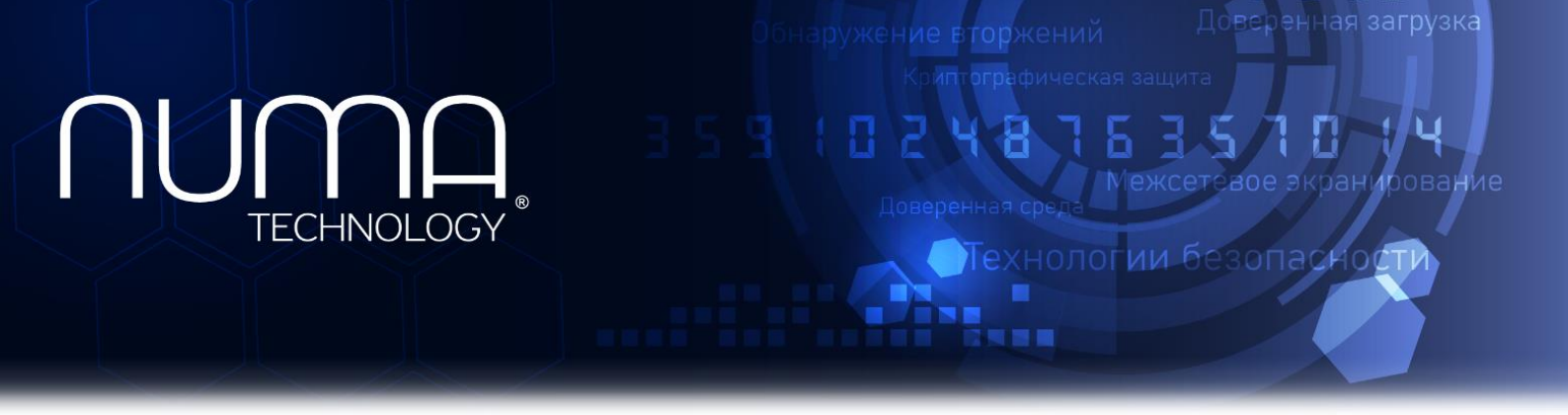

Средство доверенной загрузки уровня базовой системы ввода-вывода
Модуль доверенной загрузки Numa Arce
Руководство администратора
643.АМБН.00032-01 32 01
Листов 92

2022

Литера

АННОТАЦИЯ

Данное руководство предназначено для администраторов Изделия модуль доверенной загрузки Numa Arce 643.АМБН.00032-01 (далее – Изделие или Numa Arce).

Руководство содержит основные сведения, необходимые для установки, настройки, эксплуатации Изделия.

Условия применения Изделия, а также условия обеспечения безопасности информации и соответствия предъявляемым требованиям приведены в разделах 2 и 3 документа «Модуль доверенной загрузки Numa Arce Правила применения» 643.АМБН.00032-01 ПП (далее – Правила).

Перед началом работы с Изделием администратор должен ознакомиться с настоящим руководством, а также с Правилами.

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство администратора
Версия документа	1.0
Обозначение документа	643.АМБН.00032-01 32 01
Утвержден	643.АМБН.00032-01 32 01–ЛУ
Тип Изделия	Средство доверенной загрузки уровня базовой системы ввода-вывода
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Децимальный номер Изделия	643.АМБН.00032-01
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	СДЗ, средство доверенной загрузки уровня базовой системы ввода-вывода

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

Изделие предназначено для выполнения доверенной загрузки, заключающейся в осуществлении запуска с доверенных и предопределенных заранее носителей только проверенного набора данных, проверки аппаратных ресурсов, идентификации и аутентификации пользователей, разграничения доступа на основе ролей, а также организации доверенной загрузки ОС после процедуры контроля целостности загружаемой среды.

Целевые функций Изделия по доверенной загрузке ОС, для которых в установленном порядке подтверждено соответствие требованиям ФСБ России, приведены в Правилах.

1.2. Функциональные возможности Изделия

Полный перечень функциональных возможностей, реализацию которых обеспечивает Изделие, включает:

1) аутентификацию пользователей и администраторов Изделия:

– возможность локальной однозначной идентификации и аутентификации пользователей, администраторов Изделия;

– возможность регистрации не менее 5 равноправных администраторов;

– возможность регистрации не более 20 пользователей (в том числе не менее 5 администраторов);

– возможность аутентификации пользователя с помощью одного АНП на разных ЭВМ с установленным Изделием;

– возможность доступа к механизмам управления Изделием, а также к настройкам параметров работы Изделия только администратору изделия, который успешно прошел процедуру идентификации и аутентификации.

2) контроль целостности собственных программных компонентов и данных, а также компонентов ПО БСВВ и идентификационной информации компонентов аппаратного обеспечения ЭВМ:

– Изделие обеспечивает возможность контроля целостности следующих объектов:

– областей загрузочных секторов, расположенных на доступных через функции ПО БСВВ физических и логических дисках ЭВМ;

– файлов, расположенных на доступных через функции ПО БСВВ логических дисках ЭВМ и использующих файловые системы Ext2, Ext3, Ext4, FAT16, FAT32 и NTFS, а также неизменность списка файлов в выбранных директориях;

– журналов транзакций файловых систем Ext3, Ext4 и NTFS;

– разделов и элементов системного реестра ОС Windows;

– программного обеспечения региона ME и GbE соответствующей микросхемы SPI flash-памяти на системной плате ЭВМ;

– идентификационной информации аппаратного обеспечения, определяющей состав аппаратных средств ЭВМ при первоначальном запуске.

3) самотестирование:

– возможность самотестирования технических средств Изделия и ЭВМ, а также контроля целостности собственных программных компонент и данных, компонент БСВВ Numa BIOS до начала загрузки ОС;

– возможность блокирования доступа к ресурсам ЭВМ всех пользователей за исключением администратора Изделия в случае невыполнения самотестирования или ошибки хотя бы в одном тесте.

4) блокирование загрузки пользователем нештатной (недопущенной к эксплуатации установленным порядком) операционной системы;

5) возможность регистрации, сбора, записи, хранения, экспорта информации о событиях безопасности, в том числе:

– Изделие обеспечивает наличие системного журнала событий, разделенного на два независимых раздела: «Общий журнал», а также «Журнал безопасности», в который заносится информация об ошибках, обнаруженных при контроле целостности;

– Изделие обеспечивает максимальную емкость раздела «Общий журнал» 500 записей;

– Изделие обеспечивает максимальную емкость раздела «Журнал безопасности» 3000 записей;

– возможность полной очистки системного журнала событий Изделия (целиком или его отдельной области) и экспорт его на внешний носитель до выполнения очистки системного журнала.

6) Изделие обеспечивает возможность вывода регистрационного номера СКЗИ, используемого в АПН, и отображения его в специальном информационном окне меню Изделия;

7) Изделие обеспечивает возможность полной переинициализации Изделия из специального технологического режима, при котором осуществляется:

– гарантированное стирание служебных структур данных, хранящихся в памяти Изделия;

– создание (инициализация) служебных структур данных;

– формирование контрольных сумм служебных структур данных.

8) Изделие обеспечивает возможность генерации паролей пользователя с использованием датчика случайных чисел (ДСЧ), входящем в состав АНП, с применением случайной равномерной выборки символов алфавита;

9) Изделие обеспечивает возможность передачи блока параметров аутентифицированного пользователя внешнему (по отношению к Изделию) программному обеспечению средств защиты информации (требуется поддержка данной функции со стороны средства защиты информации);

10) Изделие обеспечивает возможность локального выполнения следующих действий для администраторов Изделия:

– просмотр и модификация списка зарегистрированных пользователей;

– блокирование и разблокирование зарегистрированных пользователей;

– просмотр и модификация конфигурационных параметров Изделия;

– задание уровня критичности событий, фиксируемых в журнале регистрации событий;

– просмотр, очистку и экспорт на внешний носитель журнала регистрации событий;

– формирование, просмотр, модификацию списка объектов контроля целостности программной среды;

– возможность настройки, просмотра, модификации контроля состава аппаратных компонент СВТ;

– просмотр, настройка установленных EFI-драйверов устройств;

– просмотр, настройка возможности защиты EFI-переменных;

– внесение, удаление, просмотр сертификатов, используемых для аутентификации пользователей;

– пересчет эталонных значений для объектов контроля целостности;

– просмотр, модификация, индивидуальных настроек (профилей) пользователей и администраторов;

– установка системного времени и даты;

– запрос, загрузка файла лицензии;

– обновление Изделия (использование данной функции ограничено Правилами);

– просмотр версии Изделия.

1.3. Роли пользователей, поддерживаемые Изделием

Изделие поддерживает три роли пользователей:

Администратор – пользователь, наделенный полными правами и привилегиями по настройке (администрированию) Изделием.

Пользователь – пользователь, наделенный правами по загрузке уже сконфигурированной полезной нагрузки (операционной системы).

Аудитор – администратор, наделенный правами исключительно по просмотру контроля целостности Изделия, файлов, поставленных на контроль администратором, а также имеющий возможность просмотр и выгрузку на USB-носитель журнала аудита.

1.4. Режимы функционирования

1.4.1. Штатный режим работы

Переход в штатный режим работы осуществляется автоматически после подачи питания на СВТ и прохождения всех процедур контроля целостности успешно.

В штатном режиме работы предусмотрена только загрузка ОС и не предусмотрено выполнение никаких административных функций.

Для загрузки специальных профилей загрузки, настроенных администратором с параметром «Требовать авторизацию», необходимо пройти успешно процедуру идентификации и аутентификации.

1.4.2. Режим администрирования

Режим администрирования предназначен для выполнения следующих функций:

- формирование, импорт, экспорт, модификация профиля загрузки;
- просмотр и модификация списка зарегистрированных пользователей;
- блокирование и разблокирование зарегистрированных пользователей;
- импорт, экспорт профилей пользователей;
- просмотр и модификация конфигурационных параметров Изделия, в том числе:
    - установка счетчика аутентификаций и счетчика попыток входа;
    - минимально допустимой длины вводимого пароля;
    - использование сложного пароля;
    - период действия паролей пользователей;
    - задание уровня критичности событий, фиксируемых в журнале регистрации событий;
- просмотр, очистку и экспорт на внешний носитель журнала регистрации событий (разделы общий журнал, журнал безопасности);
- формирование, просмотр, модификацию списка объектов контроля целостности программной среды;
- возможность настройки, просмотра, модификации контроля состава аппаратных компонент СВТ;
- просмотр, настройка установленных EFI-драйверов устройств;
- просмотр, настройка возможности защиты EFI-переменных;
- внесение, удаление, просмотр сертификатов, используемых для аутентификации пользователей;
- пересчет эталонных значений для объектов контроля целостности;
- установка системного времени и даты;
- запрос, загрузка файла лицензии;
- обновление Изделия;
- просмотр версии Изделия и БСВВ.

Переход в режим администрирования осуществляется выбором пункта меню «Панель управления», доступном в главном меню после успешной процедуры прохождения идентификации и аутентификации администратором.

Работа в режиме администрирования возможна до заполнения журнала событий. Затем записи журнала аудита должны быть выгружены на внешний носитель и очищены администратором Изделия, после чего станет возможен доступ к полным административным функциям Numa Arce и загрузка ОС, при условии, что выключена функция перезаписи журнала аудита.

При выходе из режима администрирования системы будет выполнено сохранение настроек и последующая перезагрузка комплекса или загрузка ОС.

1.4.3. Режим работы аудитора

Данный режим работы предназначен для пользователей с ролью Администратор с правами аудитора (далее – аудитор). После авторизации аудитора на экране Изделия появляется меню, которое состоит из профилей загрузки и пункта «Панель управления». В данном режиме аудитору доступно две функции:

– проверка целостности Изделия, файлов и объектов, поставленных на контроль администратором Изделия (см. пункт 4.6.5);

– действия с журналом аудита: просмотр, выгрузка, (см. пункт 4.6.3).

1.4.4. Аварийный режим работы

1) При нарушении контроля целостности Изделия (Numa_Arce.efi) осуществляется переход в аварийный режим работы, в котором дальнейшая эксплуатация СВТ невозможна без переустановки Изделия, при этом переход Изделия в аварийный режим сопровождается сообщением об ошибке и блокировкой загрузки СВТ;

2) при нарушении контроля целостности компонентов ПО БСВВ Numa BIOS Изделие переходит в аварийный режим работы, в котором дальнейшая эксплуатация СВТ невозможна без переустановки Изделия, при этом переход Изделия в аварийный режим сопровождается сообщением об ошибке и блокировкой загрузки СВТ;

3) при нарушении контроля целостности областей загрузочных секторов, расположенных на доступных через функции ПО БСВВ физических и логических дисках, Изделие блокирует дальнейшую работу СВТ, при этом:

– блокировка СВТ сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке (при наличии технической возможности), записью в журнал аудита о нарушении контроля целостности;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем перерасчета контрольной суммы ПО СВТ, нарушившего контроль целостности.

4) при нарушении контроля целостности файлов, расположенных на доступных через функции ПО БСВВ логических дисках и использующих файловые системы Ext2, Ext3, Ext4, FAT16, FAT32 и NTFS, а также неизменности списка файлов в выбранной директории Изделие блокирует дальнейшую работу СВТ, при этом:

– блокировка СВТ сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке (при наличии технической возможности), записью в журнал аудита о нарушении контроля целостности;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем перерасчета контрольной суммы файла, нарушившего контроль целостности.

5) при наличии незавершенных транзакций, модифицирующих взятые на контроль целостности файлы в журнале транзакций файловых систем Ext3, Ext4, Изделие блокирует дальнейшую работу СВТ, при этом:

– блокировка СВТ сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке (при наличии технической возможности), записью в журнал аудита о нарушении контроля целостности;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем перерасчета контрольной суммы ПО СВТ, нарушившего контроль целостности.

6) при наличии незавершенных транзакций в журнале транзакций файловой системы NTFS Изделие блокирует дальнейшую работу СВТ, либо отображает предупреждающее сообщение, в зависимости от настроенной политики, при этом:

– блокировка СВТ сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке (при наличии технической возможности), записью в журнал аудита о наличии незавершенных транзакций;

– предупреждающее сообщение сопровождается записью в журнал аудита о наличии незавершенных транзакций;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором.

7) при нарушении контроля целостности разделов и элементов системного реестра ОС Windows Изделие блокирует дальнейшую работу СВТ, при этом:

– блокировка СВТ сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке (при наличии технической возможности), записью в журнал аудита о нарушении контроля целостности;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем перерасчета контрольной суммы ПО СВТ, нарушившего контроль целостности.

8) при нарушении контроля целостности ПО регионов ME/GbE Изделие блокирует загрузку полезной нагрузки, при этом:

– блокировка загрузки сопровождается сообщением об ошибке, записью в журнале аудита;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем перерасчета контрольной суммы региона ME в меню администрирования Изделия.

9) при нарушении состава, контролируемого Изделием аппаратного обеспечения, Изделие блокирует загрузку полезной нагрузки, при этом:

– блокировка загрузки сопровождается выдачей сообщения об ошибке, звуковым сигналом об ошибке, записью в журнал аудита о нарушении контроля целостности;

– дальнейшая эксплуатация СВТ требует снятия блокировки Изделия администратором путем возвращения аппаратной конфигурации СВТ к первоначальной конфигурации или фиксации изменений в настройках Изделия.

1.4.5. Режим начальной инициализации

Режим инициализации доступен только при первом запуске Изделия или полной переустановки Изделия до заводских настроек. В данном режиме отсутствуют учетные данные пользователей. В данном режиме возможно создание профиля администратора Изделия, а также формирование запроса лицензии и загрузка самой лицензии, необходимой для дальнейшей работы с Изделием.

1.4.6. Технологический режим

Данный режим обеспечивает полную переинциализацию Изделия, в результате которой Изделие переходит к заводским настройкам и запускается в режиме начальной инициализации. Все данные, хранящиеся в памяти Изделия, служебные структуры, гарантированно стираются.

Переход в технологический режим обеспечивается только путем физического доступа к плате СВТ, на которое установлено Изделие. Для перехода в технологический режим необходимо отключить питание СВТ, извлечь батарею RTC не менее чем на 1 минуту (или переключите джампер типа «CLR CMOS» в положение «3-4» на несколько секунд). После подачи питания при

загрузке отображается информационное окно входа в технологический режима (см. рисунок 1) с предложением переинициализации Изделия.

Если батарея RTC разряжена на экран будет выведено предложение перейти в технологический режим, для продолжения штатной работы необходимо отказаться от перехода, установить текущее значение времени из раздела меню.

В случае замены батарейки RTC необходимо заменить ее, не отключая внешнего питания СВТ.

Рисунок 1 – Информационное окно технологического режима

1.5. Технические требования

В зависимости от исполнения Изделия, Изделие функционирует на следующих СВТ (см. таблицу 1).

Таблица 1 – Характеристики СВТ, на которых функционирует Изделие

Исполнение Изделия	Характеристика СВТ
Исполнение 1	Сетевая платформа Lanner NCA-1010
	Сетевая платформа Lanner FW-7573
Исполнение 2	Сетевая платформа Lanner NCA-4210
Исполнение 3	Сетевая платформа Lanner NCA-5520
Исполнение 4	Платформа Aquarius на базе материнской платы AQC300DC
	СВТ Aquarius Cmp NS585
Исполнение 5	СВТ Aquarius Cmp NS685U
	Платформа Aquarius на базе материнской платы AQH310CM
	СВТ Aquarius Cmp NS483

Исполнение Изделия	Характеристика СВТ
	СВТ Aquarius Cmp NS483R
Исполнение 6	Платформа Aquarius на базе материнской платы AQC246DF
Исполнение 7	Платформа Aquarius на базе материнской платы AQC612BJ
Исполнение 8	СВТ Aquarius Cmp NS685 исполнение 2
	СВТ Aquarius Cmp NS685 исполнение 3
	Платформа Aquarius на базе материнской платы AQ H410T
	СВТ Aquarius Cmp NS585 исполнение 2
Исполнение 9	Платформа Aquarius на базе материнской платы AQB560M
Исполнение 10	Платформа Aquarius на базе материнской платы AQC624CF

Типы применяемых аутентифицирующих носителей персональных (АНП):

– аутентифицирующий носитель пользователей (АНП) – СКЗИ «ESMART Token ГОСТ» в исполнении 3.

Список совместимых токенов, рекомендуемых к использованию в Изделии, приведен в Приложении 5.

Работа с СКЗИ должна осуществляться в соответствии с эксплуатационной документацией на СКЗИ.

Поддерживаемые операционные системы (ОС): Microsoft Windows XP, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10, операционные системы на основе ядра Linux, FreeBSD. Контроль целостности полностью реализован в программном модуле Изделия. Установки в ОС дополнительного ПО для обеспечения контроля целостности не требуется.

Поддерживаемые файловые системы: FAT16, FAT32, NTFS, EXT2, EXT3, EXT4.

1.6. Дополнительные требования

Изделие может функционировать только в среде базовой системы-ввода-вывода Numa BIOS 643.АМБН.00001-01 производства ООО «НумаТех».

Для обновления Изделия требуется USB-носитель с файловой системой FAT32.

Изделие поставляется в виде файла-прошивки, предназначенного для дальнейшего тиражирования и установки на СВТ.

1.7. Требования безопасности

Должен быть обеспечен контроль целостности СВТ, на который установлено Изделие, а также контроль конфигурации аппаратного обеспечения СВТ.

При первоначальной настройке Изделия необходимо изменить заводские установки паролей на доступ к функциям администрирования Изделия.

Необходимо сохранение в секрете паролей (PIN-кодов) администратора Изделия.

Изделие должно использоваться строго в соответствии с положениями, приведенными в данном руководстве и Правилами.

Запрещается модифицировать, реконструировать или видоизменять Изделие.

Конфигурирование и управление Изделием должны производиться только администратором в соответствии с данным руководством и Правилами.

2. ОПИСАНИЕ ПРОЦЕДУР ПРОВЕРКИ ЦЕЛОСТНОСТИ

2.1. Контроль целостности в штатном режиме автоматически

После включения питания на СВТ автоматически осуществляется контроль целостности следующих компонент:

– целостности модулей Numa BIOS с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256;

– целостности ПО Numa Arce (Numa_Arce.efi) с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256;

– целостности загрузочных секторов, расположенных на доступных через функции ПО БСВВ физический и логических дисках с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256;

– целостности файлов, расположенных на доступных через функции ПО БСВВ логических дисках и использующих файловые системы с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256;

– целостности загружаемых на исполнение объектов с вычислением контрольной суммы по ГОСТ Р 34.11-2012-256;

– целостности разделов и элементов системного реестра ОС Windows по ГОСТ 34.11-2012-256;

– целостности программного обеспечения региона ME и GbE соответствующей микросхемы SPI flash-памяти на системной плате СВТ;

– целостности журналов транзакций файловых систем EXT3/EXT4/NTFS;

– контроль несанкционированного изменения аппаратной конфигурации.

В случае нарушения контроля целостности хотя бы одного элемента Изделие переходит в аварийный режим (см. пункт 1.4.4).

2.2. Проверка целостности Изделия через пункт меню

Функция проверки целостности вручную с использованием пункта меню предназначена для запуска принудительного контроля целостности бинарного образа Изделия, загружаемых компонент операционной среды, данных, поставленный на контроль, конфигурационных параметров.

Для запуска проверки необходимо выполнить следующие действия:

– авторизоваться под учётной записью административного пользователя;

– зайти в режим «Панель управления»;

– выбрать пункт основного меню «Проверка целостности».

На экран будет выведено сообщение с результатами проверки всех компонентов (см. рисунок 2).

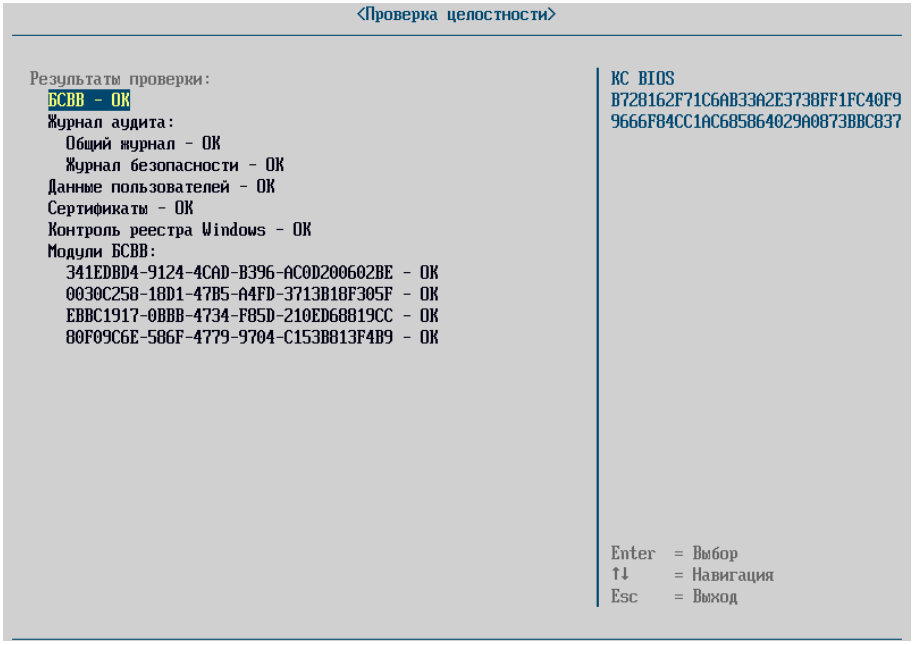

Рисунок 2 – Результат контроля целостности через пункт меню

При наведении клавишами «↓» и «↑» на одну из строк с объектами контроля целостности в правой части окна синим шрифтом выводится хеш-сумма этого объекта.

3. НАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

3.1. Установка Изделия

Установка Изделия на СВТ должна осуществляться согласно документу «Инструкция по установке Изделия на СВТ» 643.АМБН.00032-01 95 01 при производстве СВТ. При невозможности выполнения данной процедуры на производстве, допускается установка Изделия квалифицированным персоналом на месте эксплуатации. При этом доступ потенциального нарушителя к аппаратному и программному обеспечению должен быть исключен.

3.2. Запуск Изделия

Запуск и загрузка Изделия осуществляется автоматически после подачи электропитания на материнскую плату СВТ.

Во время загрузки Изделия в консоль выводится логотип ООО «НумаТех» и шкала хода загрузки.

3.3. Первичная настройка

При первом включении Изделия активируется режим начальной инициализации.

При отсутствии введенной лицензии на экране будет отображена соответствующая ошибка (см. рисунок 3), которую можно игнорировать.

Для продолжения работы необходимо нажать любую клавишу, после чего Изделие запросит статический пароль для продолжения настройки. Ввести в форму пароль «capitolium» и нажать клавишу «Enter» после чего отобразится меню «Подготовка к работе» (см. рисунок 4).

Данная форма позволяет:

– создать администратора для дальнейшей настройки Изделия;

– загрузить с USB – загрузить карточки пользователей с USB-носителя в формате JSON (экспорт учетных записей пользователей описан в разделе 4.6.1.3);

– дата и время – установить дату и время;

– сертификаты – загрузить корневой сертификат и клиентский сертификат TLS.

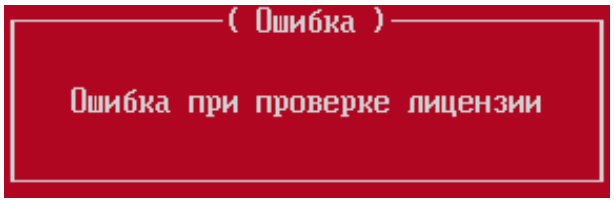

Рисунок 3 – Ошибка ввода лицензии при первом включении Изделия

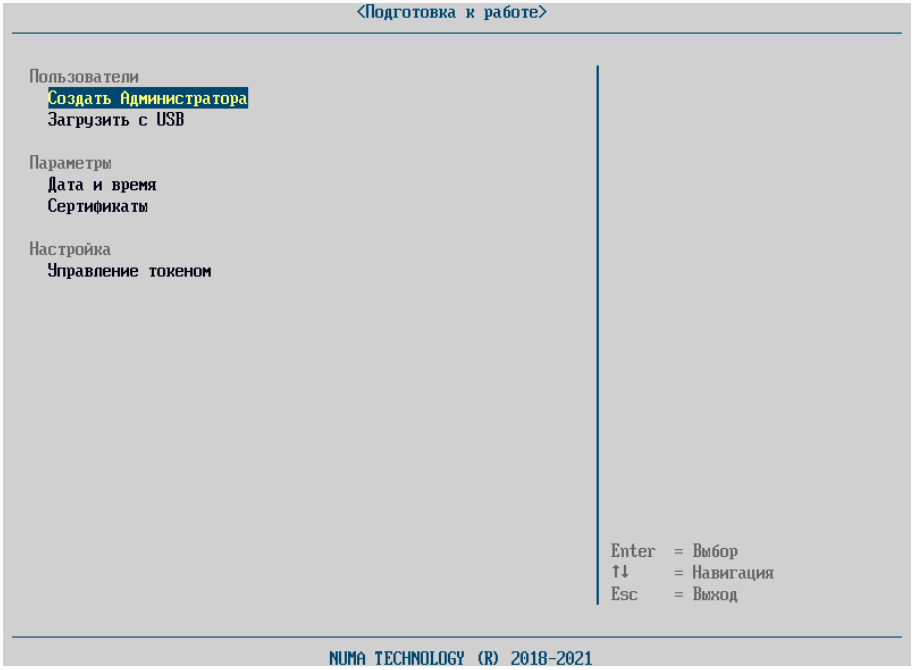

Рисунок 4 – Форма меню «Подготовка к работе»

Для дальнейшей работы необходимо:

1) подключить проинициализированный токен в СВТ;

Примечание. Для работы с АНП в Изделии необходимо, чтобы на АНП были сформированы ключевая пара, а также пользовательский сертификат. Пользовательский сертификат должен быть подписан удостоверяющим центром (далее – УЦ). Для работы с токеном в Изделии, необходимо добавить в хранилище сертификатов сертификат УЦ, которым был подписан пользовательский сертификат.

2) перейти в пункт меню «Управление токеном» и импортировать корневой сертификат из токена (см. рисунок 5);

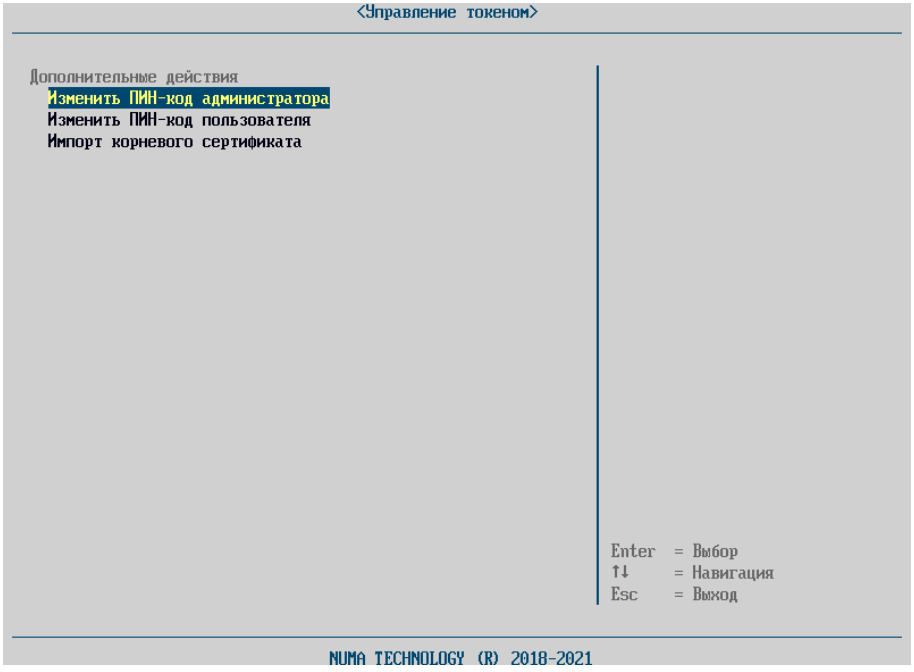

Рисунок 5 – Меню «Управление токеном»

3) в меню «Создать Администратора» ввести данные для создания административного пользователя, указав в качестве данных сопоставления пользовательский сертификат токена (см. рисунок 6). Подробно процедура создания пользователя описана в пункте 4.6.1.1;

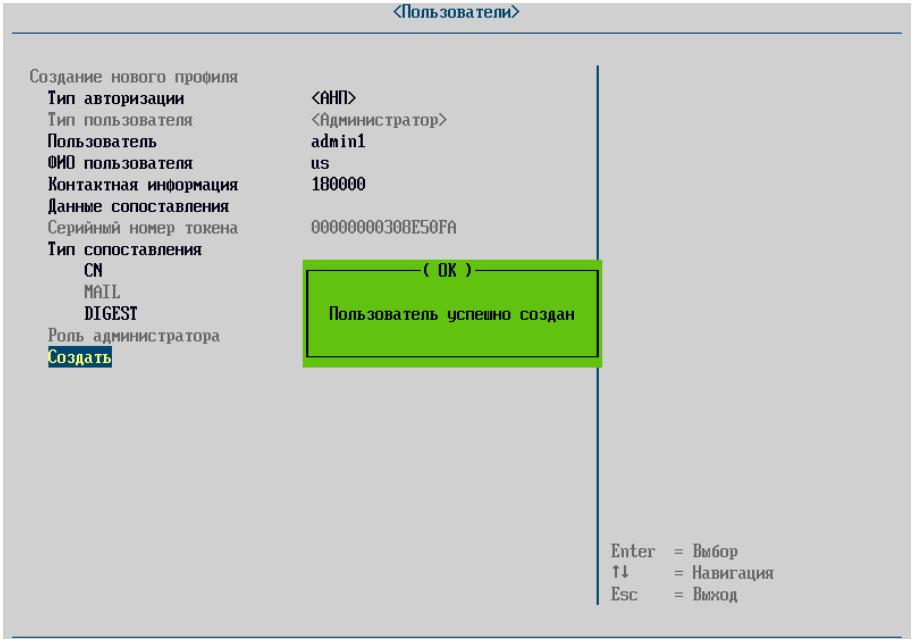

Рисунок 6 – Создание административного пользователя

4) после процедуры создания администратора Изделие в автоматическом режиме перезагрузится, после ввода PIN-кода пользователя, отобразится меню «Ручной режим запроса лицензии» (см. рисунок 7);

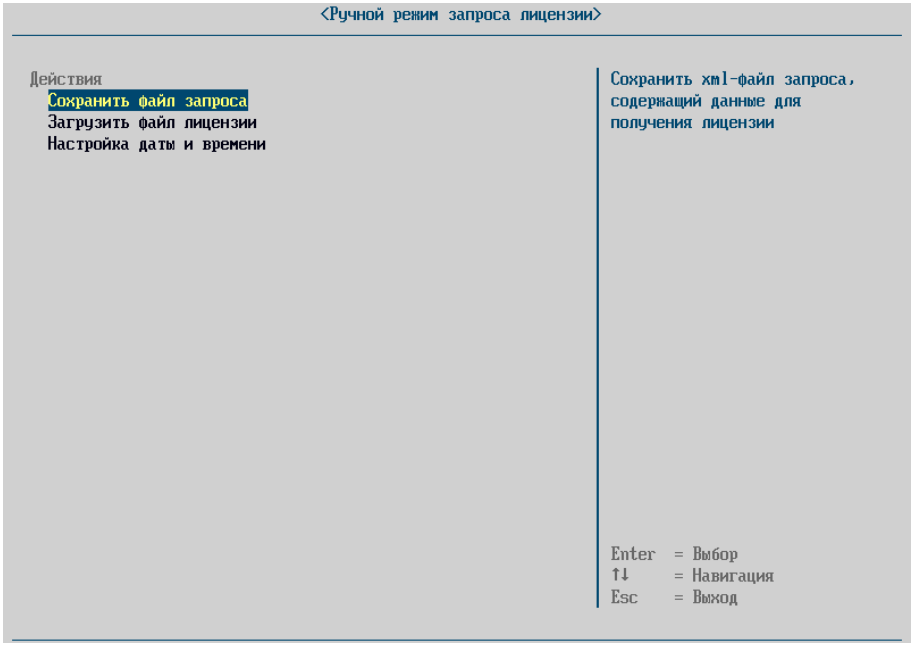

Рисунок 7 – Меню ручного режима запроса лицензии

5) для создания файла запроса для получения лицензии в меню необходимо выбрать пункт «Сохранить файл запроса». Необходимые данные будут сохранены на предварительно подключенный к СВТ USB-носитель в файл с именем «numa_license_req_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.xml» (см. рисунок 8);

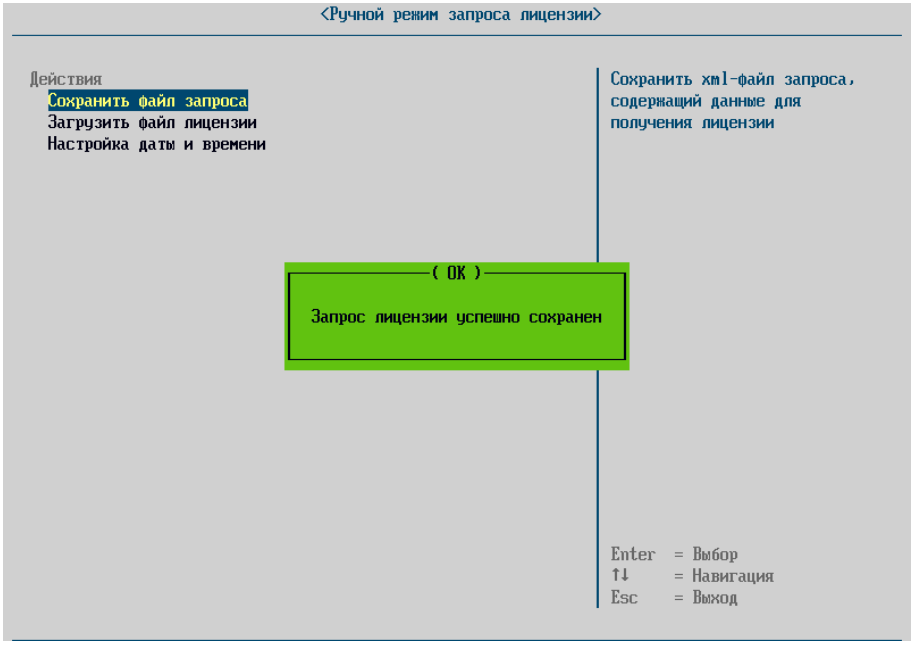

Рисунок 8 – Сохранение запроса лицензии

6) созданный файл необходимо отправить в сервисную службу ООО «НумаТех»;

7) на основе файла запроса лицензии будет создан файл лицензии («XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.p12»). Данный файл будет отправлен пользователю ответным письмом. Для активации лицензии необходимо полученный файл лицензии сохранить на USB-носитель и загрузить через пункт меню «Загрузить файл лицензии». После проверки лицензии работа Изделия будет разблокирована, Изделие будет доступно для дальнейшей настройки и использования;

8) в случае если выбран неверный файл, появляется сообщение об ошибке «Проверка лицензии завершилась с ошибкой!». В этом случае необходимо проверить соответствие устанавливаемого файла с техническими характеристиками устройства, на которое производится установка. При появлении ошибки повторно следует обратиться в сервисную службу ООО «НумаТех».

4. ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ О ПОЛЬЗОВАТЕЛЯХ И РЕЖИМЫ РАБОТЫ NUMA ARCE

4.1. Идентификация и аутентификация

Изделие поддерживает идентификацию и аутентификацию пользователей и администраторов с помощью «АНП» и «АНП+логин/пароль». Способ идентификации и аутентификации задается администратором при создании пользователя.

Для сетевых и серверных платформах, указанных в таблице 1, при включении СВТ пользователю доступна загрузка уже настроенных профилей загрузки. Для активации специальных профилей загрузки (профили такого типа создаются администратором Изделия с применением специальной метки «Требовать авторизацию» см. п.п.4.4.2.1 и отображаются серым цветом и неактивны для запуска) необходимо пройти идентификацию/аутентификацию. Для доступа к настройкам Изделия администратор в обязательном порядке должен пройти успешно процедуру идентификации и аутентификации.

Для идентификации и аутентификации необходимо:

– после появления окна «Необходимо подключить USB-токен», подключить АНП в USB-разъем СВТ;

– ввести PIN-код в соответствующем окне ввода и нажать «Enter».

В случае типа идентификации/аутентификации АНП+логин/пароль дополнительно необходимо:

– ввести логин;

– ввести пароль.

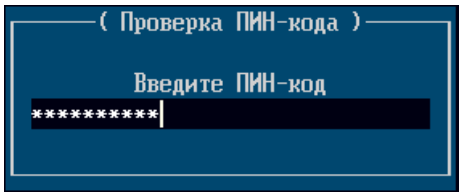

Рисунок 9 – Внешний вид окна при авторизации с помощью АНП

При вводе PIN-кода/пароля вводимые символы отображаются на экране символами «*», количество которых равно числу введенных символов.

Примечание. В случае если предварительно в Изделие не был загружен сертификат, то при попытке авторизации пользователю будет отказано в доступе с выводом сообщения «Ошибка! Доступ запрещен!».

В случае извлечения АНП во время работы с Изделием, Изделие произведет перезагрузку до повторного подключения АНП с последующим вводом аутентификационной информации.

Для мобильных и десктопных платформ, указанных в таблице 1, при включении СВТ пользователь должен пройти обязательную идентификацию и аутентификацию, прежде чем он получит доступ к профилям загрузки.

4.2. Главное меню

Рисунок 10 – Главное меню

По умолчанию меню на экране отображается в течение 7 секунд, после чего происходит запуск профиля загрузки, если он один, или первого из списка профилей, если их более одного. При нажатии на любую клавишу меню будет отображаться на экране вплоть до выбора соответствующего пункта.

Пользователь после авторизации получает доступ к списку профилей загрузки, пункт «Панель управления» для него недоступен. Если заведен всего один профиль загрузки, система сразу переходит к загрузке полезной нагрузки.

Переход и выбор пунктов меню осуществляется за счет клавиш навигации: «↑», «↓», «Enter».

4.3. Меню «Панель управления»

«Панель управления» является оснасткой для администрирования Изделием и позволяет выбрать носитель для одноразовой загрузки полезной нагрузки, создать конфигурацию загрузки и настроить параметры Изделия.

В «Панели управления» администратору с полными правами доступно 15 пунктов меню в зависимости от типа СВТ, сгруппированных в 4 раздела (см. рисунок 11).

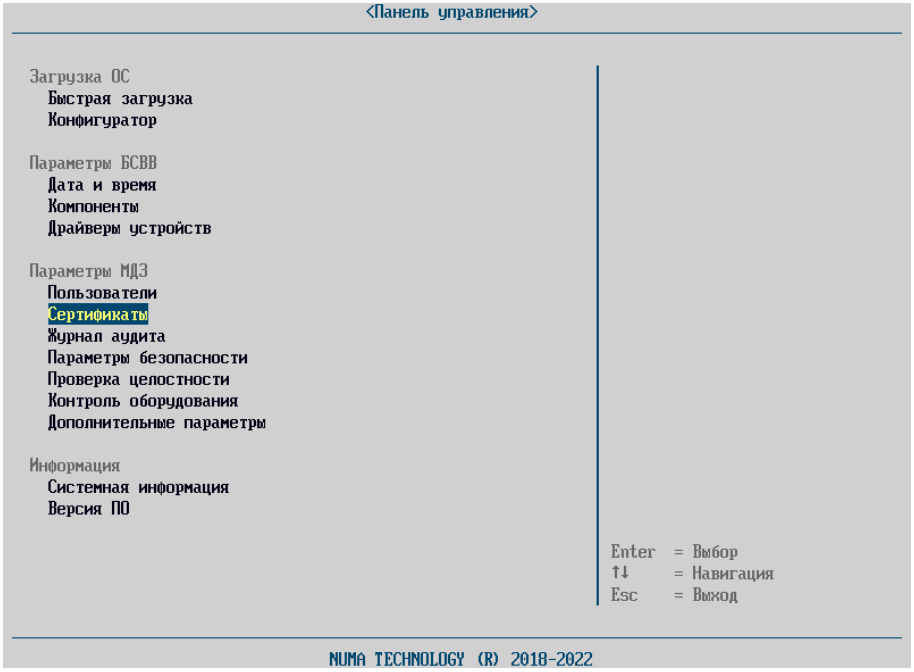

Рисунок 11 – Меню «Панель управления». Вид администратора

Администратору с правами аудитора доступны только два пункта меню (см. рисунок 12):

– «Журнал аудита»;

– «Проверка целостности».

Остальные пункты меню выводятся серым шрифтом и недоступны для выбора.

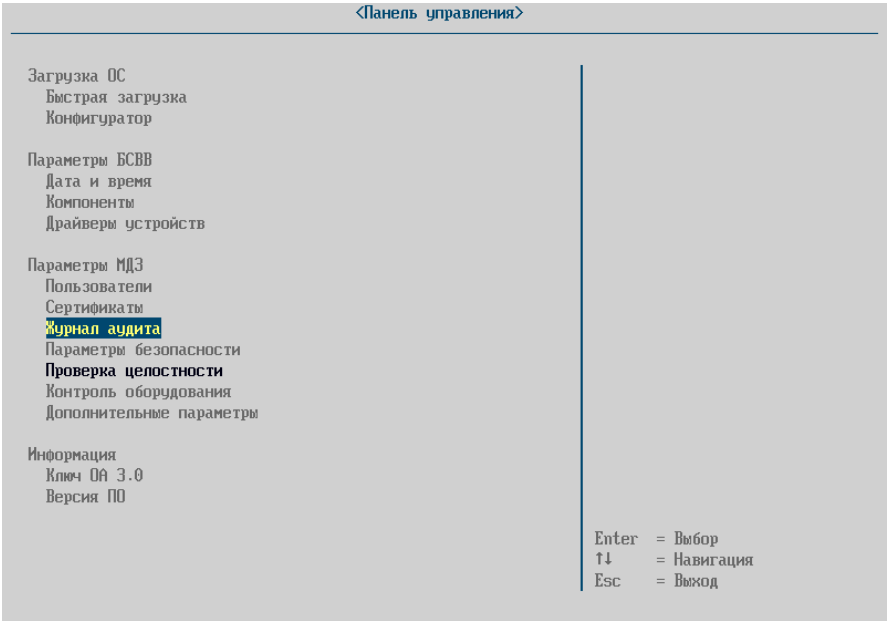

Рисунок 12 – Меню администратора с правами аудитора

Переход и выбор пунктов меню осуществляется за счет клавиш навигации: «↑», «↓», «Enter». При нажатии клавиши «Esc», предназначенной для выхода из меню «Панель управления», на экране отображается сообщение, запрашивающее подтверждение выхода из меню. При нажатии клавиши «Y» выполнится перезагрузка Изделия, а при выборе «N» – возврат в «Панель управления».

4.4. Раздел «Загрузка ОС»

4.4.1. «Быстрая загрузка»

Меню «Быстрая загрузка» (см. рисунок 13) отображает список доступных носителей и режимов загрузки. Администратору доступен выбор следующих видов загрузки:

– «EFI-авто» – загрузка с различных устройств в соответствии со спецификацией UEFI (http://www.uefi.org/specs/);

Также в этом разделе отображаются носители, определенные через EFI-переменные. Например, для Windows будет отображаться строка «Windows Boot manager».

– «EFI-файл» – администратор может выбрать файл EFI-загрузчика или EFI-приложения для загрузки ОС;

– «Legacy-загрузка» – загрузка ОС через MBR сектор носителя;

При данном типе загрузки возможность загрузки с USB-накопителей определяется настройкой в меню «Компоненты» параметра «CSM-модуль».

– «Профили загрузки» – показывает настроенные профили загрузки.

Пункт «Сканировать носители» позволяет обновить список загрузочных устройств. Необходим для отображения только что подключенных USB-накопителей.

