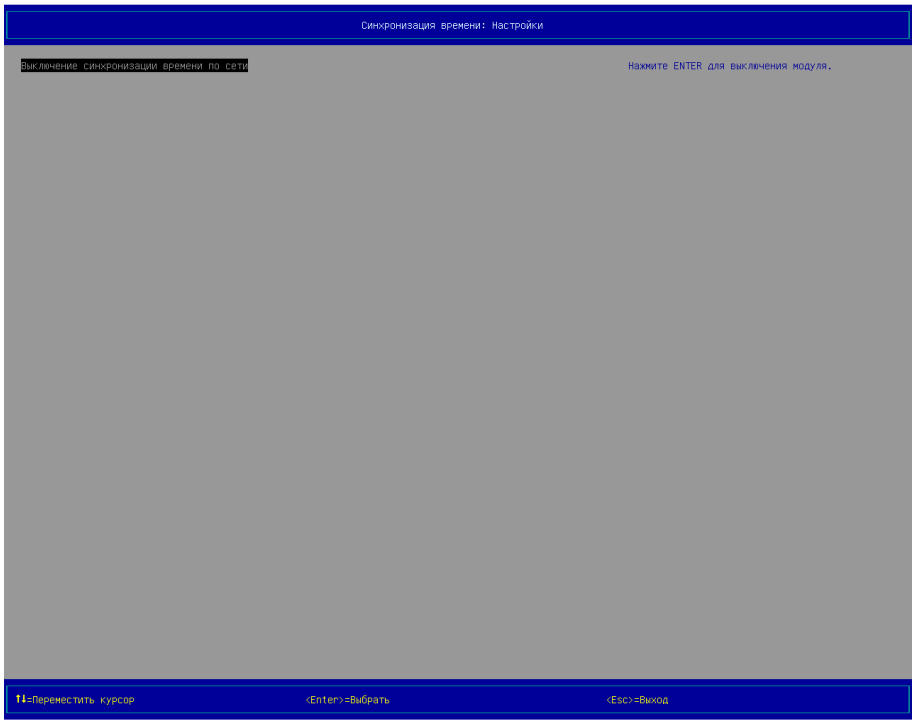

Рисунок 3.113 – Пункт *Выключение синхронизации времени*

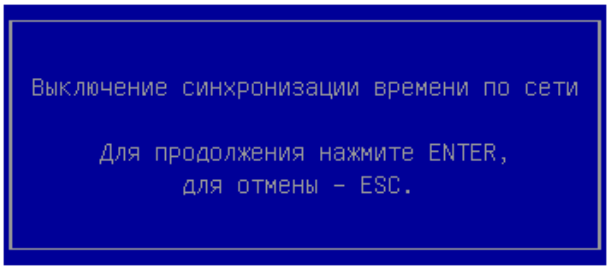

Рисунок 3.114 – Окно подтверждения на выключение *Синхронизации времени*

3.13.3 Настройка синхронизации времени

1) выберите пункт *Синхронизация времени* в разделе *Модули безопасности*, в главном меню KSS (см. Рисунок 3.2);

2) → [Enter] на клавиатуре, на экран выводится страница «Синхронизация времени» (см. Рисунок 3.115);

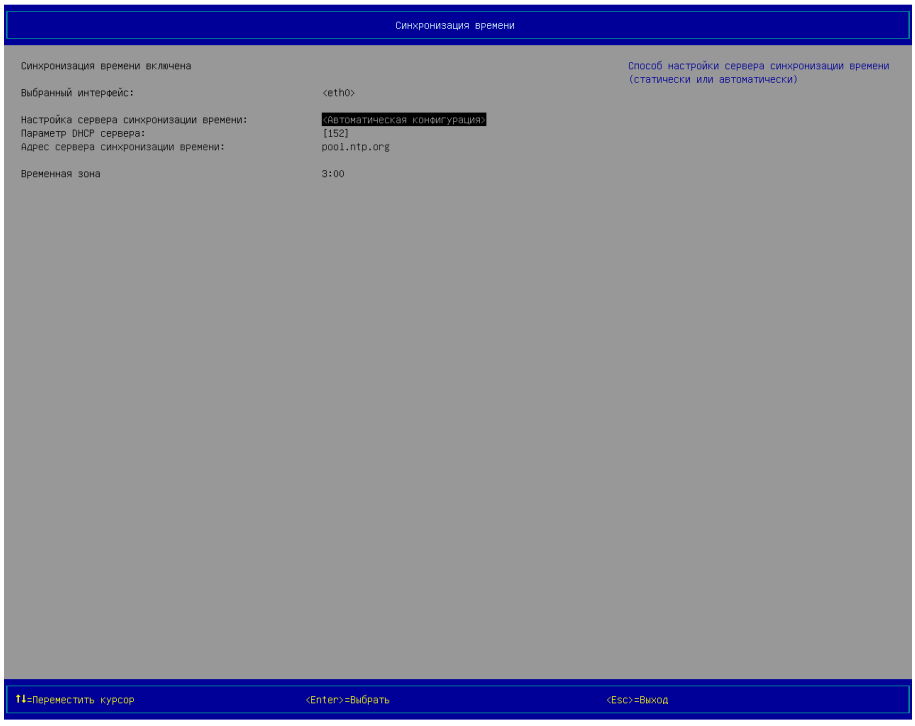

Рисунок 3.115 – Страница «Синхронизация времени»

1) выберите пункт *Выбранный интерфейс*, → [Enter], на экран выводится окно выбора сетевого интерфейса (см. Рисунок 3.116), выберите требуемый сетевой интерфейс;

Рисунок 3.116 – Окно выбора сетевого интерфейса

2) выберите пункт *Настройка сервера синхронизации времени*, → [Enter], на экран выводится окно выбора сетевого интерфейса (см. Рисунок 3.117), выберите требуемый способ настройки сервера синхронизации времени;

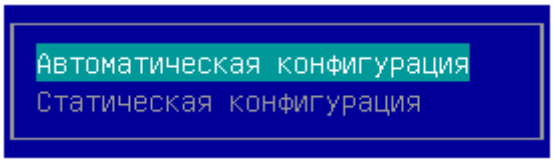

Рисунок 3.117 – Окно выбора сетевого интерфейса

– *Автоматическая конфигурация*

Выберите пункт *Параметр DHCP сервера*, → [Enter], поле ввода данных становится активным, введите значение *Параметра DHCP сервера* (по умолчанию 152). Значение параметра *Адрес сервера синхронизации времени* будет установлено автоматически сервером DHCP;

– *Статическая конфигурация*

Выберите пункт *Адрес сервера синхронизации времени*, → [Enter], на экран выводится окно ввода данных (см. Рисунок 3.118), введите адрес сервера, вида: «pool.ntp.org»;

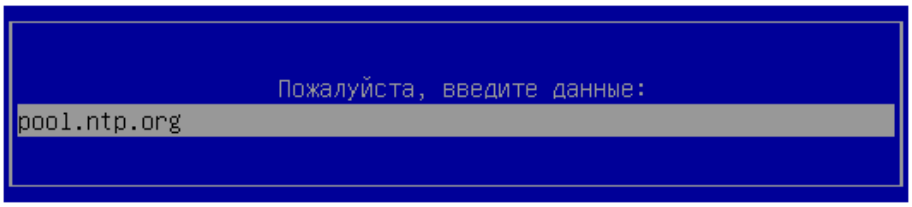

Рисунок 3.118 – Окно ввода адреса сервера синхронизации времени

3) → [Enter], для подтверждения введенных данных;

4) выберите пункт *Временная зона* – значение временной зоны в формате +HH:MM, которое соответствует сдвигу локального времени для Вашей временной зоны относи-

тельно UTC, → [Enter], на экран выводится окно ввода данных (см. Рисунок 3.119), введите значение сдвига временной зоны;

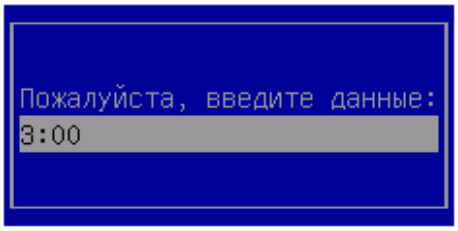

Рисунок 3.119 – Окно ввода значения сдвига локального времени

5) → [Enter], для подтверждения введенных данных;

3.14 Антивирус Касперского для UEFI

Модуль *Антивирус Касперского для UEFI* позволяет проверять файлы, используемые в процессе загрузки компьютера, и обеспечивает защиту от функционирования вредоносного кода до начала работы операционной системы и основного антивируса.

3.14.1 Включение модуля антивируса

Для включения модуля антивируса оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

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

3) выберите в разделе *Настройки модулей безопасности* пункт *Антивирус Касперского для UEFI* со статусом [Выкл];

4) → [Enter] на клавиатуре, на экран выводится страница Антивирус Касперского для UEFI (см. Рисунок 3.120);

Рисунок 3.120 – Пункт *Включить Антивирус Касперского для UEFI*

5) выберите пункт *Включить Антивирус Касперского для UEFI*;

6) → [Enter] на клавиатуре, для включения модуля. На экран выводится страница «Антивирус Касперского для UEFI» с текстом Лицензионного соглашения (см. Рисунок 3.121), прочтите соглашение;

7) выберите пункт *Принять*;

Рисунок 3.121 – Лицензионное соглашение ЗАО «Лаборатория Касперского»

8) → [Enter] на клавиатуре, на экран выводится страница «Антивирус Касперского для UEFI» (см. Рисунок 3.120);

9) → [Esc] на клавиатуре, на экран выводится окно «Настройки» (см. Рисунок 3.17). Статус пункта *Антивирус Касперского для UEFI* изменится с [Выкл] на [Вкл];

3.14.2 Выключение модуля антивируса

Для выключения модуля антивируса оболочки безопасности Kraftway Security Shell необходимо выполнить следующие действия:

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

2) → [Enter] на клавиатуре, на экран выводится страница *Настройки* (см. Рисунок 3.17);

3) выберите в разделе *Настройки модулей безопасности* пункт *Антивирус Касперского для UEFI* со статусом [Вкл];

4) → [Enter] на клавиатуре, на экран выводится страница Антивирус Касперского для UEFI (см. Рисунок 3.120);

5) выберите пункт *Включить Антивирус Касперского для UEFI*;

6) → [Enter] на клавиатуре, для выключения модуля;

7) → [Esc] на клавиатуре, на экран выводится окно «Настройки» (см. Рисунок 3.5). Статус пункта *Антивирус Касперского для UEFI* изменится с [Вкл] на [Выкл];

3.14.3 Настройка модуля антивируса

Для настройки модуля антивируса смотрите документацию на соответствующую версию антивируса.

3.15 Вход в интерфейс настройки UEFI материнской платы

В интерфейс настройки UEFI материнской платы могут входить Администраторы обладающие правом доступа к настройкам UEFI.

3.15.1 Вход в графический интерфейс UEFI при выключенном СДЗ

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

1) включите персональный компьютер, дождитесь вывода на экран приглашения на вход в KSS (см. Рисунок 3.1);

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.