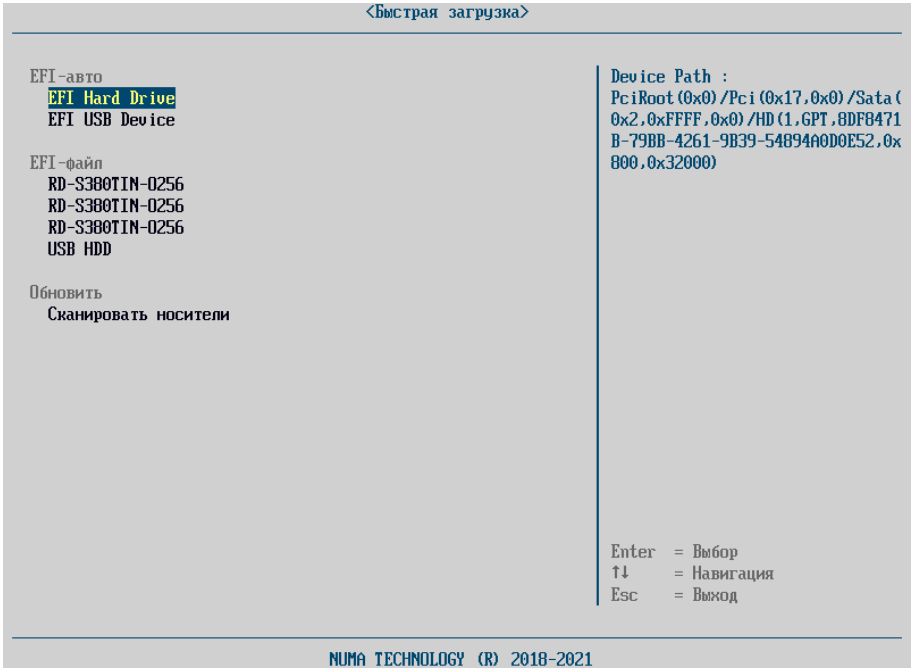

Рисунок 13 – Меню «Быстрая загрузка»

Для загрузки ОС необходимо выбрать вариант загрузки и нажать клавишу «Enter». ОС будет загружена с выбранного устройства.

4.4.2. «Конфигуратор»

Операции управления профилями загрузки осуществляются из основного пункта меню «Конфигуратор», который содержит три раздела (см. рисунок 14): «Профили загрузки», «Действия с профилями», «Параметры».

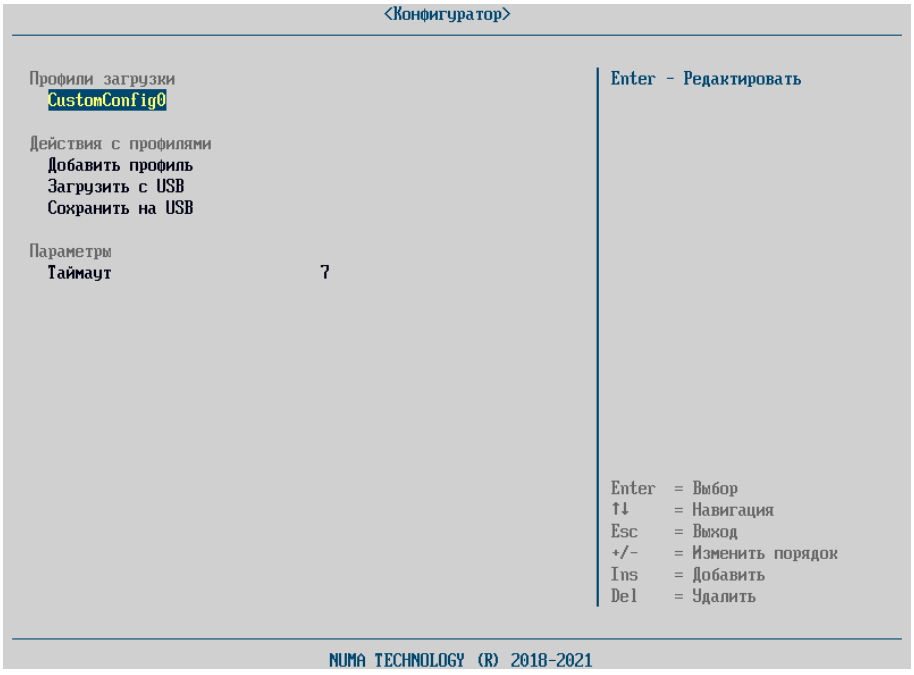

Рисунок 14 – Меню «Конфигуратор»

Раздел «Профили загрузки» содержит информацию о созданных профилях загрузки.

Раздел «Действия с профилями» содержит следующие пункты:

– «Добавить профиль»;
– «Загрузить с USB»;
– «Сохранить на USB».

При создании двух и более профилей загрузки в Изделии возможно настроить приоритет загрузки профилей с помощью клавиш «+» и «–».

Параметр «Таймаут» в разделе «Параметры» устанавливает время ожидания выбора в главном меню при запуске Изделия. Параметр может принимать значения от 1 до 30 секунд.

4.4.2.1. Создание нового профиля загрузки

Для создания новой конфигурации профиля загрузки необходимо нажать кнопку «Ins» или выбрать пункт «Добавить профиль» и заполнить необходимые поля:

– «Имя профиля» – имя профиля, отображаемое в «Главном меню»;

– «Тип загрузки» – необходимо выбрать загрузочное устройство;

– «Требовать авторизацию» – активация данного параметра делает создаваемый профиль загрузки недоступным для всех пользователей, кроме администратора с полными правами доступа (подробное описание параметра представлено в пункте 4.4.2.5);

– «Контроль целостности» – выбор файлов/каталогов для контроля целостности. Автоматически при создании профиля загрузки на контроль целостности ставится загрузочный файл ОС;

– «Сохранить профиль» – сохранение настроек профиля загрузки.

Доступны следующие типы загрузки:

– Legacy-загрузка (загрузка через MBR-сектор). Отображается в виде «PX-<диск>», загрузка возможна только с жестких дисков и CD/DVD;

– EFI-загрузка (присутствует загрузочный EFI файл), отображается строкой «USB Hard Drive» или «EFI USB Device»;

– Пользовательский тип – позволяет выбрать альтернативный EFI-загрузчик или настроить Linux-загрузку (если соответствующий параметр включен в «Компонентах»).

В зависимости от загружаемой полезной нагрузки типов загрузки может быть больше.

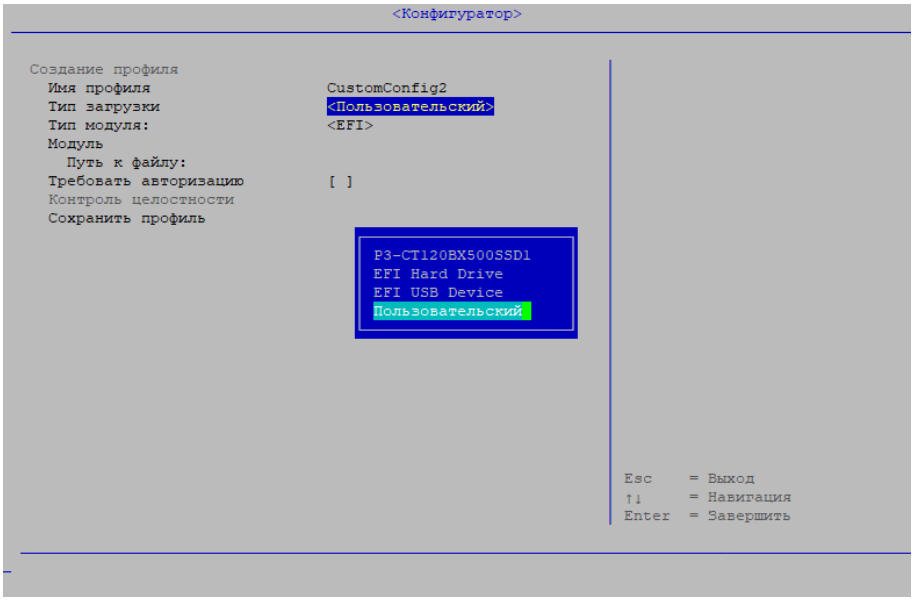

Рисунок 15 – Выбор типа загрузки

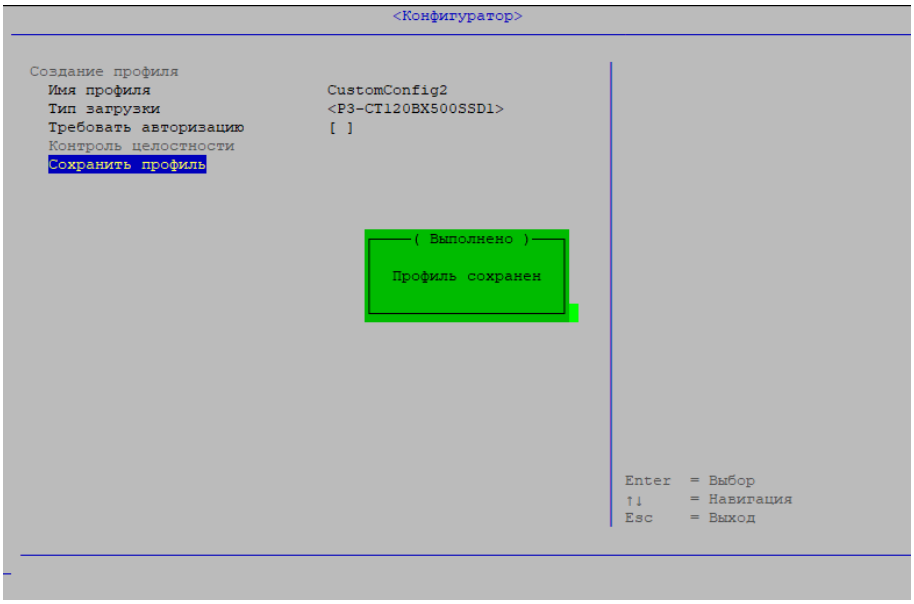

Рисунок 16 – Созданный профиль загрузки

4.4.2.2. Удаление профилей загрузки

Для удаления профиля загрузки необходимо перейти на профиль загрузки и нажать кнопку «Del» (см. рисунок 17).

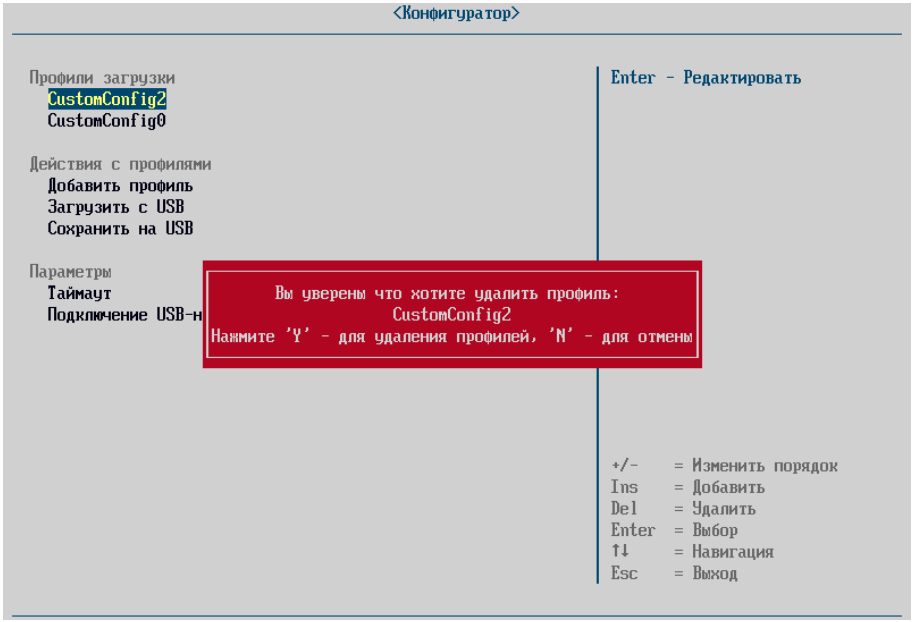

Рисунок 17 – Удаление профиля загрузки

4.4.2.3. Импорт профилей загрузки

Для импорта ранее сохраненных настроек профилей из внешнего файла необходимо перейти в пункт «Загрузить с USB» выполнить следующие действия:

- подключить USB-носитель с файлом конфигурации;
- выбрать пункт меню «Конфигуратор» → «Загрузить с USB»;
- выбрать требуемый файл из каталога, соответствующий формату JSON.

В случае успешной загрузки конфигурации будет выдано соответствующее сообщение:

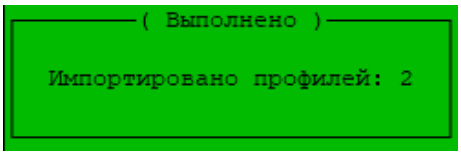

Рисунок 18 – Импорт профилей загрузки

В случае отсутствия в USB-портах СВТ хотя бы одного рабочего носителя будет выдано сообщение об ошибке:

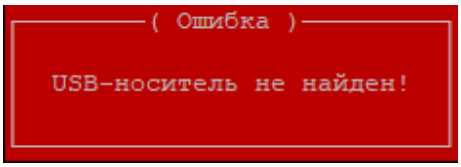

Рисунок 19 – USB-носитель не найден

4.4.2.4. Экспорт профилей загрузки

Для того чтобы экспортировать конфигурацию во внешний файл, необходимо перейти в пункт меню «Конфигуратор» → «Сохранить на USB» и выполнить следующие действия:

- подключить USB-носитель (с файловой системой формата FAT32);
- выбрать пункт меню «Конфигуратор» → «Сохранить на USB».

В случае успешной выгрузки файла конфигурации будет выдано соответствующее сообщение:

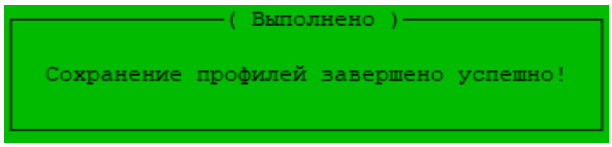

Рисунок 20 – Экспорт профилей загрузки

Файл с конфигурацией будет сохранен в каталоге /bios USB-носителя с именем BootProfiles[YY-MM-DD].json, где YY-MM-DD – дата сохранения.

4.4.2.5. Параметр «Требовать авторизацию»

Примечание. Данная настройка доступна только для сетевых и серверных платформ, указанных в таблице 1.

Для защиты определенного профиля загрузки от несанкционированного запуска необходимо в форме создания/просмотра профиля активировать чекбокс напротив параметра «Требовать авторизацию» (см. рисунок 21).

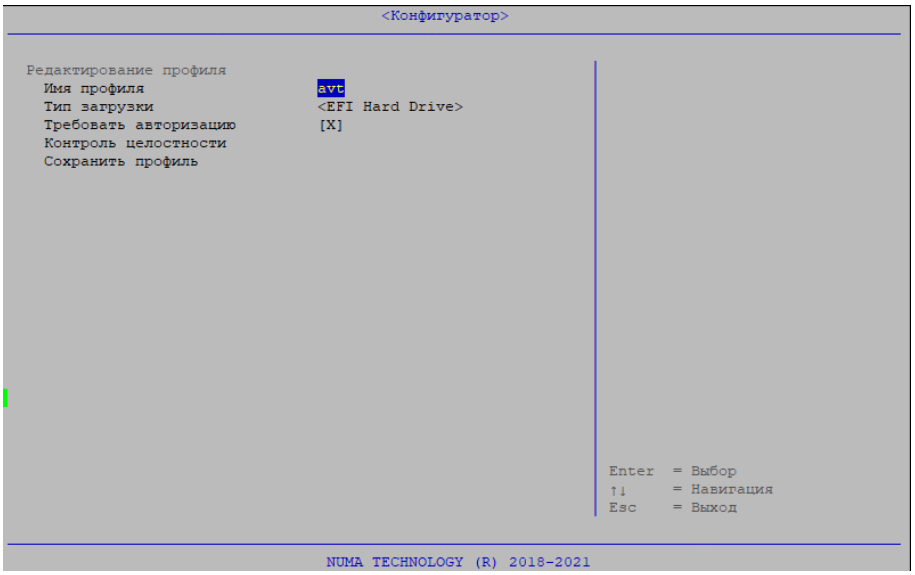

Рисунок 21 – Активация параметра «Требовать авторизацию»

При запуске Изделия и отображении главного меню профили загрузки с включенным параметром «Требовать авторизацию» будут недоступны (см. рисунок 22).

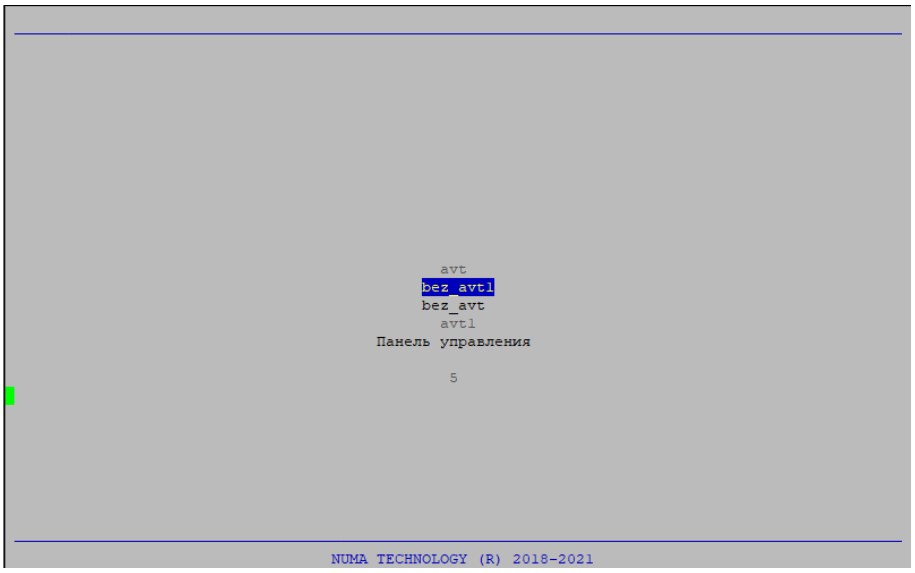

Рисунок 22 – Главное меню

Для возможности запуска защищенных профилей загрузки необходимо через главное меню перейти в «Панель управления» и авторизоваться под любой существующей учетной записью.

Администратору с полным доступом необходимо перейти в меню «Быстрая загрузка» и выбрать профиль загрузки (см. рисунок 23).

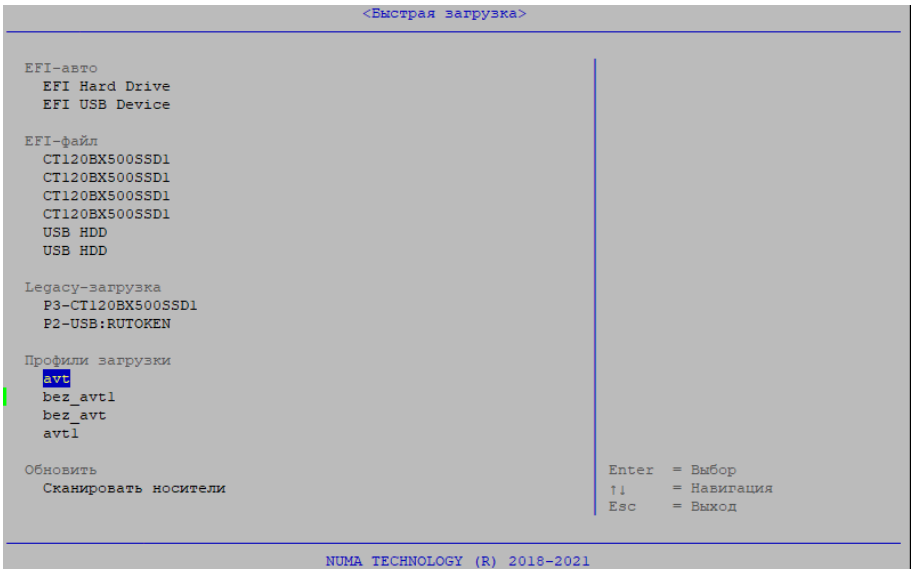

Рисунок 23 – Меню «Быстрая загрузка»

В случае авторизации под учетной записью пользователя, Изделие перейдет в главное меню только со списком профилей загрузки. Пользователю доступны все профили загрузки, включая те, для которых администратор активировал параметр «Требовать авторизацию» (см. рисунок 24).

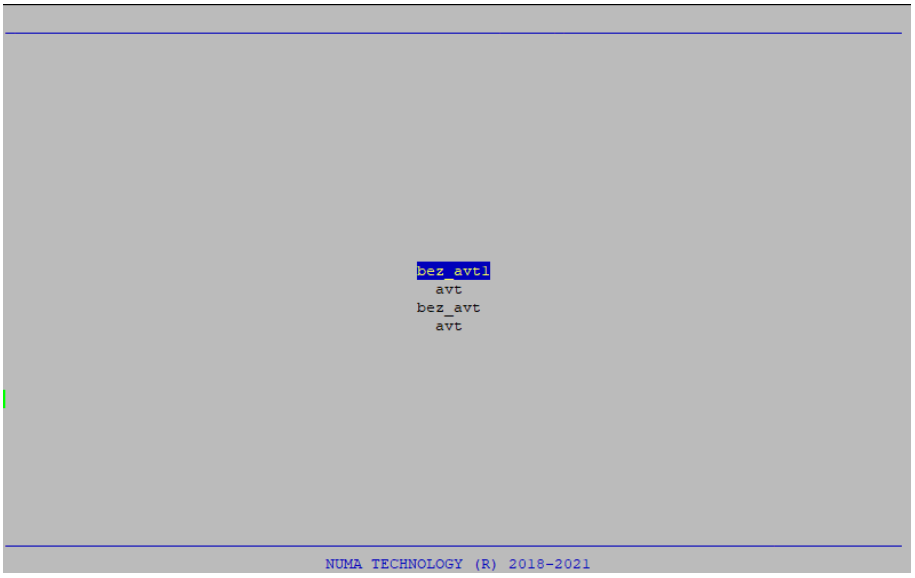

Рисунок 24 – Главное меню пользователя

4.4.2.6. Настройка контроля целостности

Нарушение целостности загружаемой программной среды, нарушение целостности оборудования или параметров загрузки, заданных в «Конфигураторе», приведет к блокированию загрузки ОС.

Настройка контроля целостности производится в отдельном меню «Конфигуратор» → «Редактирование профиля» → «Контроль целостности» (см. рисунок 25).