3.15.2 Вход в графический интерфейс UEFI при включённом СДЗ

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

1) включить персональный компьютер;

2) пройти процедуру аутентификации в СДЗ;

3) → [Delete] на клавиатуре при выводе на экран приглашения на вход в KSS (см. Рисунок 3.1), 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 ПЕРЕДАЧА ЗНАЧЕНИЙ ПАРАМЕТРОВ МОДУЛЕЙ KSS С СЕРВЕРА KSC

При правильных сетевых настройках в KSS и регистрации рабочей станции на сервере безопасности KSC, администратору KSC доступна функция передачи значений параметров на KSS.

Список параметров KSS доступных для передачи значений с сервера безопасности KSC приведен в Приложение 1.

5 СООБЩЕНИЯ АДМИНИСТРАТОРУ

Сообщения администратору – это текстовые сообщения (записи), выводимые на страницах или в окнах в процессе работы с KSS B2.2.

Основная часть сообщений, выводимых на экран монитора, представлена в соответствующих разделах данного руководства. В данном разделе приводятся дополнительные сообщения СДЗ, 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 СДЗ приводятся ниже по тексту при описании различного рода ситуаций, с которыми администратор может столкнуться при работе с СДЗ.

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)

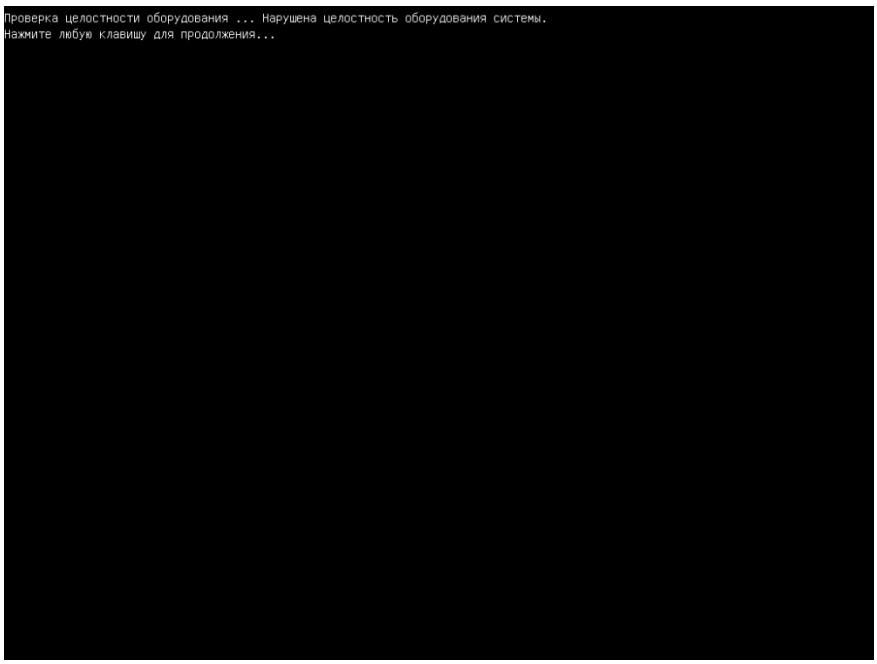

Рисунок 5.1 – Нарушена целостность оборудования системы.

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

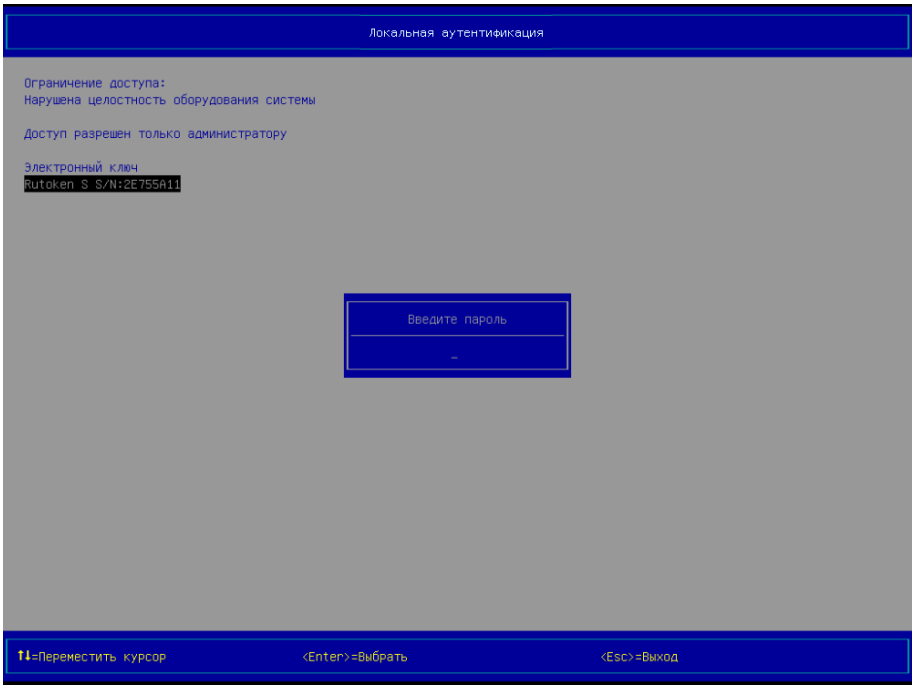

Рисунок 5.2 – Ограничение доступа: Нарушена целостность оборудования системы. Доступ разрешен только администратору.

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

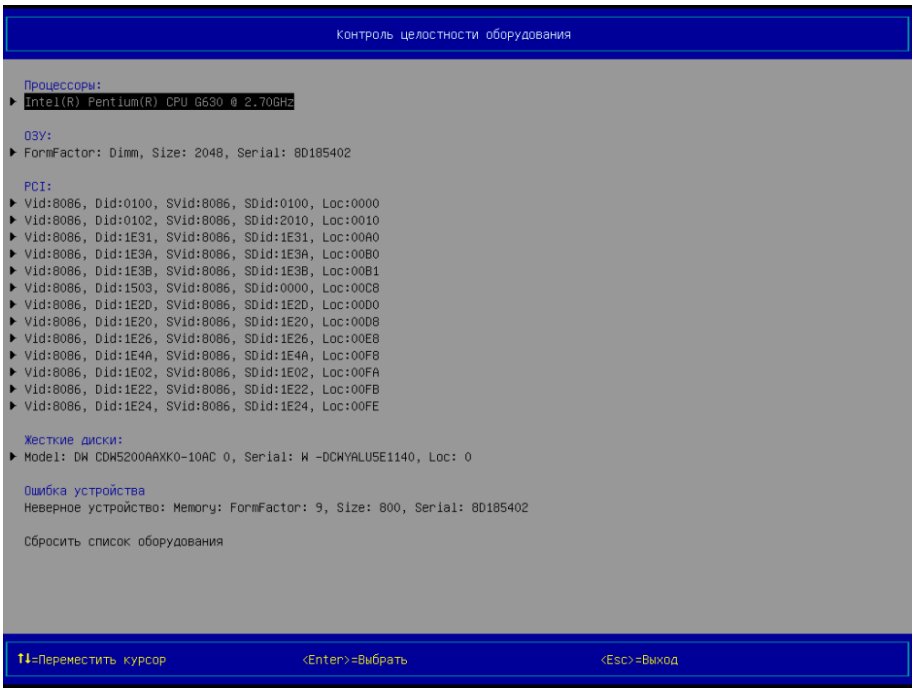

Рисунок 5.3 – Ошибка устройства: Неверное устройств: Memory FormFactor: 9, Size: 800, Serial: 80185402

4. Журнал событий (см. Рисунок 5.4)

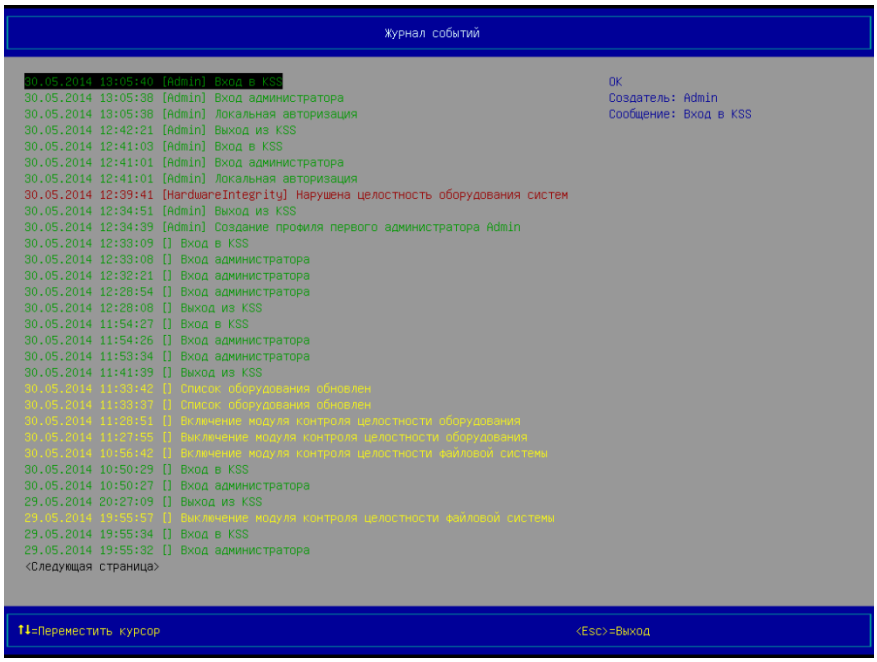

Рисунок 5.4 – Нарушена целостность оборудования системы

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…

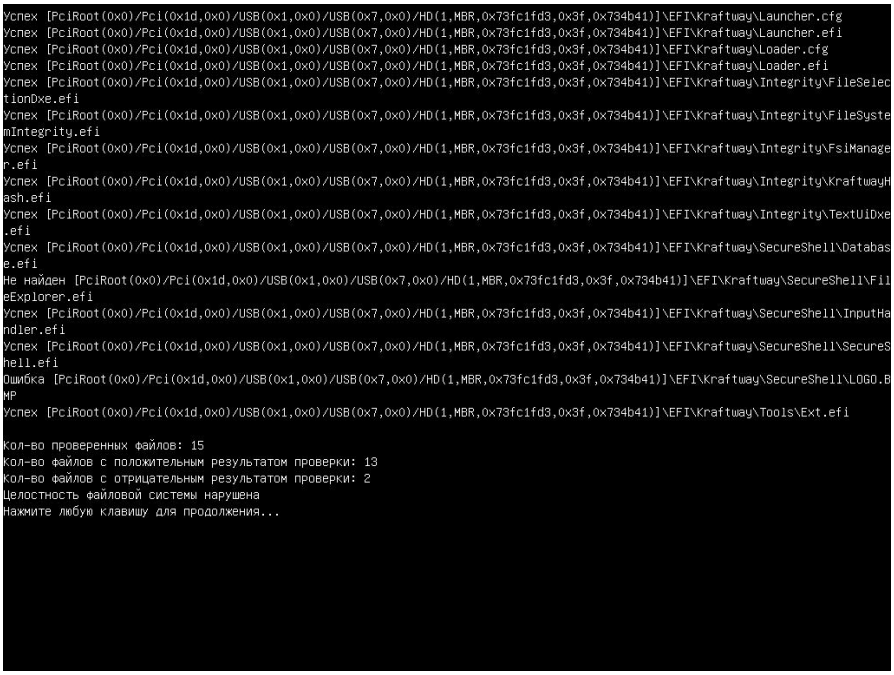

Рисунок 5.5 – Целостность файловой системы нарушена

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 СДЗ и проанализировать данные, хранящиеся в нём, для нахождения причины нарушения целостности файлов.