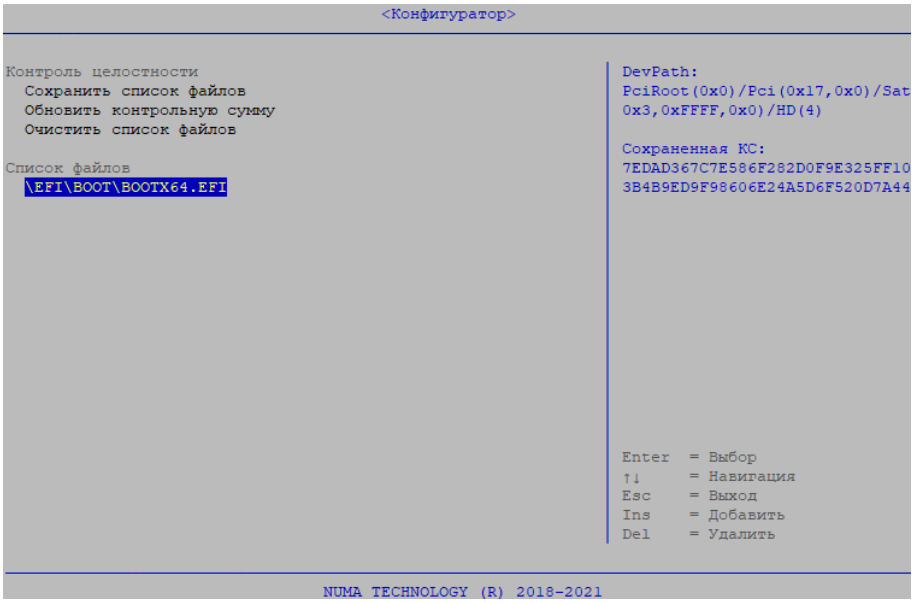

Рисунок 25 – Настройка контроля целостности

Для добавления нового файла в список проверяемых перед загрузкой ОС файлов необходимо выполнить следующие действия:

– нажать клавишу «Ins» для перехода в меню проводника;

– выбрать устройство, с которого необходимо добавить файл;

– выбрать требуемый файл и нажать «Enter» – файл появится в списке добавляемых файлов, справа будет выведены его путь и контрольная сумма (см. рисунок 25);

– для удаления файла из этого списка необходимо выделить его и нажать «Del» (подтверждение не запрашивается); чтобы удалить все файлы из предварительного списка, необходимо выбрать пункт меню «Очистить список файлов»;

– для добавления в список ещё одного файла необходимо вернуться к первому шагу;

– после окончания процедуры добавления файлов следует выбрать пункт меню «Сохранить список файлов» и нажать «Enter». На экране появится сообщение:

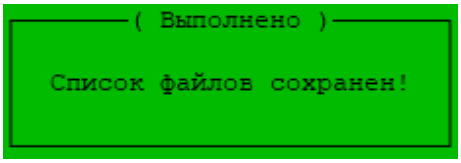

Рисунок 26 – Сохранения списка файлов на контроль целостности

Для пересчета контрольной суммы необходимо выбрать пункт «Обновить контрольную сумму» и нажать клавишу «Enter», после чего будет произведено автоматическое обновление контрольной суммы.

4.5. Раздел «Параметры БСВВ»

4.5.1. «Дата и время»

Для того чтобы установить системные дату и время необходимо выполнить следующие действия (см. рисунок 27):

– выбрать меню «Дата и время»;

– с помощью клавиш «+» и «–» отредактировать значение;

– выйти из меню с помощью клавиши «Esc».

После выхода из меню данные сохранятся автоматически.

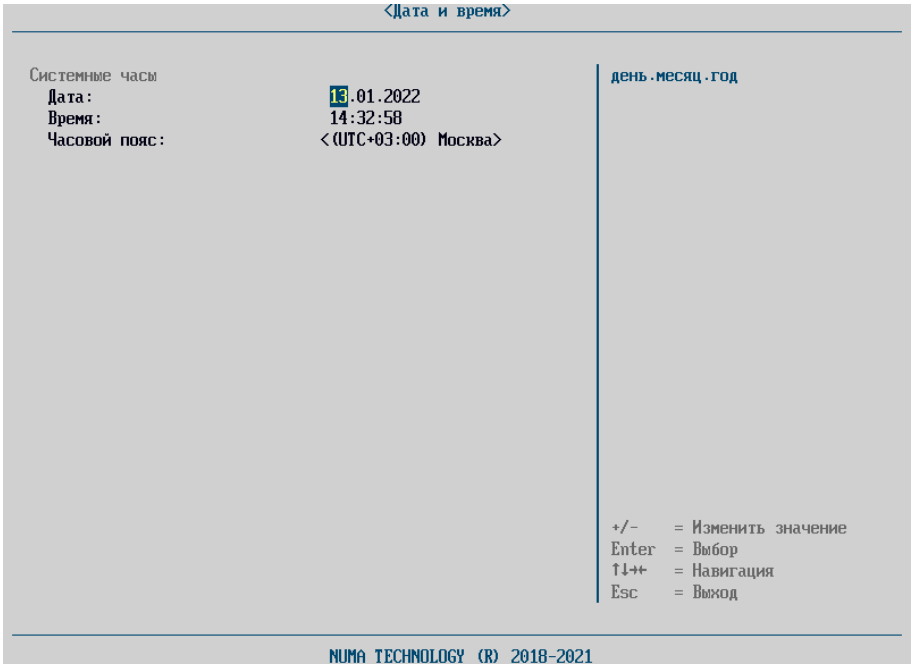

Рисунок 27 – Установка даты и времени

4.5.2. «Компоненты»

Меню «Компоненты» предназначено для управления работой модулей БСВВ (см. рисунок 28).

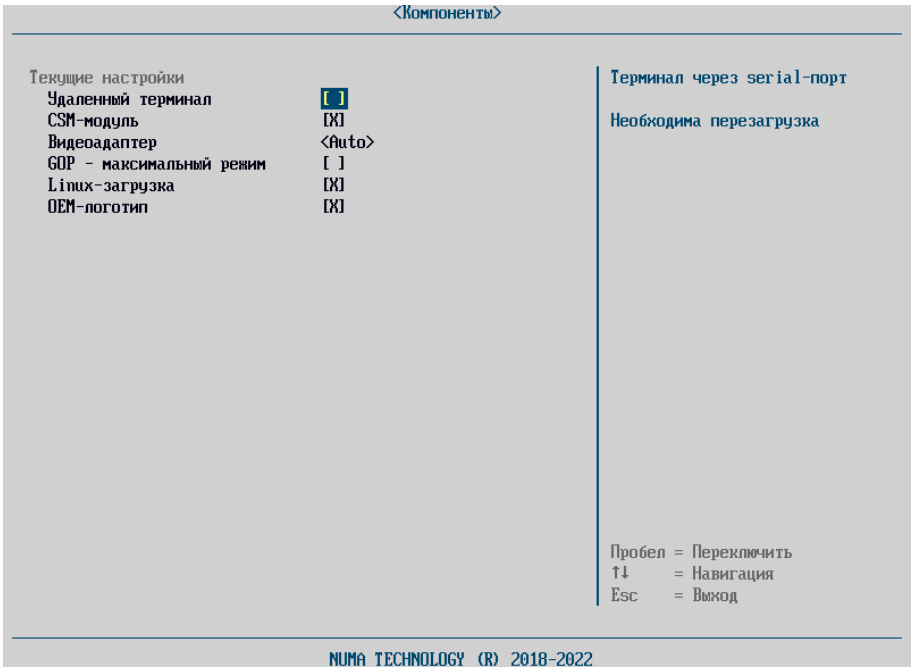

Рисунок 28 – Меню «Компоненты»

Примечание. Список параметров зависит от типа СВТ, на которое установлено Изделие.

Меню предоставляет возможность изменения значений следующих параметров:

– Удаленный терминал подключает вывод информации в предварительно подключенную консоль через serial-порт;

– CSM-модуль – поддержка Legacy-загрузки. Отключение ускоряет запуск БСВВ и ОС, в меню «Быстрой загрузки» перестает появляться раздел Legacy-загрузки. Включение-выключение параметра автоматически включает/выключает параметр «Драйвер USB-Legacy (CSM)»;

– Драйвер USB Legacy (CSM) – драйвер для использования USB устройств в Legacy-режиме;

– Видеоадаптер определяет порядок выбора видеоадаптера для работы (интегрированный/ внешний);

– GOP – максимальный режим подключает максимально возможное разрешение видеоадаптера при запуске ОС;

– Linux-загрузка – загрузка драйверов Ext2/Ext4 и добавление тип модуля «Linux» для пользовательской загрузки;

– OEM логотип – параметр, позволяющий настраивать отображение логотипов при загрузке ОС Windows/ОС Linux в режиме EFI. При включенном параметре при загрузке отображается логотип производителя СВТ, в случае выключенного параметра отображается стандартный логотип загрузки Windows/Linux.

Примечания:

1. При включении/выключении параметров внесенные изменения вступят в силу при следующей перезагрузке.

2. Для включения параметров «CSM-модуль» и «Драйвер USB Legacy (CSM)» необходимо выключить параметр «Secure Boot» (см. пункт 4.6.4.2).

4.5.3. «Драйверы устройств»

Данный пункт позволяет просматривать драйверы устройств, установленные на СВТ, проверять правильность их работы и изменять параметры (см. рисунок 29).

Примечание. Список устройств зависит от типа СВТ, на которое установлено Изделие.

Настройка и переключение параметров осуществляется с помощью навигационных клавиш и клавиш-переключателей. Допустимые для данного раздела меню клавиши описаны в правом нижнем углу форм.

Примечание. Все настройки вступят в силу только после перезагрузки СВТ!

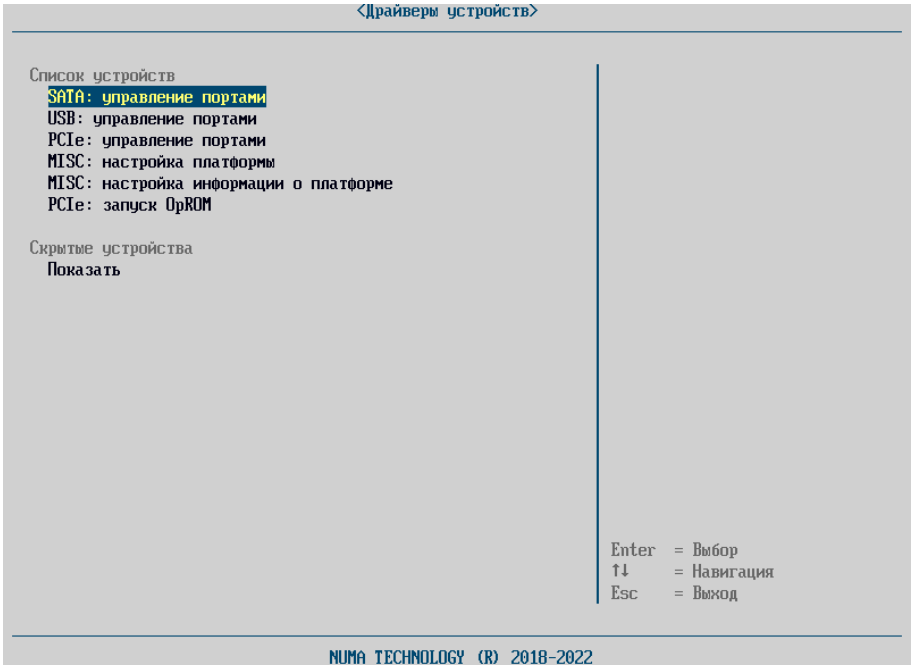

Рисунок 29 – Меню режима «Драйверы устройств»

4.5.3.1. CPU: конфигурация

Данный пункт настраивает функцию Hyper-threading, которая обеспечивает более эффективное использование ресурсов процессора, позволяя выполнять несколько потоков на каждом ядре (см. рисунок 30).

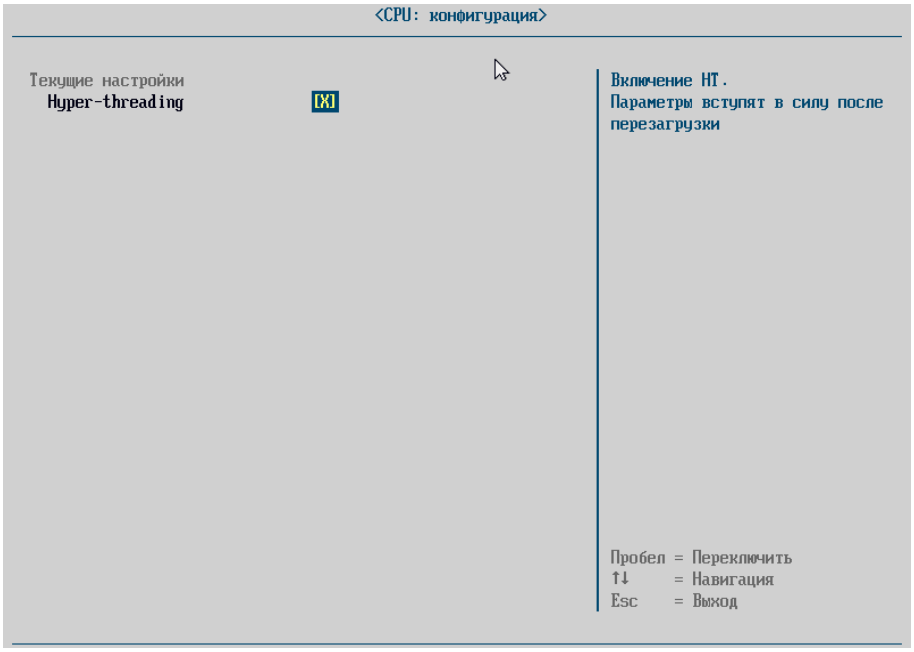

Рисунок 30 – Меню «CPU: конфигурация»

4.5.3.2. SATA: управление портами

Меню «SATA: управление портами» отображает все доступные SATA-порты и дает возможность администратору отключать/подключать порты, с помощью механизма чекбоксов (см. рисунок 31). При отключении SATA-порта отключается и устройство, подключенное к этому порту. Отключение можно наблюдать на меню «Быстрая загрузка». Для этого на форме SATA: управление портами необходимо отключить SATA-порт, отображаемый в переменной Device Path для подключенного SATA-устройства и обязательно выполнить перезагрузку. Подключенное устройство перестанет отображаться в меню «Быстрая загрузка», хотя физически подключено к порту или плате кабелями питания и передачи данных. Кроме этого, факт отключения устройства можно увидеть в меню «Системная информация»: если устройство было единственным SATA-устройством, в меню перестанет отображаться раздел «SATA-носители». Состояние чекбокса этого порта будет отображаться как – [ ] «отключено».

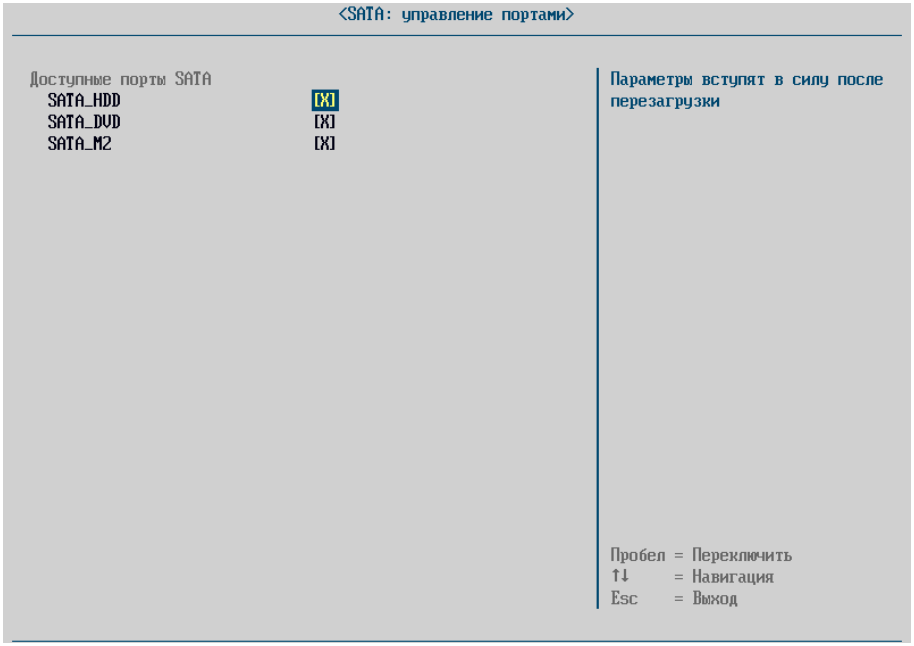

Рисунок 31 – Меню «SATA: управление портами»

4.5.3.3. SATA: контроль доступа

Меню предназначено для управления доступом к подключенным SATA-устройствам. На подключенные жесткие диски можно установить пароль для доступа к диску.

Пароли вводятся парой – User/Master: User-пароль позволяет осуществлять ставить и снимать защиту с жесткого диска, Master-пароль позволяет сбрасывать User-пароль в случае его потери. Поддерживается два уровня защиты:

– High level – сброс User-пароля происходит без удаления информации с жесткого диска;

– Maximum level – сброс User-пароля происходит только после полного форматирования жесткого диска.

Для установки защиты необходимо:

– выбрать необходимый диск из списка подключенных дисков и нажать клавишу «Enter». На появившейся форме в разделе «Действия», выбрать пункт «Установить защиту»;

– в разделе «Установить защиту», выбрать «тип пароля» и «security level», внимательно читая советы-подсказки в правой части экрана. Сначала для User-пароля, затем для Master-пароля. Пароли устанавливаются с последующим подтверждением. Поддерживаются пароли до 32 символов;

– обязательно сохранить эти пароли на любом доступном носителе в надежном месте.

Примечание. В случае потери паролей можно потерять всю информацию на диске. Снятием блокировок в случае утраты Master пароля занимаются узкоспециализированные сервисы!

После установки пароля, появится информационное сообщение:

```
Для того, чтобы изменения вступили в силу необходимо выключение питания
```

После включения на экране будет появляться окно запроса:

```
Для разблокировки диска введите user пароль:
(Для перехода к master паролю оставьте поле пустым)
```

Окно запроса будет выводиться во время загрузки прогресс-бара инициализации Изделия и появления окна «Главного меню».

Если установлены несколько жестких дисков с контролем доступа, то будут последовательно выведены формы запросов паролей для каждого диска.

Если пароль не введен, диск будет недоступен для использования, в меню контроля доступа будут активированы чекбоксы для параметров «Security Enabled» и «Security locked».

При корректном вводе пароля – только «Security Enabled».

При вводе некорректного пароля дважды, происходит блокировка и активируются поля: «Security Count Expired», «Security Locked» (см. рисунок 33).

Значения сбрасываются при отключении питания. На экран выводится сообщение об ошибке:

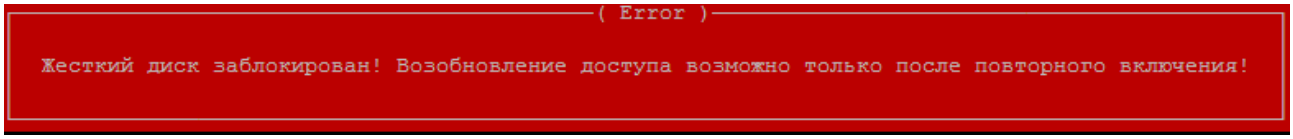

Рисунок 32 – Окно сообщения об ошибке

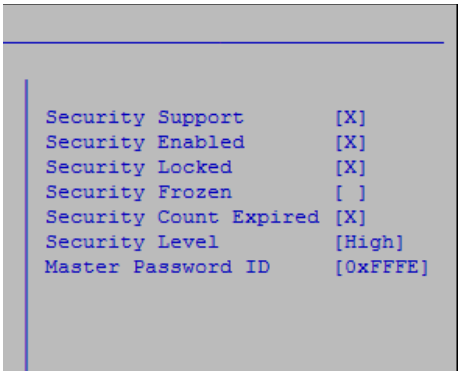

Рисунок 33 – Состояния полей формы контроль доступа при блокировке диска

При попытке выполнить какие-либо действия на форме контроля доступа, Изделие выведет следующее сообщение:

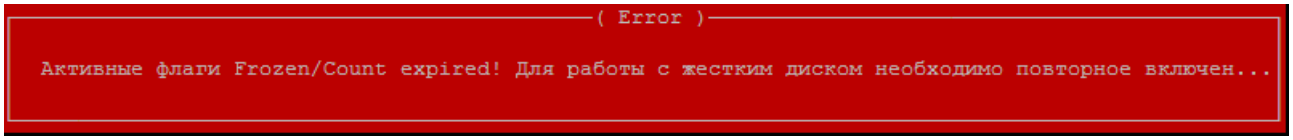

Рисунок 34 – Сообщение на форме контроля доступа

Поле «Security Frozen» активируется, если после ввода пароля и загрузки ОС выполнить перезагрузку. Перезагрузка происходит без запроса пароля к диску. Загрузка ОС в этом случае разрешена.

Для снятия защиты, необходимо:

– выбрать жесткий диск с установленной защитой и нажать клавишу «Enter»;

– на появившейся форме в разделе «Действия», выбрать пункт «Снять защиту»;

– ввести значение User-пароля в диалоговой форме «Введите старый пароль». После ввода корректного пароля, появится сообщение «Операция выполнена»;

– вернуться на форму с разделом «Подключенные диски» и убедиться, что для диска активирован только один чекбокс «SecuritySupport».

4.5.3.4. USB: управление портами

Меню «USB: управление портами» (см. рисунок 35) отображает все доступные USB-порты и дает возможность администратору отключать/подключать порты с помощью механизма чекбоксов.

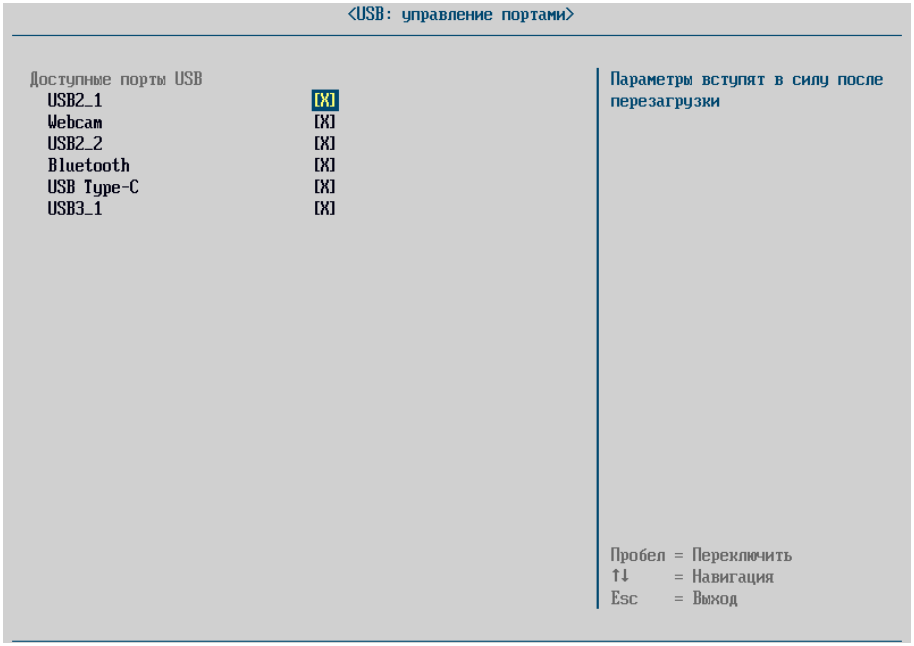

Рисунок 35 – Меню «USB: управление портами»

При отключении USB-порта соответственно отключается и устройство, подключенное к этому порту. Отключение можно наблюдать в меню «Быстрая загрузка». Для этого в меню «USB: управление портами» необходимо отключить USB-порт, отображаемый в переменной Device Path для подключенного USB-носителя и обязательно выполнить перезагрузку. Подключенное устройство перестанет отображаться в меню «Быстрая загрузка», хотя физически остается подключенным к порту.

Кроме раздела управления доступностью USB-портов, в некоторых платформах доступен раздел «Фильтрация устройств». Фильтр может блокировать работу USB-носителей определенных категорий (см. рисунок 36):

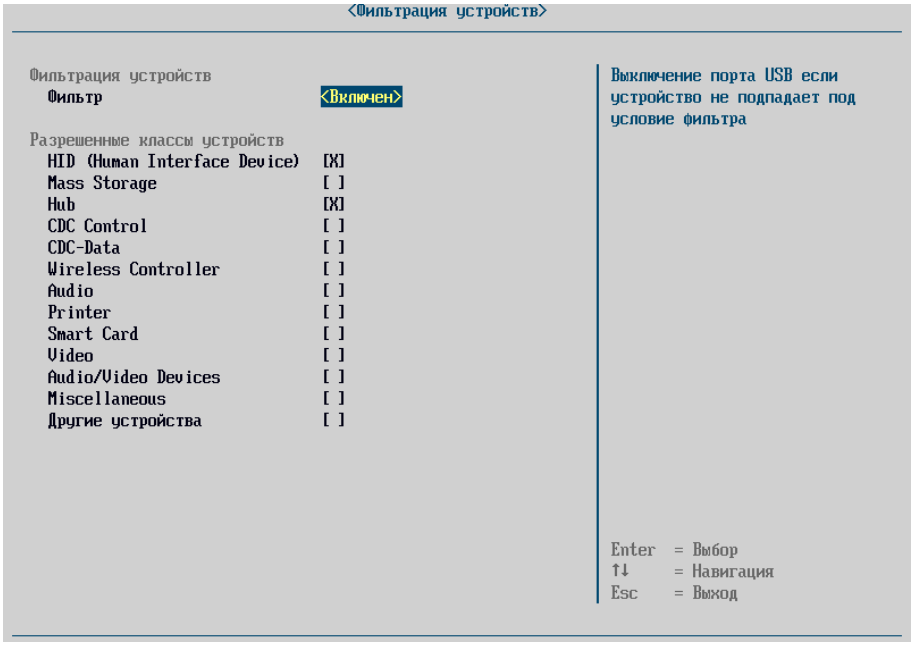

Рисунок 36 – Меню «USB: управление портами». Разрешенные классы устройств

– к USB HID (human interface device) устройствам относятся USB-клавиатура и USB-мышь, USB-джойстик;
– к Mass Storage относятся USB-носители;
– к Hub относятся USB-хабы;

– к CDC Control относятся модем, сетевая карта, COM-порт;
– CDC-Data используется совместно с классом CDC;
– к Wireless Controller относится Bluetooth-адаптер;
– к Audio относятся звуковая карта, MIDI;
– к Printer относятся принтеры и сканеры;
– к Smart Card относятся карты памяти;
– к Video относятся веб-камеры;
– Audio/Video Devices относятся аудио- и видеоустройства;
– к Miscellaneous относятся ActiveSync-устройства;
– другие устройства.

При попытке осуществить загрузку с USB-носителя в меню «Быстрая загрузка» или при запуске Изделия (если в меню «Конфигуратор» для подключенного носителя выбрано действие «Загрузить с USB») Изделие выдаст сообщение об ошибке (см. рисунок 37) и автоматически осуществит перезагрузку. Дополнительно к этому, после перезагрузки USB-порт будет отключен до момента следующей перезагрузки Изделия. В меню «USB: управление портами» данный порт будет выделен серым цветом и недоступен (заблокирован).

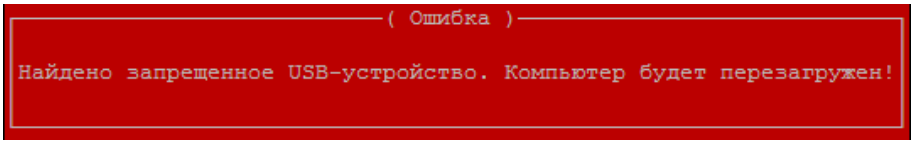

Рисунок 37 – Форма сообщения об ошибке

Примечание. Если USB-накопитель подключен вместе с HID-устройствами к одному USB-хабу, будет заблокирована работа всех устройств, подключенных к USB-хабу.

4.5.3.5. PCI: управление портами

Меню «PCI: управление портами» (см. рисунок 38) отображает все доступные PCI-порты и дает возможность администратору отключать/подключать порты с помощью механизма чекбоксов. При отключении PCI-порта соответственно отключается и устройство, подключенное к этому порту. Для этого в меню «PCI: управление портами» отключить PCI-порт, отображаемый в переменной Device Path для подключенного PCI-устройства, и обязательно выполнить перезагрузку. Подключенное устройство перестанет отображаться в меню «Быстрая загрузка», хотя физически подключено к порту (плате кабелями питания и передачи данных). Кроме этого факт отключения устройства можно увидеть в меню «Системная информация»: если устройство было единственным PCI-устройством, на форме перестанет отображаться раздел «PCI-носители». Состояние чекбокса этого порта будет отображаться как – [ ] «отключено».

Для переключения состояния определения PCI-портов в меню «PCI: управление портами» необходимо нажать клавишу «Пробел».

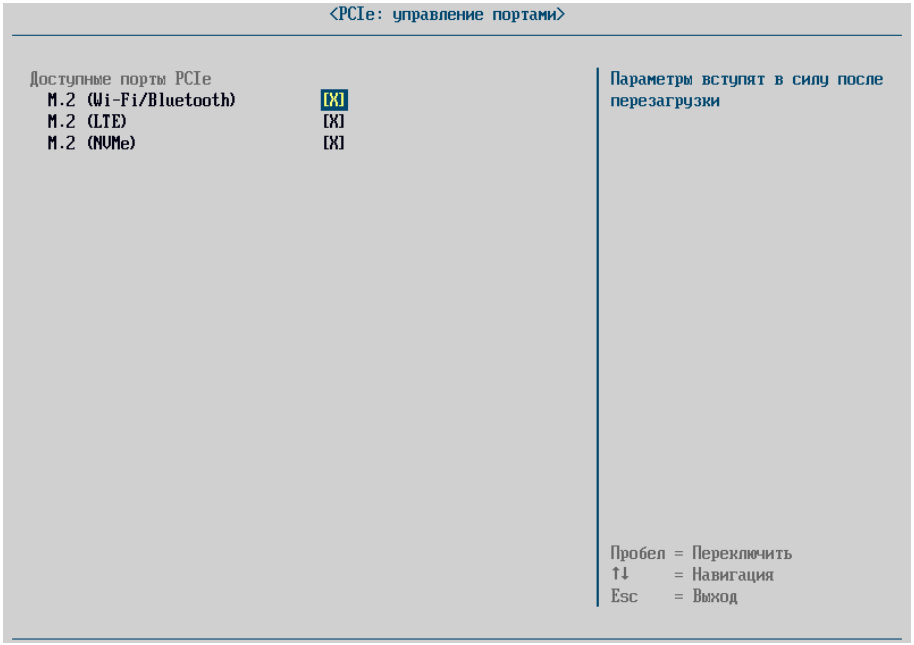

Рисунок 38 – Меню «PCI: управление портами»

4.5.3.6. PCI: конфигурация

Данная настройка позволяет устанавливать количество используемых линий шины PCIe для соответствующего порта (см. рисунок 39).

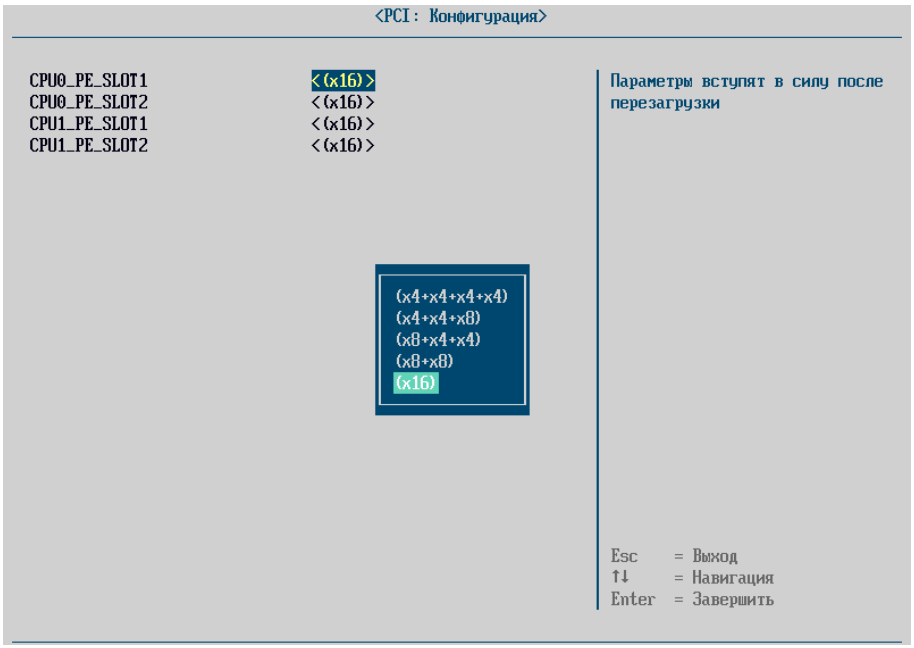

Рисунок 39 – Меню выбора конфигурации PCI

Для настройки параметра необходимо клавишами навигации выбрать подходящее значение и нажать клавишу «Enter».

4.5.3.7. PCIe: запуск OpRom

Данный пункт необходим для настройки запуска OpRom внешних PCIe устройств. Для включения параметра необходимо перейти в пункт «PCIe: запуск OpRom», добавить устройство, выбрав действие «Добавить» в разделе «Действия с устройствами». На форме «Добавление устройства» отобразится идентификатор подключенного устройства и тип поддерживаемой загрузки (Legacy/EFI). Добавленную запись необходимо сохранить, нажав кнопку «Сохранить». По умолчанию запуск OpRom разрешен.

Примечания:

1. В случае поддержки устройством обоих типов загрузки одновременно, необходимо добавить отдельную запись для каждого типа загрузки.

2. Значение настройки «Запуск OpRom» для конкретного устройства имеет больший приоритет, чем значение настройки «Запуск OpRom по умолчанию».

В разделе «Дополнительно» устанавливается настройка параметра «Режим по умолчанию» (см. рисунок 40).

Параметр может иметь три значения:

– «Нормальный запуск» или «Разрешен» – OpRom запускается во время инициализации БСВВ;

– «Запрещен» или «Запуск отключен» – OpRom устройство не должно отработать;

– «Отложенный запуск» – OpRom устройство должно успешно стартовать при передаче управления (загрузке) ОС.

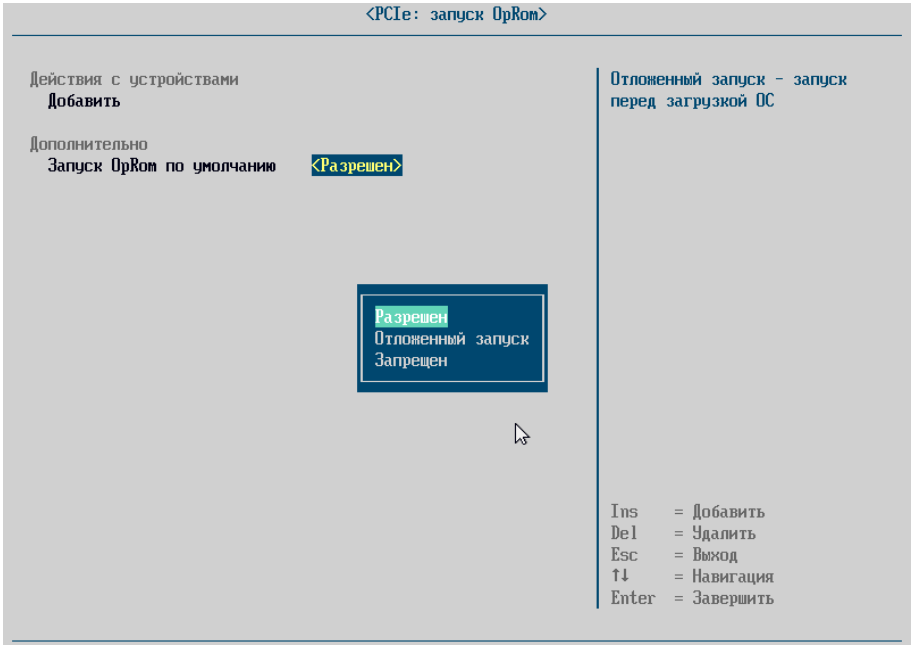

Рисунок 40 – «PCIe: запуск OpRom»

Список совместимых PCIe устройств определен в Приложении 4 настоящего документа.

4.5.3.8. MISC: настройка платформы

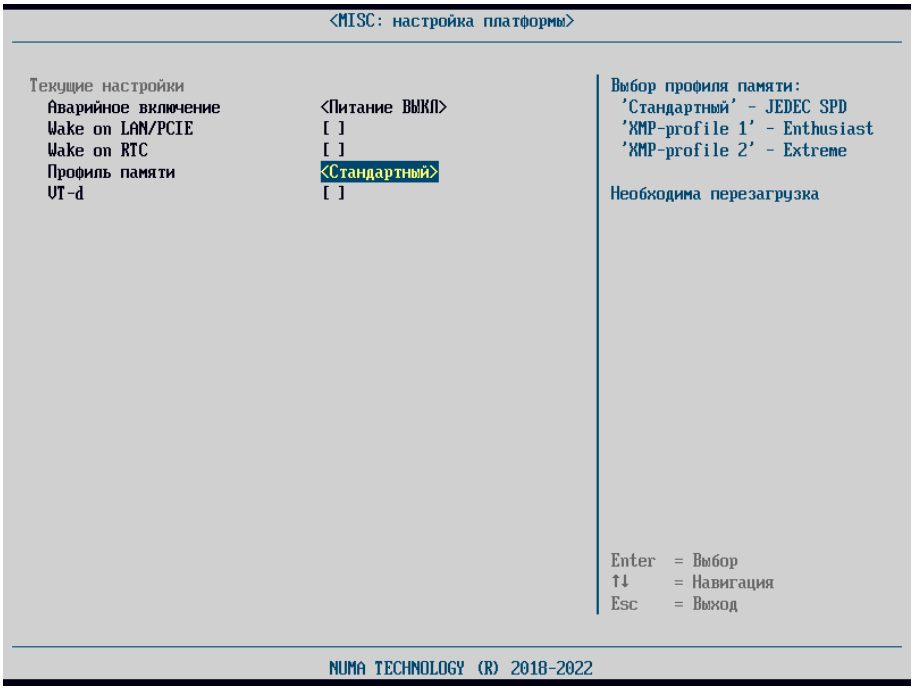

Рисунок 41 – Меню «MISC: настройка платформы»

4.5.3.8.1. Аварийное включение

Данный пункт предназначен для настройки поведения Изделия в случае аварийного выключения питания (см. рисунок 41).

В зависимости от установленного значения настройки, после аварийного отключения питания плата:

– при значении <Питание ВКЛ> будет автоматически включаться при восстановлении питания;

– при значении <Питание ВЫКЛ> не будет автоматически включаться при восстановлении питания.

4.5.3.8.2. Wake on LAN/PCIe

Настройка параметра «Wake on LAN/PCIE» позволяет отключать/включать СВТ посредством отправки через локальную сеть специального сигнала на сетевой адаптер и PCIe-порты (см. рисунок 41).

4.5.3.8.3. Wake on RTC

Параметр «Wake on RTC» отвечает за автоматическое включение питания компьютера в заданное время по сигналу от часов RTC (см. рисунок 41).

4.5.3.8.4. Профиль памяти

Профили памяти предназначены для задания параметров работы ОЗУ (см. рисунок 41). В зависимости от установленных планок оперативной памяти доступны:

– Стандартный профиль – стандартные значения работы оперативной памяти согласно JEDEC SPD;

– XMP-профили, предназначенные для увеличения производительности ОЗУ.

4.5.3.8.5. VT-d

Параметр «VT-d» предназначен для поддержки технологии виртуализации Intel VT-x и позволяет создавать на обычном ЭВМ несколько виртуальных машин (см. рисунок 41).

4.5.3.8.6. Настройка аудиокодека

Данное меню предназначено для выбора аудиокодека. На выбор доступно два аудиокодека: I2S (ES8336) и HDA (Realtek). По умолчанию установлен «I2S (ES8336)».

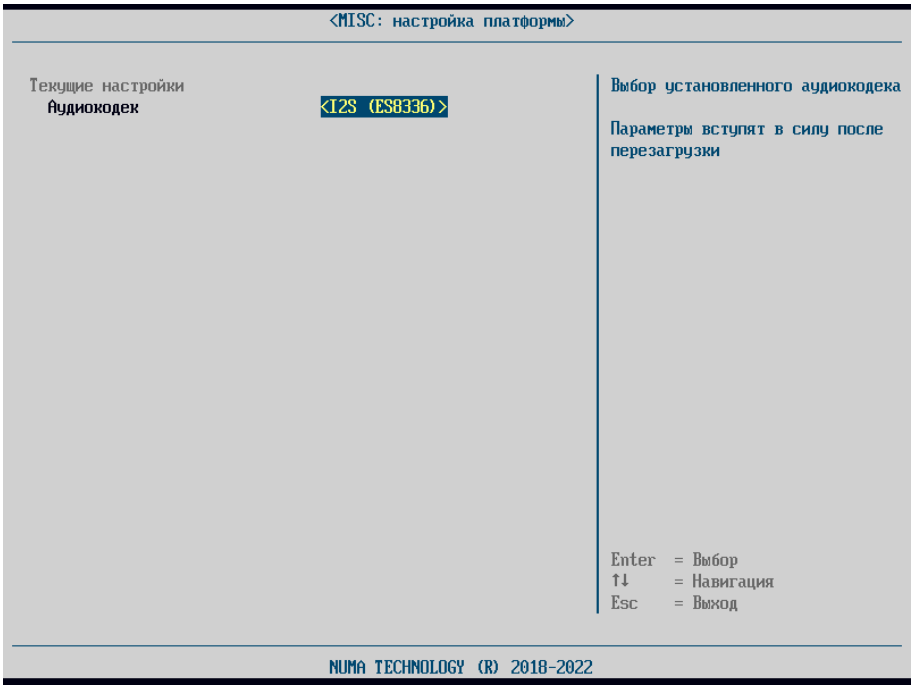

Рисунок 42 – Меню «MISC: настройка платформы»

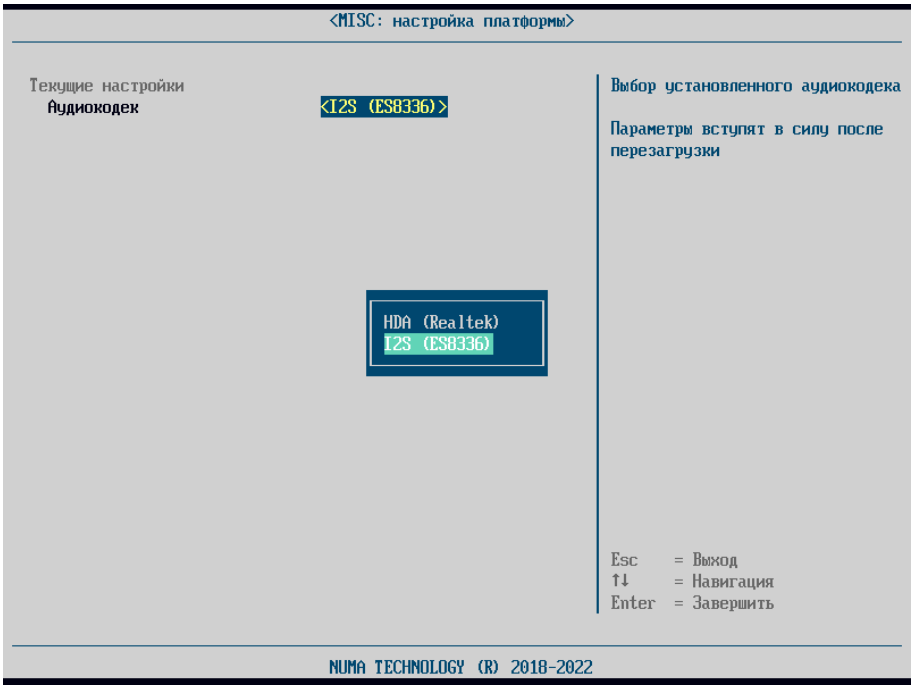

Рисунок 43 – Параметры аудиокодека

4.5.3.9. MISC: настройка информации о платформе

Данный пункт меню позволяет присваивать и изменять инвентарный номер платформы (см. рисунок 44).

Изделие поддерживает ввод до 15 символов.

Введенный инвентарный номер отображается в меню «Системная информация».