Ситуация № 2

При отрицательном результате процедуры КЦ, и когда СДЗ 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

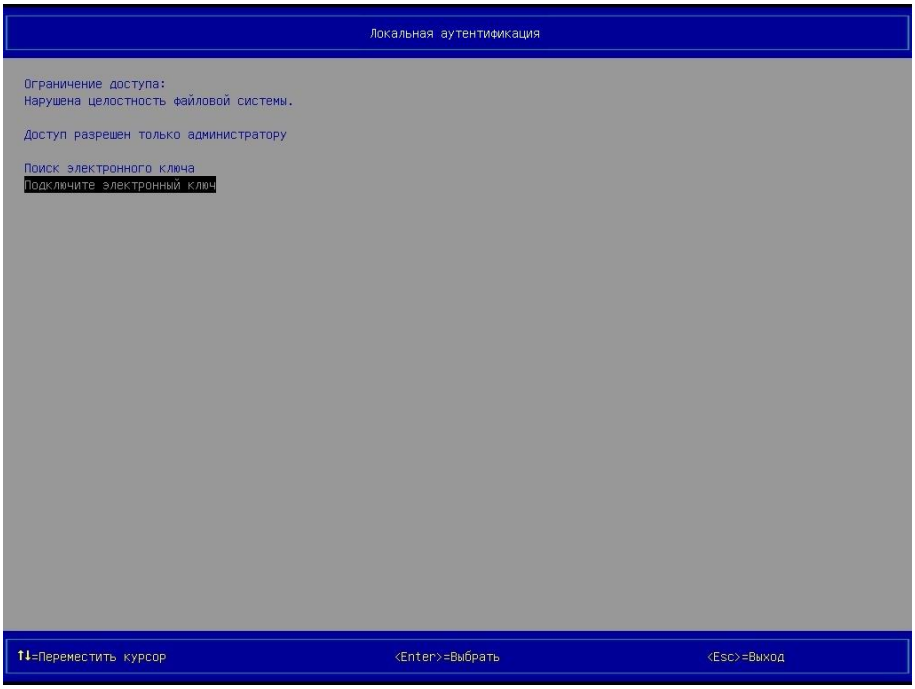

Рисунок 5.6 – Страница *Локальная аутентификация* (вид 5), СДЗ заблокировал компьютер

Решение: при появлении записей такого вида администратору следует: пройти процедуру идентификации, 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.

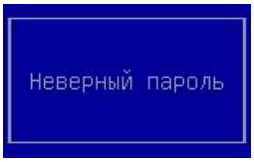

Рисунок 5.7 – Неправильно введён пароль

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 СДЗ.

Ситуация № 4

Если количество неправильно введённого пароля пользователя во время его аутентификации равно значению параметра *Максимальное количество попыток ввода пароля* (см. п.), 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.

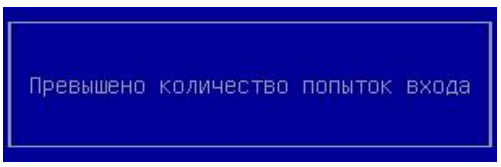

Рисунок 5.8 – Превышено количество попыток
ввода пароля

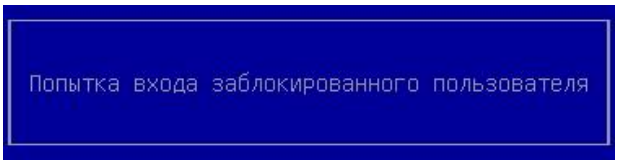

Рисунок 5.9 – Попытка входа заблокированного пользователя

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

Ситуация № 5

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

Решение: администратору следует отключить ИУ пользователя от USB-порта персонального компьютера, профиль которого был заблокирован, пройти процедуру аутентификации в СДЗ с помощью ИУ 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 идентификации было превышено максимальное количество попыток аутентификации, т.е. количество подключений ИУ пользователя к USB-порту персонального компьютера, которое было задано администратором ранее в настройках СДЗ;
- если во время прохождения пользователем процедуры идентификации количество попыток ввода пароля пользователя превысило максимальное количество попыток аутентификации, которое было задано администратором ранее в

настройках СДЗ, 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 идентификации.

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

Ситуация № 7

Если при прохождении процедуры идентификации подключить ИУ пользователя, незарегистрированное в БД СДЗ, 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 идентификации при следующих настройках СДЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Электронный ключ» или «Цифровой сертификат и электронный ключ».

Решения:

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

2. Отключить ИУ пользователя от USB-порта персонального компьютера, которое не было ранее зарегистрировано в СДЗ, подключить ИУ администратора к USB-порту персонального компьютера, пройти процедуру аутентификации, войти в оболочку KSS, создать профиль нового пользователя с применением ИУ, с помощью которого идентификация пользователя ранее была невозможна.

Ситуация № 8

Если во время прохождения процедуры аутентификации пользователем было выбрано значение ключевого поля на странице *Локальная аутентификация*, которое отсутствует в БД СДЗ, 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 СДЗ.