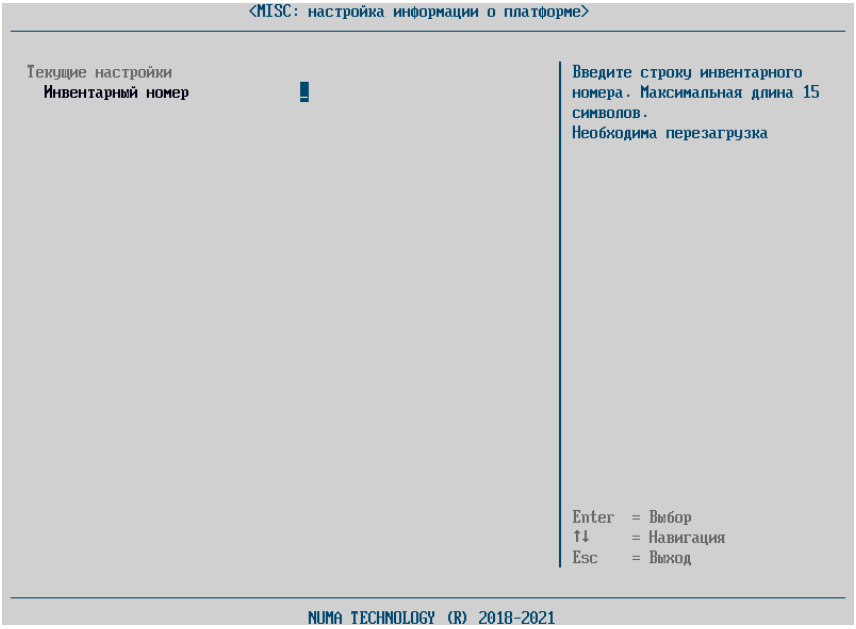

Рисунок 44 – Меню «MISC: настройка информации о платформе»

4.5.3.10. Скрытые устройства

В меню «Скрытые устройства» отображается информация о Gigabit Ethernet контроллерах:

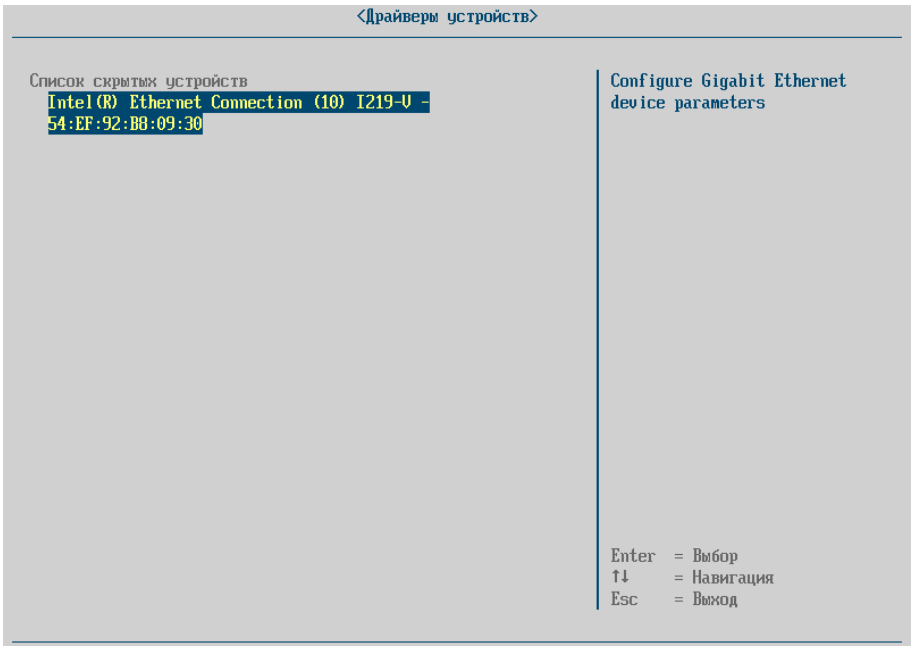

Рисунок 45 – Меню «Драйверы устройств: Скрытые устройства»

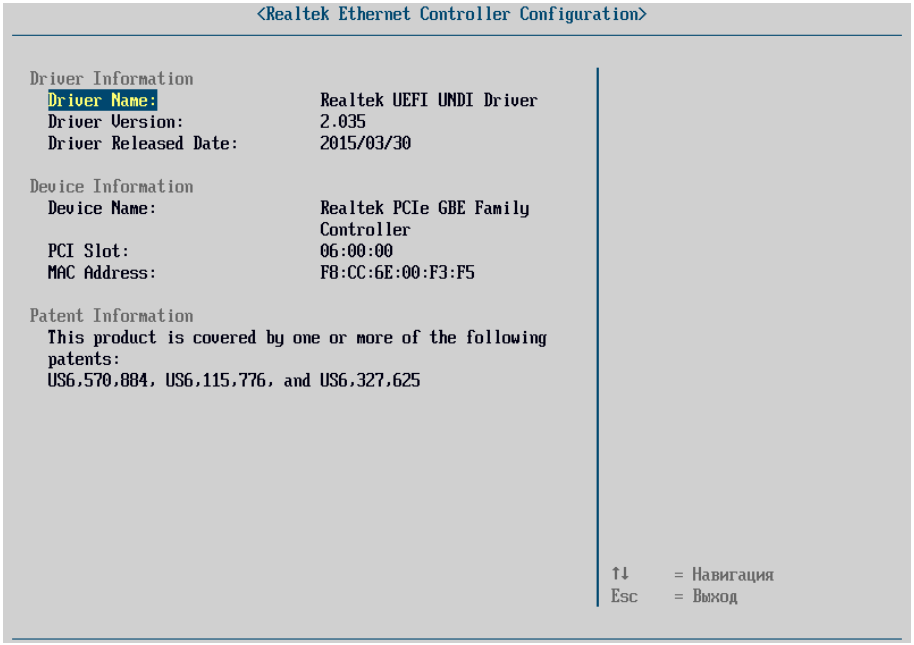

Рисунок 46 – Меню «Драйверы устройств: Скрытые устройства: Параметры»

4.6. Раздел «Параметры МДЗ»

4.6.1. «Пользователи»

Операции управления пользователями Изделия осуществляются из основного пункта меню «Пользователи», которое содержит (см. рисунок 47):

– «Профили пользователей» – в данном разделе отображаются уже созданные пользователи, редактирование профиля уже созданного пользователя доступно из данного пункта меню;

– «Действия с пользователями» – раздел, предназначенный для создания пользователей и экспорта учетных карточек созданных пользователей на USB-носитель;

– «Настройки» – раздел для настроек парольной политики и управления токеном.

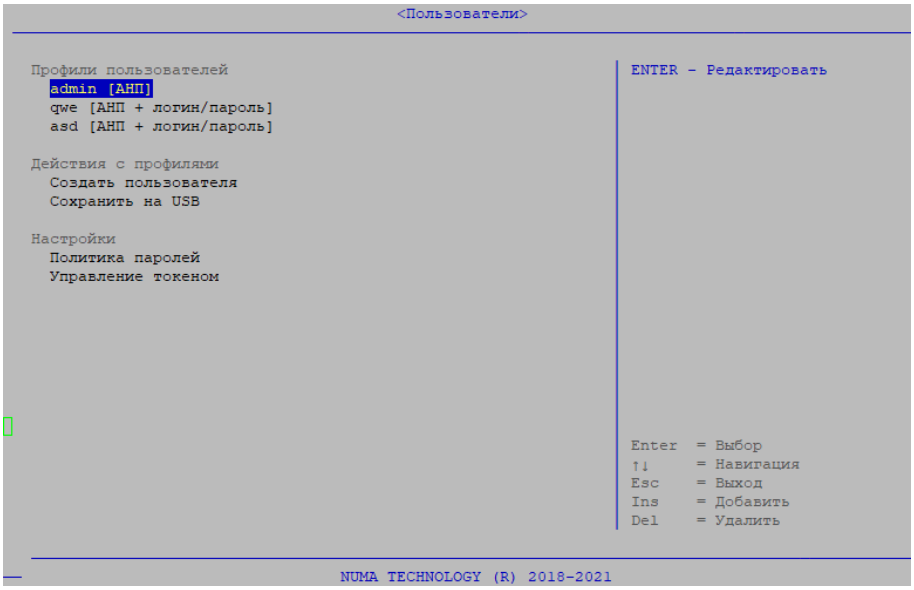

Рисунок 47 – Разделы меню «Управление пользователями»

4.6.1.1. Создание профиля пользователя

Для создания пользователя необходим токен с сформированной ключевой парой и пользовательский сертификат для этой ключевой пары. Процесс работы с токеном описан в пункте 4.6.1.6.

Для создания пользователя необходимо выполнить следующие действия (см. рисунок 48, рисунок 49):

– выбрать пункт меню «Создать пользователя» или нажать клавишу «Ins»;

– заполнить атрибуты пользователя:

а) «Тип авторизации» – «АНП», «АНП+логин/пароль»;

б) «Тип пользователя» – «Пользователь/Администратор»;

в) «Пользователь» – введенное значение служит логином пользователя. Допустимое имя пользователя длиной не менее 3 символов и не более 25 символов;

г) «Установить пароль» – только для типа авторизации «АНП+логин/пароль»;

д) «Ф.И.О. пользователя»;

е) «Контактная информация»;

ж) «Данные сопоставления» – выбрать пользовательский сертификат (см. рисунок 50 и рисунок 51);

з) «Тип сопоставления» – установить флаг для полей, по которым будет осуществляться сопоставление сертификата на АНП (CN, MAIL, DIGEST). Рекомендуется всегда устанавливать флаг на поле DIGEST, так как в отличие от других полей оно уникально, что позволит корректно создать пользователя с типом авторизации «АНП»;

и) «Политики безопасности»:

– «Статус блокировки» – статус меняется двумя способами:

– администратор Изделия с полным доступом может вручную заблокировать учетную запись пользователя, установив соответствующее значение «заблокирован»;

– при активации чекбокса напротив пунктов «Счетчик аутентификации» и/или «Счетчик попыток входа» и по истечении количества попыток аутентификаций и/или количества попыток входа соответственно (см. пункты 4.6.1.4.7 - 4.6.1.4.8) Изделие автоматически блокирует пользователя (см. рисунок 58);

– «Счетчик аутентификаций» – при активации чекбокса Изделие будет подсчитывать все попытки аутентификации (успешные и неуспешные) для определенного пользователя;

– «Счетчик попыток входа» – при активации чекбокса Изделие будет подсчитывать все неуспешные попытки аутентификации для определенного пользователя;

– «Неограниченный период» – при активации чекбокса Изделие будет игнорировать срок действия сертификата АНП, что позволит работать с Изделием вне зависимости от начала/конца действия сертификата АНП. Параметр доступен только для типа пользователя «Администратор» с ролью «Полный доступ». Для обычных пользователей и для администраторов с ролью «Аудит» данный параметр недоступен для активации.

Внимание. Если в Изделии создан только один администратор с полным доступом, то для него рекомендуется отключить параметры «Счетчик попыток входа» и «Счетчик аутентификаций», а также активировать параметр «Неограниченный период» во избежание блокирования администратора при истечении всех попыток аутентификации, неуспешных попыток входа и (или) ненаступлении/истечении срока действия сертификата АНП. Блокирование единственного администратора с полным доступом приводит к блокированию работы всего Изделия. Для восстановления работы Изделия необходимо перейти в «Технологический режим», при котором все настройки будут сброшены (см. пункт 1.4.6).

к) для пользователей типа «Администратор» выбрать значение поля «Роль администратора». Доступны значения «Полный доступ» или «Аудит»;

– сохранить изменения, выбрав пункт меню «Создать».

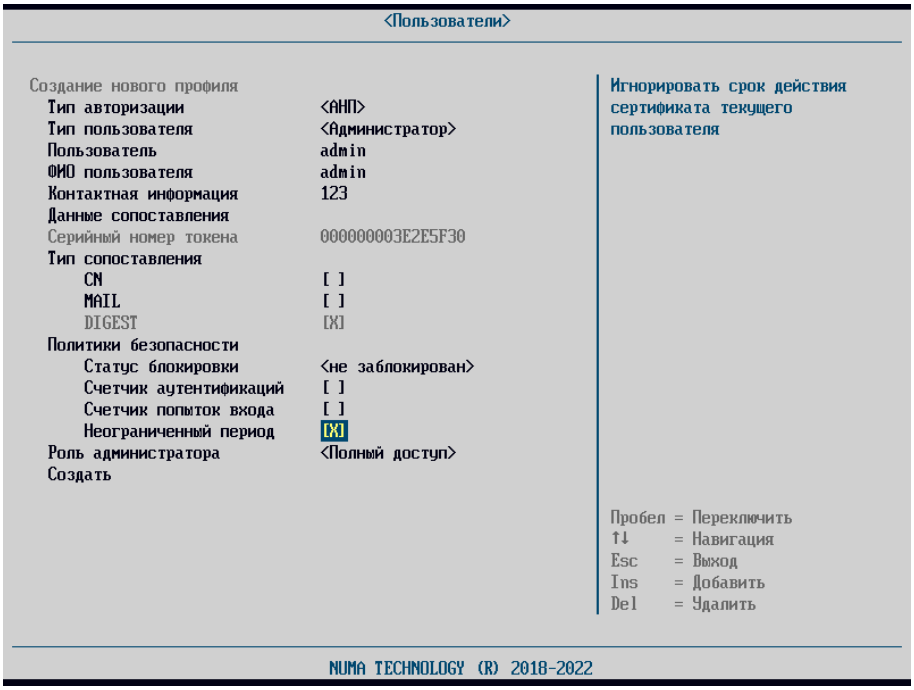

Рисунок 48 – Пример заполнения карточки пользователя «Администратор» с ролью «Полный доступ»

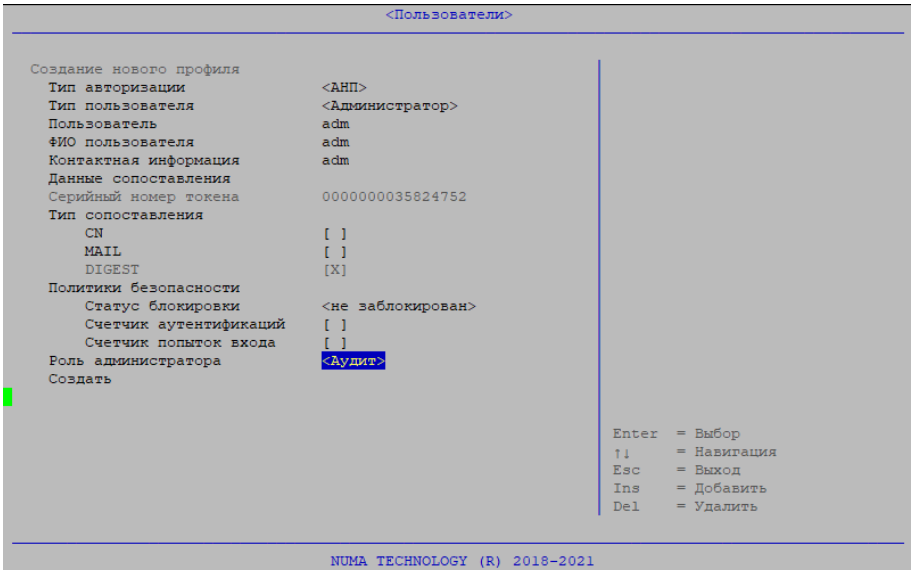

Рисунок 49 – Пример заполнения карточки пользователя «Администратор» с ролью «Аудит»

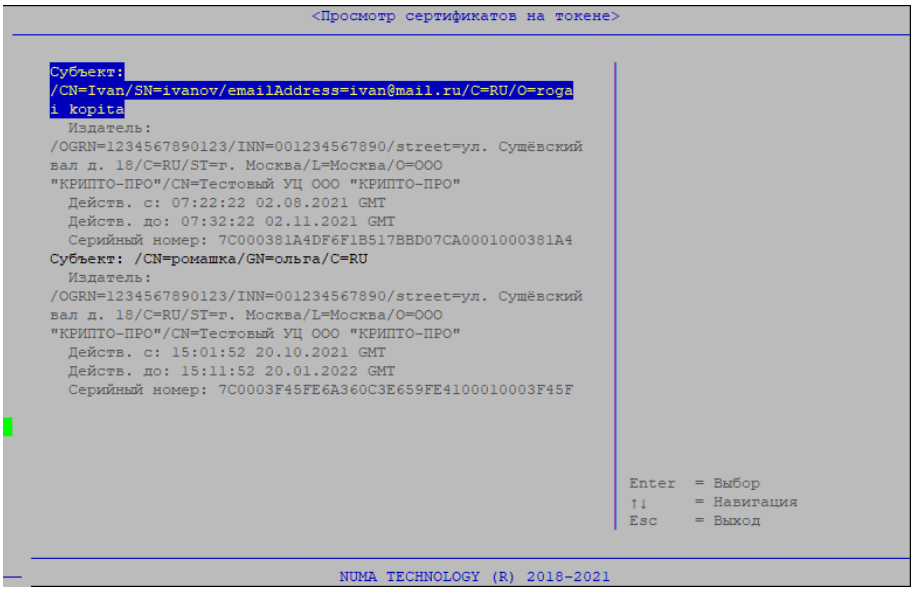

Рисунок 50 – Просмотр сертификатов на токене

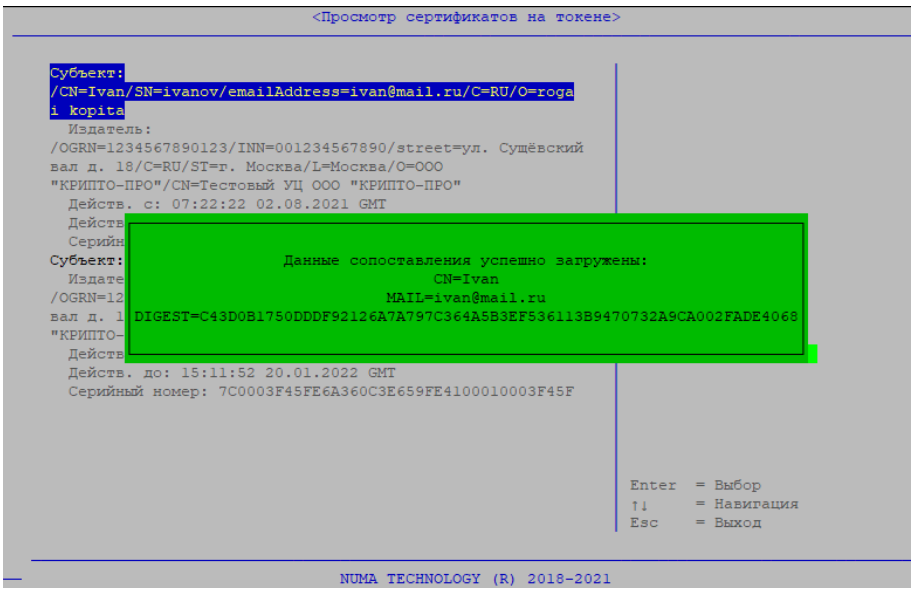

Рисунок 51 – Данные для сопоставления

Если при заполнении карточки пользователя указаны не все атрибуты, то Изделие выдаст сообщение об ошибке и укажет поля, обязательные к заполнению.

4.6.1.2. Просмотр/редактирование/удаление профиля пользователя

Для просмотра/редактирования пользователей необходимо выполнить следующие действия:

– выбрать в разделе «Профиль пользователя» пользователя, чьи данные необходимо просмотреть или отредактировать;

– изменить/просмотреть необходимые данные;

– выбрать пункт «Обновить» для сохранения внесенных изменений или нажать клавишу «Esc» для выхода без сохранения.

При успешном сохранении изменений будет выведено сообщение:

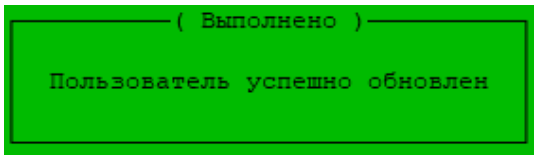

Рисунок 52 – Пользователь обновлен

При попытке обновить данные сопоставления текущего токена, Изделие выведет ошибку:

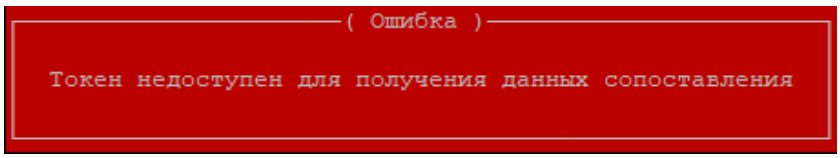

Рисунок 53 – Токен недоступен для получения данных сопоставления

Если изменению подверглась текущая запись администратора, система автоматически будет перезагружена для применения новых значений параметров после предупреждения:

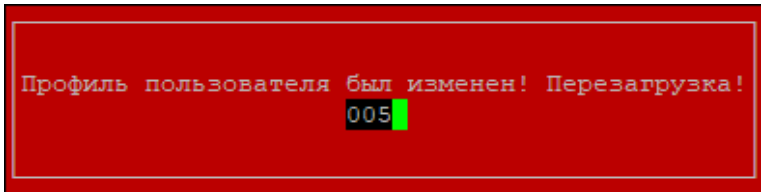

Рисунок 54 – Обновление профиля текущего администратора

Для удаления пользователя необходимо выполнить следующие действия:

– выбрать пользователя, которого необходимо удалить и нажать клавишу «Del» (указанную в списке клавиш навигации в правом нижнем углу экрана);

– в диалоге запроса на подтверждение удаления выбрать клавишу «Y» для удаления пользователя или клавишу «N» для отмены (см. рисунок 55).

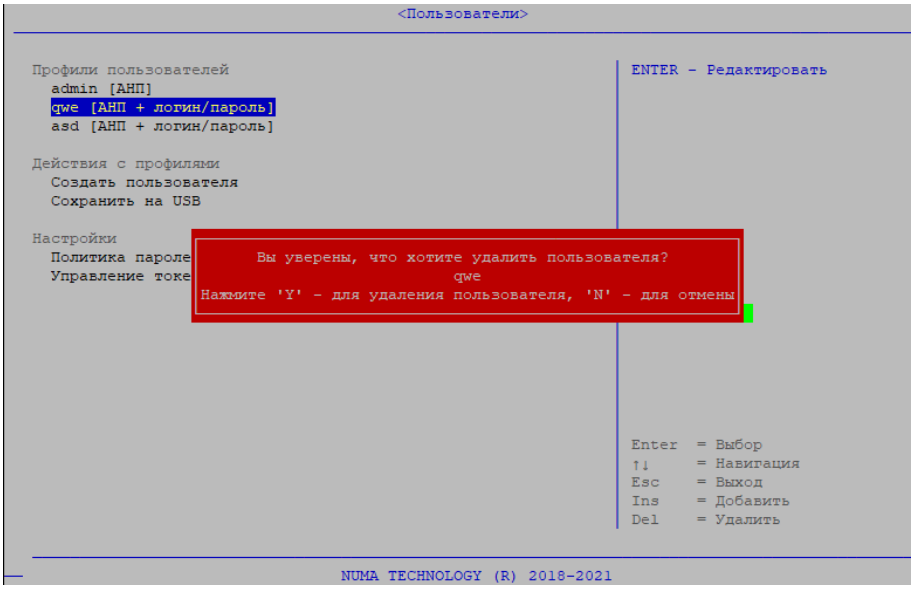

Рисунок 55 – Вид операции подтверждения удаления пользователя

4.6.1.3. Экспорт профилей пользователей

Для сохранения данных пользователей на USB-носитель необходимо выполнить следующие действия:

– подключить USB-носитель;

– выбрать пункт меню «Сохранить информацию на USB». В случае успешного экспорта данных на экране появится сообщение:

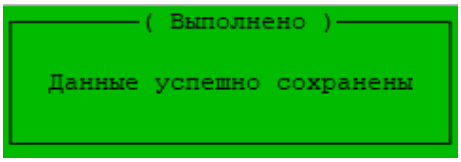

Рисунок 56 – Успешный экспорт профилей пользователей

Примечание. При ошибке экспорта профилей пользователей на USB-носителя необходимо проверить тип файловой системы (поддерживаются USB-носители с файловой системой FAT32).

4.6.1.4. Политика паролей

Изделие поддерживает настраиваемую парольную политику. Для настройки парольной политики необходимо перейти в меню «Пользователи» → «Политика паролей» (см. рисунок 57).

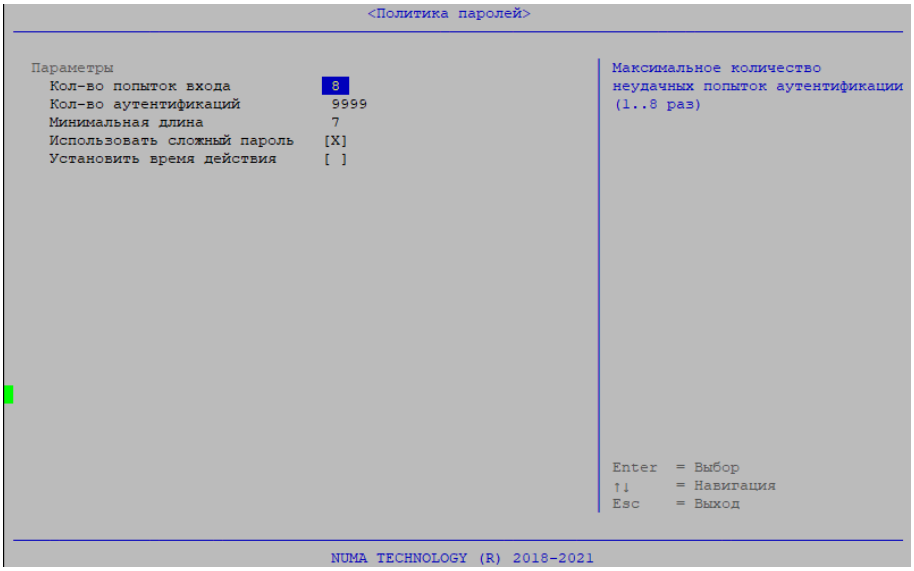

Рисунок 57 – Меню настройки парольной политики

4.6.1.4.7. «Количество попыток входа»

Данный параметр указывает на количество неуспешных попыток аутентификации пользователя и функционирует только при включенном параметре «Счетчик попыток входа» при создании/редактировании учетной записи пользователя.

Параметр может принимать значения от 1 до 8. При превышении заданного значения Изделие блокирует пользователя и подает звуковой сигнал при наличии технической возможности (см. рисунок 58). Заблокированного пользователя может разблокировать только администратор с полными правами вручную через редактирование учетной записи пользователя.

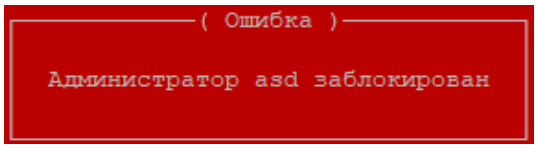

Рисунок 58 – Блокирование пользователя

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести допустимое значение. При попытке ввода числового параметра отличного от допустимых значений Изделие автоматически установит значение равного 8.

Примечания:

1. При отключенном параметре «Счетчик попыток входа» и первой попытке ввода неправильного пароля работа Изделия блокируется на 10 секунд. Вторая неуспешная попытка блокирует работу Изделия на 30 секунд. Третья и последующие неуспешные попытки блокируют работу Изделия на 60 секунд с звуковым сигналом (при наличии технической возможности).

2. Максимальное количество неуспешных попыток ввода PIN-кода АНП задается через утилиту управления токеном.

4.6.1.4.8. «Количество аутентификаций»

Параметр указывает на количество всех попыток аутентификации (успешных и неуспешных) и функционирует только при включенном параметре «Счетчик аутентификаций» при создании/редактировании учетной записи пользователя.

Параметр может принимать значения от 1 до 9999. При превышении заданного значения Изделие блокирует пользователя и подает звуковой сигнал при наличии технической возможности (см. рисунок 58). Заблокированного пользователя может разблокировать администратор с полными правами только вручную через редактирование учетной записи пользователя.

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести допустимое значение. При попытке ввода числового параметра отличного от допустимых значений Изделие автоматически установит значение равного 9999.

4.6.1.4.9. «Минимальная длина»

Параметр указывает минимально допустимую длину пароля пользователя. Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести допустимое значение в диапазоне от 3 до 20 символов. При попытке ввода числового параметра отличного от допустимых значений Изделие автоматически установит допустимое значение числового параметра, ближайшее введенному числу (3 или 20).

4.6.1.4.10. «Сложность пароля»

При включении данного параметра в пароле должны использоваться символы не менее чем из 3 следующих категорий (алфавит пароля 75 символов):

- прописные буквы английского алфавита от 'A' до 'Z';
- строчные буквы английского алфавита от 'a' до 'z';
- десятичные цифры от 0 до 9;
- спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+').

При выключенном параметре «Использовать сложный пароль» ограничения не накладываются.

Для переключения параметра «Сложность пароля» в активное состояние необходимо нажать клавишу «Пробел» или «Enter».

4.6.1.4.11. «Установить время действия пароля»

Параметр отвечает за срок действия пароля при типе авторизации «АНП+логин/пароль».

При включении данного параметра в поле «Время действия пароля» устанавливается числовой параметр, который может принимать значение от 30 до 365 дней.

Для ввода действия пароля необходимо нажать клавишу «Enter» и ввести числовой параметр в диапазоне от 30 до 365. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение числового параметра равного 30.

При выключенном параметре «Установить время действия» ограничения на срок действия пароля не накладываются.

Для переключения параметра «Установить время действия» в активное состояние необходимо нажать клавишу «Пробел» или «Enter».

По истечении срока действия пароля выводится сообщение:

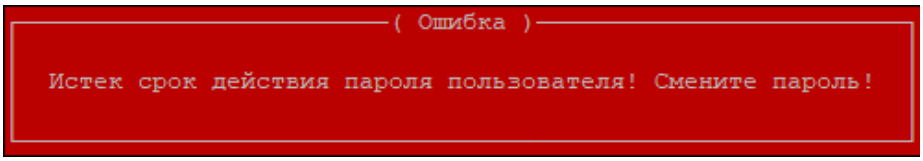

Рисунок 59 – Срок действия пароля истек

Пользователю необходимо ввести новый пароль в диалоговом окне, подтвердить его. После сообщения об успешном обновлении пароля СВТ произведет перезагрузку.

4.6.1.5. Управление токеном

В данном разделе можно изменить PIN-коды администратора, пользователя и импортировать корневой сертификат с токена в хранилище сертификатов.

Примечание. Если к Изделию подключены 2 и более токенов, то при переходе на любой пункт необходимо ввести номер нужного токена из отображаемого списка. Текущий токен обозначен с символом «*».

Для изменения PIN-кода администратора или пользователя в появившемся диалоговом окне «Сгенерировать PIN-код?» необходимо выбрать способ задания нового PIN-кода: для генерации нажать клавишу «Y», для ввода вручную нажать клавишу «N».

При нажатии клавиши «Y», отображается меню генерации PIN-кода (см. рисунок 60), состоящее из трех разделов:

– «Текущее значение» – данное поле отображает новый сгенерированный PIN-код;

– «Опции» – здесь задается количество символов в PIN-коде (от 6 до 32 символов);

– «Действия» – пункт «Сгенерировать» соответственно генерирует новое значение PIN-кода, а при нажатии на пункт «Продолжить» Изделие выводит предупреждающее окно (см. рисунок 61). Для сохранения PIN-кода необходимо нажать «Y», иначе – «N».

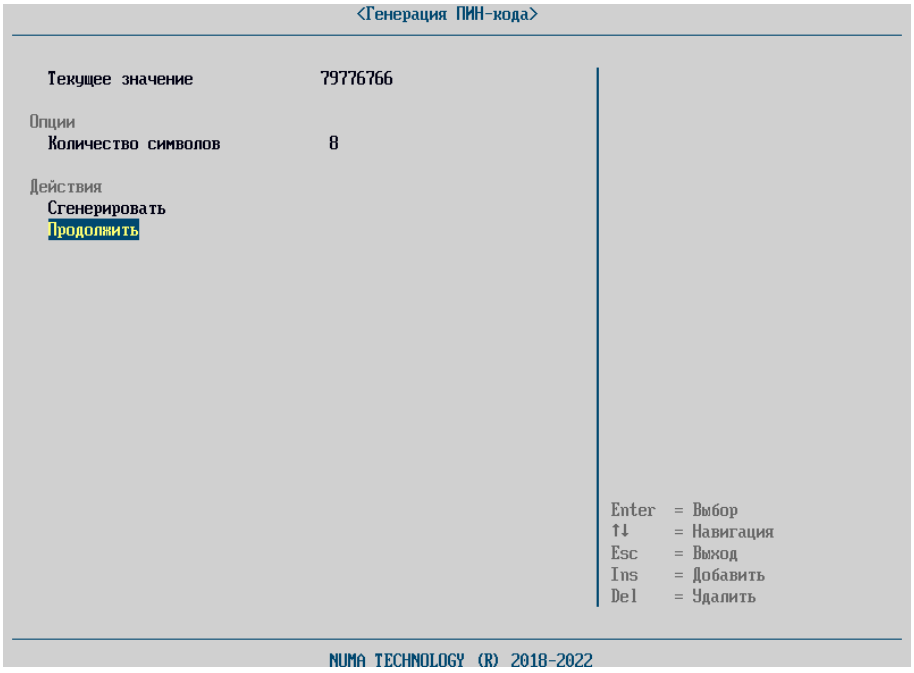

Рисунок 60 – Меню «Генерация PIN-кода»

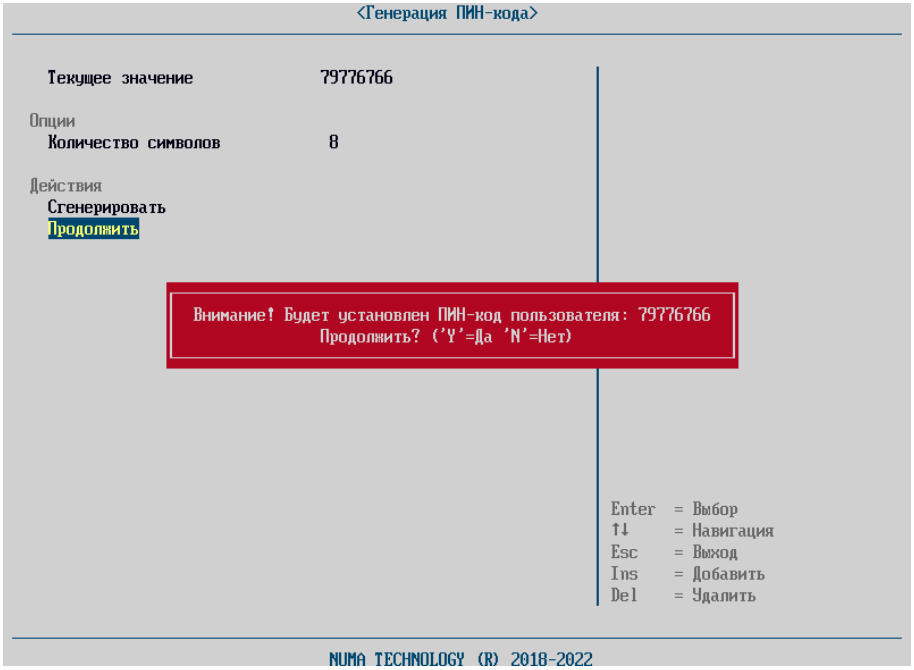

Рисунок 61 – Предупреждающее окно при сохранении сгенерированного PIN-кода

При сохранении сгенерированного пароля необходимо ввести PIN-код администратора в соответствующем окне.

Для импорта корневого сертификата токена необходимо в меню «Просмотр сертификатов на токене» выбрать необходимый сертификат. Данное действие необходимо выполнить перед сопоставлением пользователя с токеном.

4.6.1.6. Работа с токеном

Работа с токеном, включая его инициализацию, должна осуществляться в соответствии с эксплуатационной документацией на СКЗИ.

Список совместимых токенов приведен в Приложении 5.

Для создания пользователя и для работы с Изделием в целом необходимо, чтобы на токене были сформированы ключевая пара и пользовательский сертификат для этой ключевой пары. Пользовательский сертификат должен быть подписан удостоверяющим центром (далее – УЦ). Сертификат УЦ должен быть сохранен на токене и импортирован в Изделие. Также сертификат УЦ можно сохранить на обычный USB-носитель и импортировать через пункт меню «Сертификаты» (см. пункт 4.6.2.1).

Данные действия необходимо выполнить перед сопоставлением пользователя с токеном.

При создании пользователя происходит сопоставление токена с конкретным пользователем. Серийный номер токена прописывается в учетной карточке созданного пользователя.

Внимание. В Изделии к одному пользователю можно сопоставить только один токен. Если в токене содержится несколько пользовательских сертификатов, и администратор привязал их к разным пользователям, то на этапе аутентификации Изделие считывает только один сертификат для одного пользователя. Другие пользователи не смогут авторизоваться с этим токеном.

В случае отсутствия на токене пользовательского сертификата, при попытке в профиле пользователя выбрать данные сопоставления, Изделие сообщит об ошибке (см. рисунок 62), а в журнале аудита появится запись о внутренней ошибке OpenSSL (см. рисунок 63).

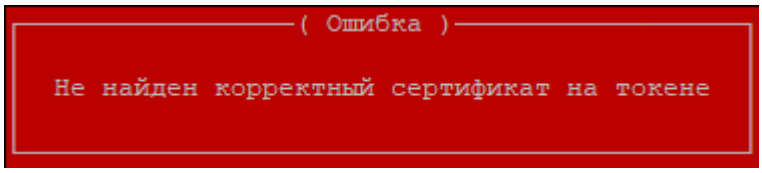

Рисунок 62 – Не найден корректный сертификат

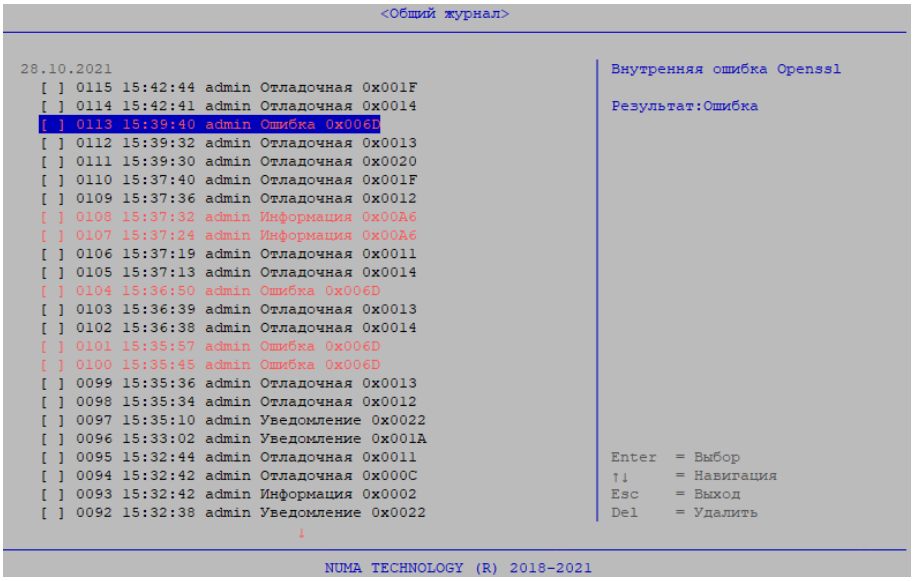

Рисунок 63 – Журнал аудита. Внутренняя ошибка OpenSSL

При установлении уровня журналирования 6 и ниже и подключении незарегистрированного АНП, который не привязан к какому-либо пользователю, в момент запуска Изделия отобразится сообщение «Ошибка! Доступ запрещен!» (см. рисунок 66). В общем журнале аудита появится запись с типом события «Ошибка» (см. рисунок 64), который помимо стандартного формата записи содержит информацию о подключенном АНП: VID/PID и серийный номер.

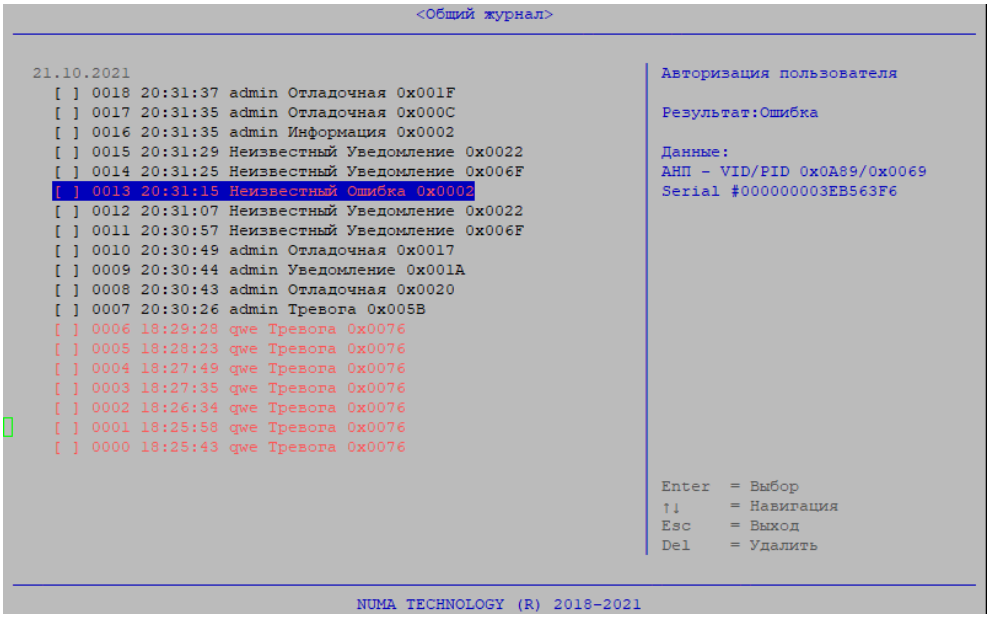

Рисунок 64 – Запись в журнале аудита о незарегистрированном АНП

4.6.1.6.12. Срок действия сертификата

Срок действия пользовательского сертификата можно посмотреть в профиле пользователя и перейдя в пункт «Данные сопоставления». Данное действие невозможно выполнить для текущего пользователя.

По истечении срока действия пользовательского сертификата Изделие выдает сообщения об ошибках (см. рисунок 65 – рисунок 66).

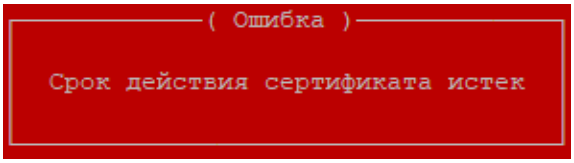

Рисунок 65 – Срок действия сертификата истек

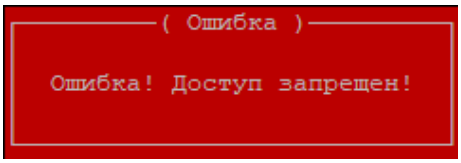

Рисунок 66 – Доступ запрещен

В журнале аудита данное событие отобразится двумя записями: об истечении срока действия сертификата (см. рисунок 67) и о неуспешной попытке авторизации с информацией о подключенном токене (см. рисунок 68).

Примечание. События отображаются при уровне журналирования 6 и ниже (см. пункт 4.6.3.3).

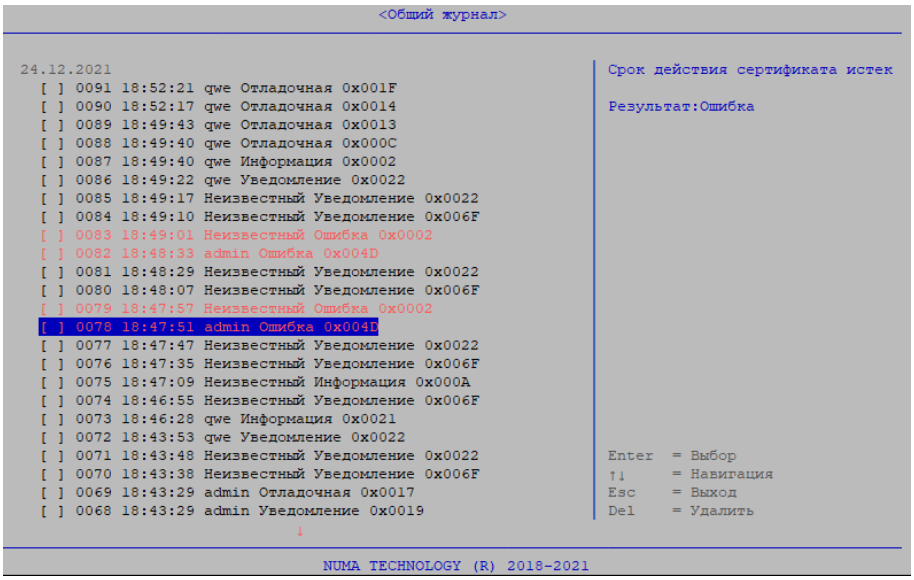

Рисунок 67 – Запись в журнале аудита об истечении срока сертификата

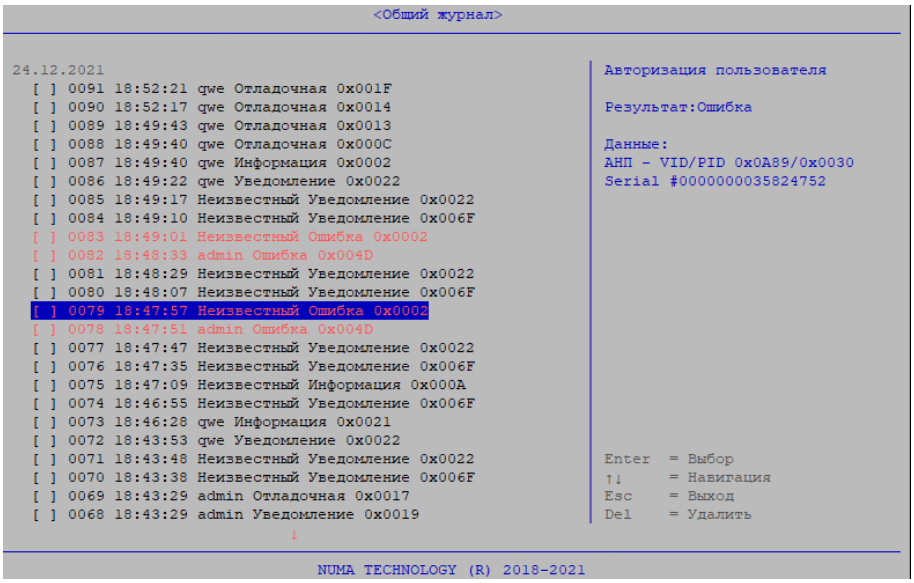

Рисунок 68 – Запись в журнале аудите об ошибке авторизации пользователя

Если срок действия пользовательского сертификата токена еще не наступил, то Изделие выдает сообщения об ошибках: (см. рисунок 69, рисунок 66):

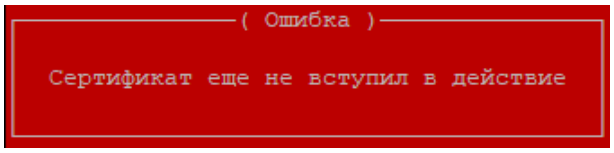

Рисунок 69 – Сертификат не вступил в действие

В журнале аудита данное событие отобразится двумя записями: о невступлении сертификата в действие (см. рисунок 70) и о неуспешной попытке авторизации с информацией о токене (см. рисунок 68).

Примечание. События отображаются при уровне журналирования 6 и ниже (см. пункт 4.6.3.3).

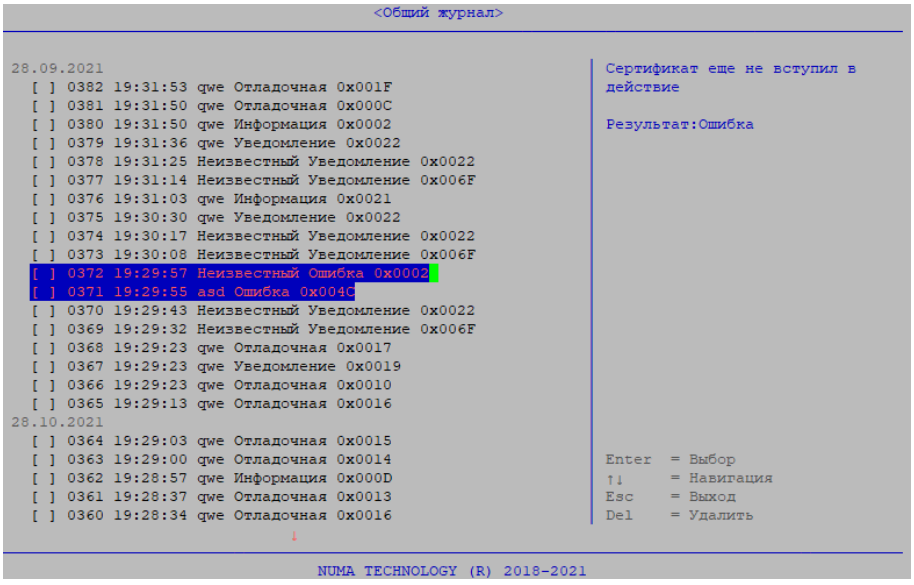

Рисунок 70 – Запись в журнале аудита о невступлении в действие сертификата

4.6.2. «Сертификаты»

Для управления сертификатами пользователей необходимо выбрать пункт меню «Сертификаты» (см. рисунок 71).