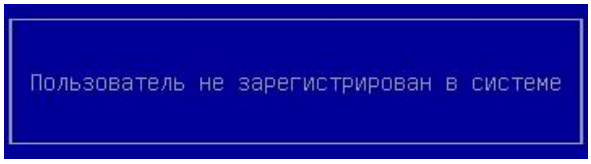

Рисунок 5.11 – Пользователь не зарегистрирован в СДЗ

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

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

Примечание. Т.к. в настройках СДЗ параметру *Способ аутентификации* было присвоено значение «Цифровой сертификат», то перед созданием профиля нового пользователя администратору следует проверить наличие сертификата пользователя в ИУ.

Ситуация № 9

Если во время прохождения процедуры аутентификации не были найдены сертификаты пользователей на ИУ, то на странице *Локальная аутентификация* (см. Рисунок 5.12) выводится запись следующего вида:

Сертификатов не обнаружено

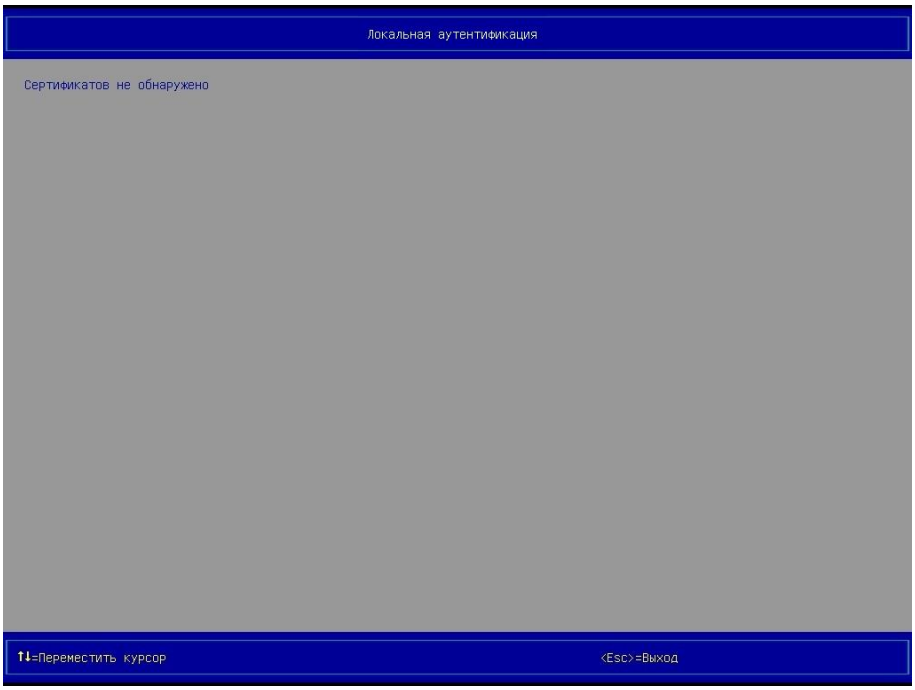

Рисунок 5.12 – Страница *Локальная аутентификация* (вид 6), сертификаты не были найдены на ИУ

Примечание. Запись, представленная на странице *Локальная аутентификация* (см. Рисунок 5.12), может быть выведена тогда, когда пользователь проходит процедуру идентификации при следующих настройках СДЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решение: администратору следует сохранить сертификат пользователя на ИУ.

Ситуация № 10

Если во время прохождения пользователем процедуры идентификации результат проверки сертификата пользователя на подлинность отрицательный, то на экран выводится окно (см. рисунок 5.13), информирующее об ошибке идентификации.

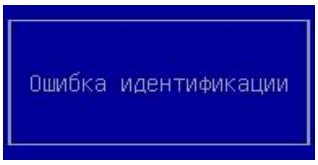

Рисунок 5.13 – Ошибка идентификации

Примечание. Окно (см. рисунок 5.13) выводится на экран только тогда, когда пользователь проходит процедуру идентификации при следующих настройках СДЗ: *Электронный замок "Витязь"* – «Вкл», *Способ аутентификации* – «Цифровой сертификат» или «Цифровой сертификат и электронный ключ».

Решения:

1. Администратору следует сохранить сертификат пользователя на ИУ, который был подписан с помощью сертификата УЦ, добавленного ранее в СДЗ.

2. Администратору следует пройти процедуру идентификации, 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 идентификация в СДЗ невозможна (см. предупреждение п. 0).

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. 0).

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. 3.5.1).

Ситуация № 14

Если при создании профиля нового пользователя с применением его ИУ попытаться создать данный профиль, не подключив ИУ пользователя и нажав на клавишу [Enter] клавиатуры после соответствующего запроса, то в этом случае на экран выводится окно (см. рисунок 5.17), информирующее о том, что ИУ не найден.

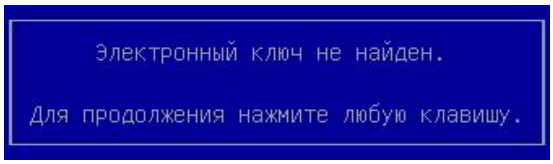

Рисунок 5.17 – ИУ (электронный ключ) не найден

Решение: администратору следует нажать любую клавишу на клавиатуре, после чего повторить процедуру создания профиля нового пользователя, подключить ИУ пользователя при соответствующем запросе, закончить создание профиля нового пользователя.

Ситуация № 15

Если при создании профиля нового пользователя с применением его ИУ поле окна для ввода пароля 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.

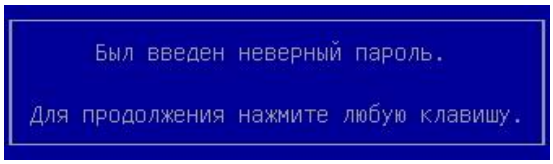

Рисунок 5.18 – Был введён неверный пароль

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 ИУ после вывода на экран окна для ввода пароля пользователя нажать на клавишу [Esc], то на экран будет выведено окно (см. рисунок 5.19), информирующее о том, что операция прервана.

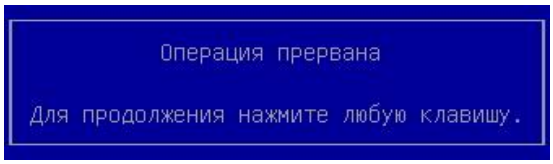

Рисунок 5.19 – Операция прервана

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 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.

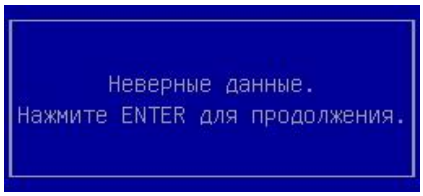

Рисунок 5.20 – Были введены неверные данные

Решение: администратору следует ввести данные в поля окон для ввода данных пользователя.

Ситуация № 18

Если при создании профиля нового пользователя с применением ИУ попытаться создать данный профиль, подключив ИУ, которое ранее использовалось при создании профиля другого пользователя, и нажав на клавишу [Enter] клавиатуры после соответствующего запроса, то в этом случае на экран выводится окно (см. рисунок 5.21), информирующее о том, что ИУ был зарегистрирован ранее в СДЗ.

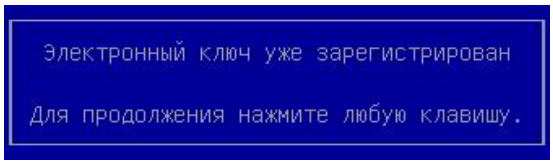

Рисунок 5.21 – ИУ (электронный ключ) уже зарегистрирован

Примечание. Окно (см. рисунок 5.21) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках СДЗ: *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 ИУ, которое было инициализировано (отформатировано) специально для данного пользователя.

Ситуация № 19

Если при создании профиля нового пользователя с применением ИУ попытаться создать данный профиль, подключив ИУ, на котором отсутствует сертификат пользователя,

то после выполнения поиска сертификатов на ИУ на экран выводится окно (см. рисунок 5.22), информирующее о том, что сертификат недоступен.

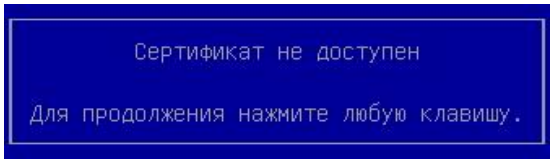

Рисунок 5.22 – Сертификат недоступен

Примечание. Окно (см. рисунок 5.22) выводится на экран только тогда, когда создание профиля нового пользователя выполняется при следующих настройках СДЗ: *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 ИУ, 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 СДЗ, сохранить этот сертификат пользователя на ИУ пользователя, повторить создание профиля нового пользователя с применением данного ИУ.

Ситуация № 20

Если не подключить ИУ пользователя перед сменой его пароля или подключить ИУ 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 ИУ 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 – ИУ не был подключен

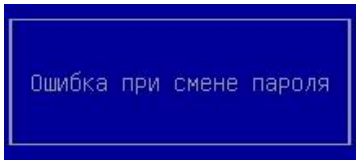

Рисунок 5.24 – Произошла ошибка при смене пароля

Решение: администратору следует нажать на любую клавишу клавиатуры, далее подключить ИУ 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.

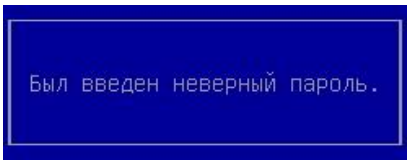

Рисунок 5.25 – Неправильно введён пароль

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.

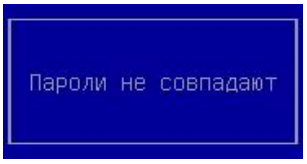

Рисунок 5.26 – Пароли не совпадают

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 3.49) 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 3.49).

Ситуация № 24

Если при добавлении списка файлов, подлежащих КЦ, ввести название списка файлов с использованием специальных символов в соответствующем окне (см. рисунок 3.49) 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.

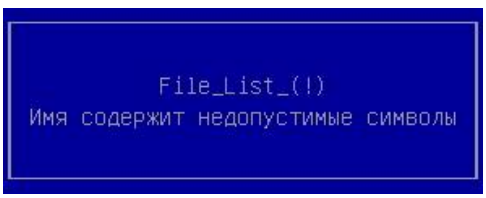

Рисунок 5.27 – Название списка файлов содержит недопустимые символы

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 3.49) 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.

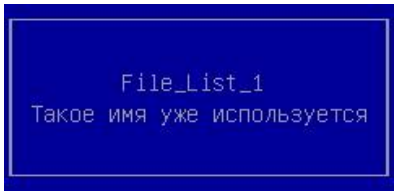

Рисунок 5.28 – Название списка файлов уже присвоено добавленному списку

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 СДЗ.

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.

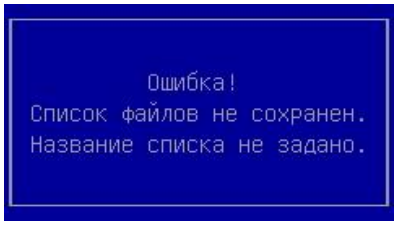

Рисунок 5.29 – Требуется задать название списку файлов

Решение: для сохранения списка файлов, подлежащих КЦ, администратору следует присвоить название добавляемому списку файлов.

Ситуация № 27

Если во время добавления сертификата УЦ в СДЗ на странице *Файловый менеджер* (см. п. 0) отменить данную операцию, то на экран будет выведено окно (см. рисунок 5.30), информирующее о том, что не удалось импортировать сертификат УЦ.

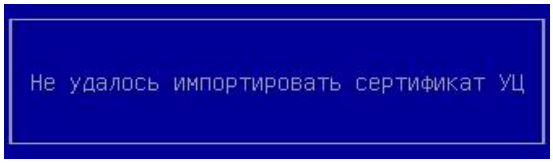

Рисунок 5.30 – Ошибка добавления сертификата УЦ

Ситуация № 28

При попытке добавления сертификата УЦ, который ранее был добавлен в СДЗ, на экран выводится окно (см. рисунок 5.31), информирующее о наличии данного сертификата УЦ в СДЗ.

Рисунок 5.31 – Добавляемый сертификат УЦ был добавлен в СДЗ ранее

Решение: администратору следует добавить другой сертификат УЦ при необходимости.

Ситуация № 29

Если во время добавления сертификата компьютера в СДЗ на странице *Файловый менеджер* отменить данную операцию, то на экран будет выведено окно (см. рисунок 5.32), информирующее о том, что не удалось импортировать сертификат компьютера.

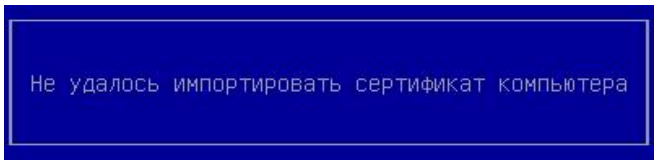

Рисунок 5.32 – Ошибка добавления сертификата компьютера

Ситуация № 30

Если во время добавления сертификата компьютера в СДЗ на странице *Файловый менеджер*, а именно после вывода окна, 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 СДЗ на странице *Файловый менеджер* ввести неправильно пароль для сертификата компьютера в соответствующем окне, 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.

6 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

При возникновении различных проблем, связанных с работой KSS B2.2, а также для получения консультации, администратор может обратиться в Единый центр поддержки пользователей компании Kraftway. Перед обращением в Единый центр поддержки пользователей системному администратору предлагается подготовить следующую информацию:

– версию KSS;

– аппаратные характеристики персонального компьютера;

– журнал событий;

– подробное описание неисправностей или ошибок;

– «скриншоты» ошибок KSS;

Консультацию Единого центра поддержки пользователей компании Kraftway можно получить:

1) по телефонам (круглосуточно):

– тел. №1: 8 (495) 969-24-04 – для Москвы;

– тел. №2: 8 (800) 200-03-55 – для регионов;

2) через веб-форму (круглосуточно):

– www.kraftway.ru/support/techsupport/ask/.

7 ПРИЛОЖЕНИЕ 1

СПИСОК ПАРАМТРОВ МОДУЛЕЙ, ПЕРЕДАВАЕМЫХ ЧЕРЕЗ СЕТЕВУЮ КОМПОНЕНТУ KSS С СЕРВЕРА БЕЗОПАСНОСТИ KSC

1. *Оболочка безопасности KSS*
   – запрет загрузки с внешних устройств
   – таймаут для входа в KSS
   – инвентарный номер ПК

2. Модуль *Электронный замок*
   – включение/выключение модуля;
   – максимальное количество попыток идентификации;
   – минимальная длинна пароля;
   – таймаут на ввод пароля;

3. Модуль *Управление сертификатами*
   – включение/выключение модуля.

4. Модуль *Контроль целостности файловой системы*
   – включение/выключение модуля;
   – используемая хеш-функция;
   – контрольные списки файлов.

5. Модуль *Контроль целостности оборудования*
   – включение/выключение модуля;
   – включение/выключение проверки целостности системного блока;
   – сброс состояния контроля вскрытия корпуса.

6. Модуль *Логические диски*
   – включение/выключение модуля.

7. Модуль *Журнал событий*

– включение/выключение модуля;

– очистка журнала событий;

– экспорт журнала событий.

8. Модуль *Управление обновлениями*

– включение/выключение модуля;

– установка запрета/разрешения на автоматическое обновление рабочей станции);

– установка максимального количества попыток обновления рабочей станции).

9. Модуль *Сетевой клиент безопасности*

– включение/выключение модуля;

– установка/выбор сетевого интерфейса из раскрывающегося списка;

– присвоение сетевого имени рабочей станции;

– ввода IP-адреса или URI сервера безопасности;

– установка запрета/разрешения на автоматическое получение IP-адреса по DHCP;

– установка запрета/разрешения на использование протокола SSL при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на проверку сертификата сервера безопасности при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на проверку имени сервера при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на проверку даты сертификата;

– установка запрета/разрешения на использование сертификата компьютера при обращении рабочей станции к серверу безопасности. Выбирать данный параметр следует только после добавления сертификата компьютера на рабочую станцию;

– установка запрета/разрешения на синхронизацию журнала событий при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на обновление модулей безопасности при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на сетевую аутентификацию пользователей;

– установка запрета/разрешения на инвентаризацию модулей безопасности при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на инвентаризацию оборудования при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на выполнение контроля целостности файлов при обращении рабочей станции к серверу безопасности;

– установка запрета/разрешения на выполнение синхронизации настроек с сервером безопасности при обращении рабочей станции к серверу безопасности;

10. Модуль *Синхронизация времени*

– включение/выключение модуля.