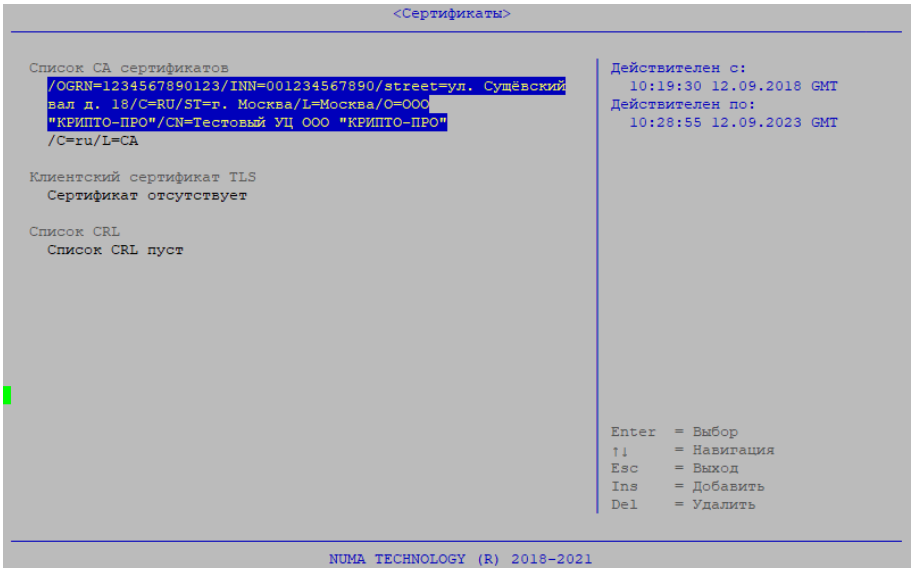

Рисунок 71 – Меню «Сертификаты»

4.6.2.1. Корневые сертификаты

Для аутентификации пользователей с помощью токена необходимо, чтобы был загружен корневой сертификат удостоверяющего центра (далее – CA, сертификат УЦ или CA сертификат) в меню «Сертификаты».

Для загрузки сертификата с USB-носителя необходимо выполнить следующие действия:

– подключить USB-носитель с CA сертификатом;

– перейти в меню «Сертификаты»;

– нажать клавишу «Ins»;

– в запустившемся файловом обозревателе перейти в каталог, содержащий CA сертификат;

– выбрать файл сертификата – будет выполнена загрузка сертификатов и в случае успешной загрузки/обновления сертификатов в строке меню список CA сертификатов будет прописано имя файла FILE_NAME, выбранного в качестве сертификата.

4.6.2.2. Клиентский сертификат TLS

Для загрузки/обновления клиентского сертификата TLS необходимо выполнить следующие действия:

– подключить USB-носитель с TLS-сертификатом;

– перейти в меню «Сертификаты»;

– нажать клавишу «Enter» или «Ins» в разделе «Клиентский сертификат TLS»;

– в проводнике выбрать файл, содержащий сертификат – в случае успешной загрузки/обновления сертификата, в разделе «Клиентский сертификат TLS» будет прописано имя выбранного файла FILE_NAME.

4.6.2.3. Список отозванных сертификатов

Отзыв сертификатов токена осуществляется путем удаления корневого сертификата и/или загрузки списка отозванных сертификатов.

Для выполнения загрузки/обновления списка отозванных сертификатов (CLR) необходимо выполнить следующие действия:

– установить USB-носитель со списком CLR;

– выбрать пункт меню «CRL»;

– нажать клавишу «Enter» или «Ins»;

– в файловом обозревателе выбрать файл, содержащий список отозванных сертификатов – в случае успешной загрузки/обновления сертификата в строке меню «CRL: <FILE_NAME>» будет прописано имя выбранного файла FILE_NAME.

Настройка проверки параметров CRL осуществляется из раздела меню «Дополнительные параметры» (см. раздел 4.6.7).

Если сертификат находится в загруженном списке отозванных сертификатов, то будет выведено сообщение:

```
Сертификат отозван!
```

4.6.3. «Журнал аудита»

Управление журналом аудита осуществляется из меню «Панель управления» → «Журнал аудита» (см. рисунок 72). Полный список регистрируемых событий приведен в Приложение 3.

Журнал аудита имеет два независимых раздела: общий журнал и журнал безопасности.

В журнал безопасности фиксируются все события безопасности о нарушении целостности образов вне зависимости от установленного уровня журналирования. Максимальный объем раздела журнала безопасности 3000 записей.

Раздел «Общий журнал» фиксирует все иные события безопасности в зависимости от установленного уровня журналирования. Максимальный объем общего журнала 500 записей.

После превышения максимального объема записей в разделах журнала работа Изделия блокируется. Для возобновления работы администратору необходимо выгрузить и очистить журнал аудита. В случае если настроена автоматическая перезапись (см. пункт 4.6.3.4), Изделие в автоматическом режиме перезаписывает старые записи аудита на новые при превышении объема раздела журнала аудита.

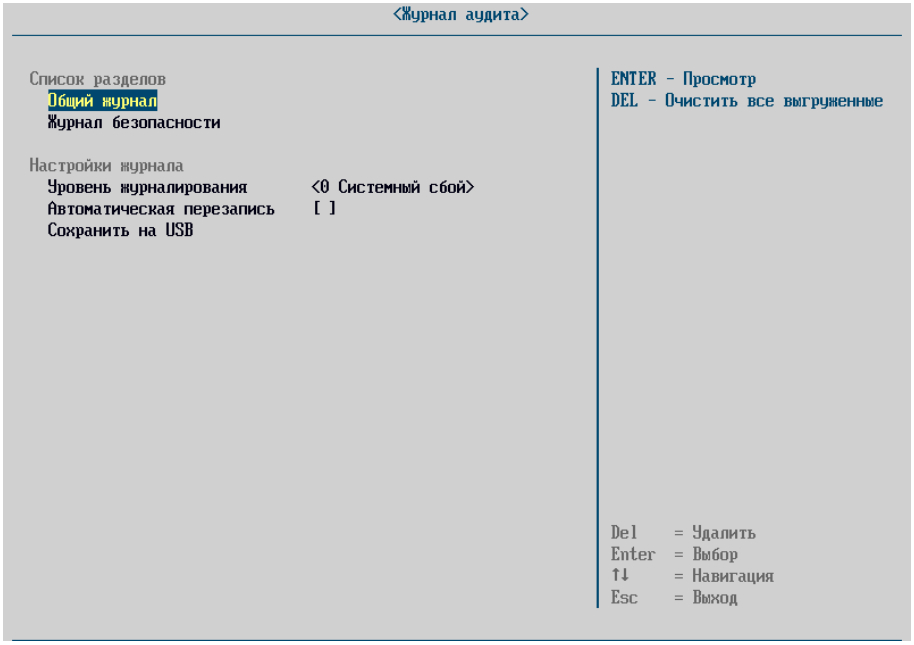

Рисунок 72 – Меню «Журнал аудита»

С записями журналов можно ознакомиться, выбрав соответствующий вид журнала. Записи имеют следующий формат (см. рисунок 73):

– порядковый номер события;
– время наступления события;
– имя пользователя, действиями которого инициировано событие;
– тип события;
– код события;
– описание события (произвольный текст);

– результат попытки осуществления действия («ОК» или «Ошибка»).

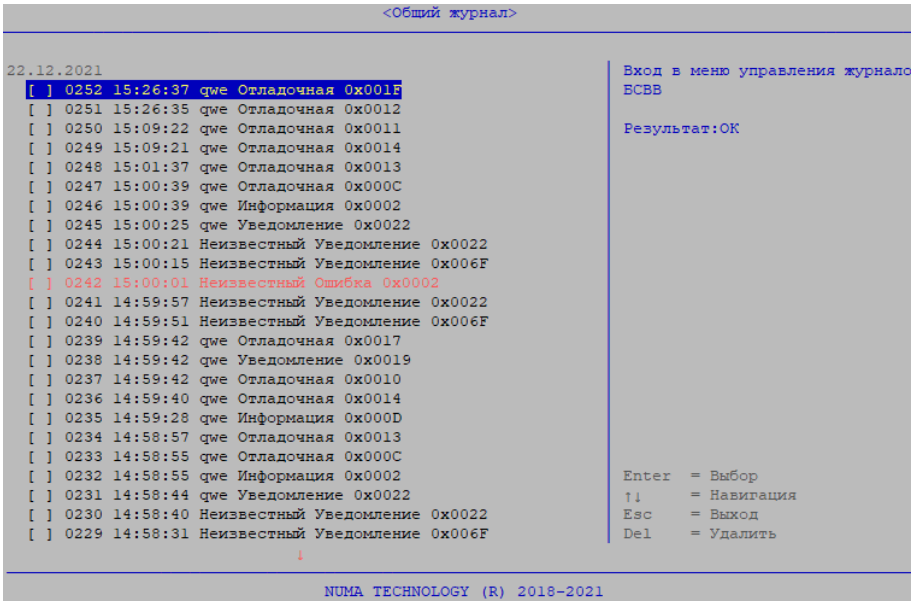

Рисунок 73 – Вид записей общего журнала аудита

4.6.3.1. Удаление записей из журнала аудита

Записи, ранее выгруженные на USB, отмечены «X» и доступны для удаления. Для удаления выделенной записи необходимо нажать «Enter». Если запись не была предварительно выгружена на USB-носитель, удаление будет заблокировано с выводом соответствующего сообщения (см. рисунок 74):

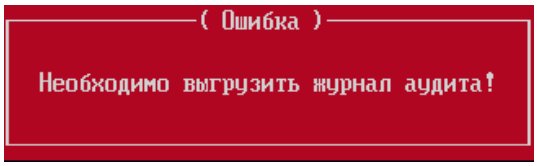

Рисунок 74 – Ошибка удаления невыгруженного журнала

Для удаления уже экспортированных данных (см. пункт 4.6.3.2) из Изделия необходимо подтвердить их удаление путем нажатия клавиши «Y», в случае отмены необходимо нажать клавишу «N», которая вернет в меню «Журнал аудита (см. рисунок 75).

Удаление разделов журнала осуществляется отдельно, при удалении выгруженных записей раздела Общий журнал, записи раздела Журнал безопасности не удаляются и наоборот.

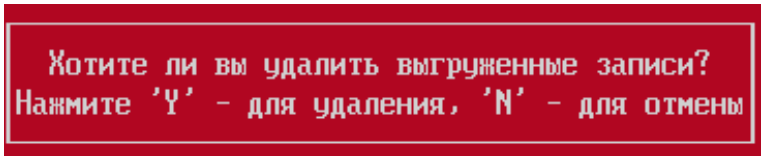

Рисунок 75 – Диалоговое окно удаление уже выгруженных данных

4.6.3.2. Экспорт журнала аудита

Для выгрузки журнала необходимо подключить USB-носитель в СВТ и выбрать пункт меню «Сохранить на USB».

В случае успешной выгрузки данных будет выдано сообщение:

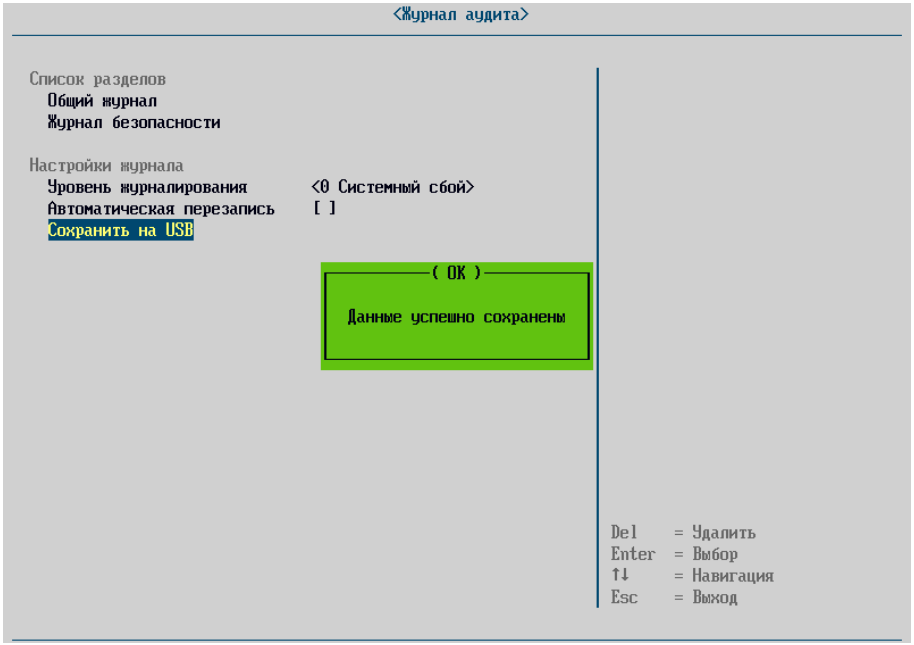

Рисунок 76 – Сообщение об успешном экспорте журнала аудита

В папке «\bios», появившейся на USB-носителе, будет создан файл с записями журнала аудита Изделия.

Имя файла создается автоматически по шаблону: Journal[yy-mm-dd], где yy-mm-dd – текущая дата.

Примечания:

1. Просмотр файла рекомендуется производить в программе «Notepad++».

2. Разделы журнала аудита экспортируются в один файл.

3. При ошибке экспорта на USB-носитель необходимо проверить тип файловой системы (поддерживаются USB-носители с файловой системой FAT32).

После выгрузки журнала аудита в разделе «Общий журнал» появляется запись о выгрузке журнала (см. рисунок 77).

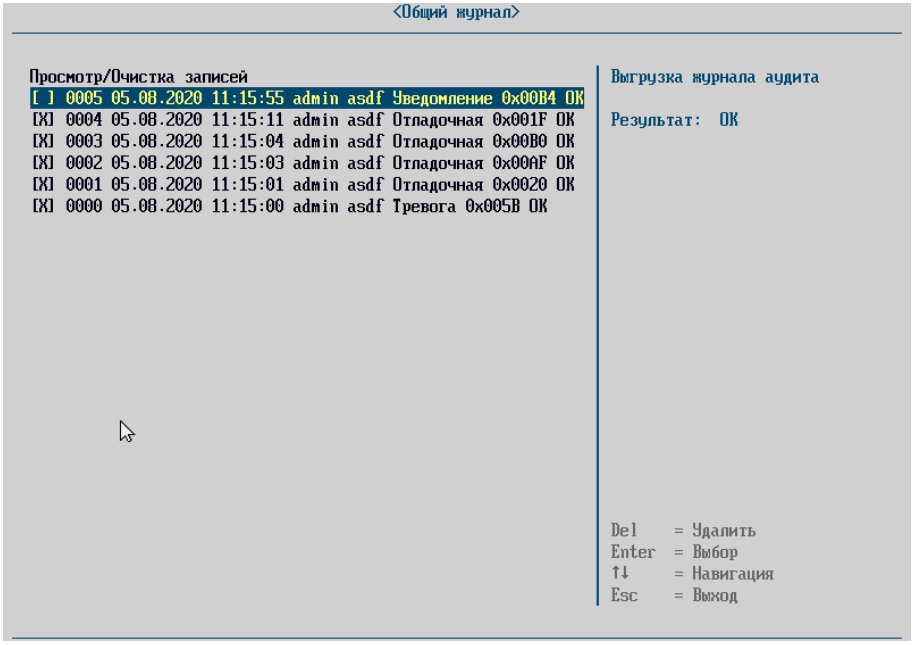

Рисунок 77 – Уведомление о выгрузке журнал аудита

4.6.3.3. Уровень журналирования

В Изделии можно настраивать уровень критичности информации, которая будет записываться в журнал аудита. Уровень критичности может принимать следующие значения:

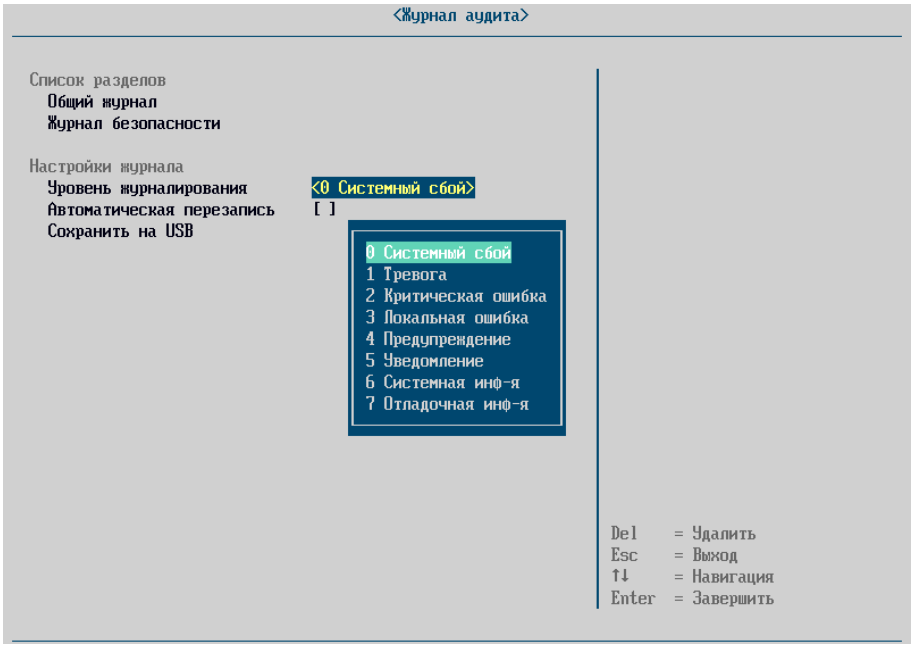

Рисунок 78 – Уровни журналирования

Для того чтобы задать уровень критичности событий, фиксируемых в журнале, необходимо выбрать пункт меню «Управление журналом» и задать значение уровня критичности из выпадающего списка.

4.6.3.4. Автоматическая перезапись

Для возможности автоматически перезаписывать невыгруженные записи при достижении предельного количества записей в журнале Изделия необходимо активировать чекбокс [x] напротив пункта «Автоматическая перезапись».

4.6.4. «Параметры безопасности»

Раздел меню «Параметры безопасности» предназначен для настроек безопасности загружаемых ОС (см. рисунок 79).

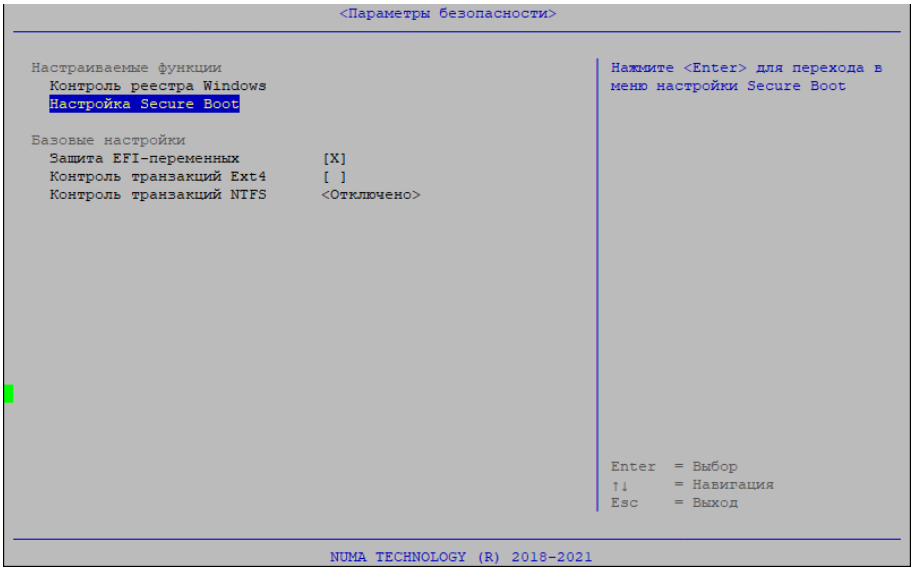

Рисунок 79 – Меню Параметры безопасности

4.6.4.1. Контроль реестра Windows

Раздел «Контроль целостности реестра Windows» позволяет настраивать и просматривать контроль целостности элементов реестров Windows (см. рисунок 80).

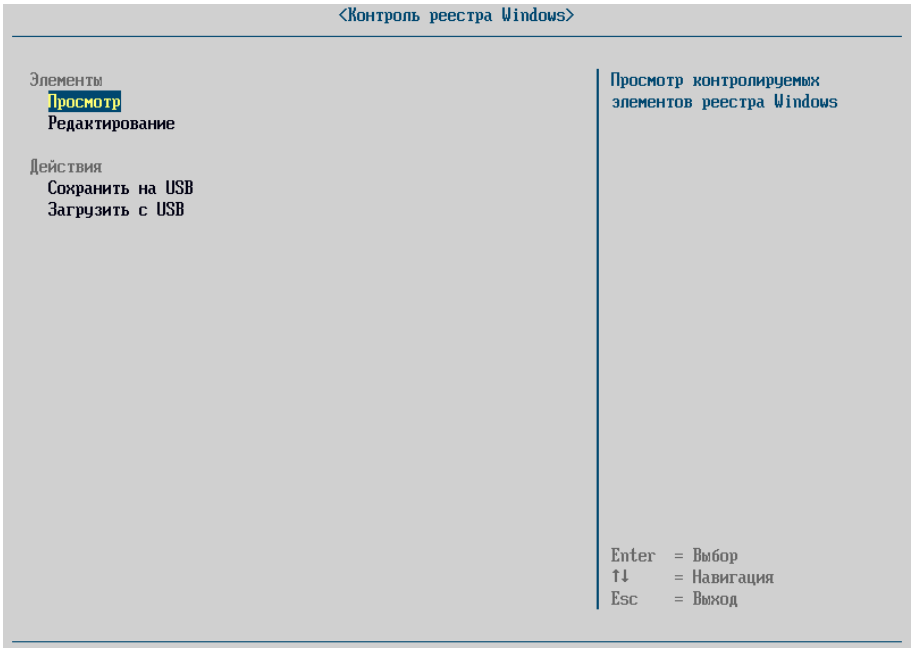

Рисунок 80 – Главное окно управления контролем целостности реестра Windows

Данный раздел доступен для настройки только при наличии профиля загрузки с ОС Windows в режиме EFI.

В случае отсутствия профиля загрузки с ОС Windows будет выдано сообщение об ошибке:

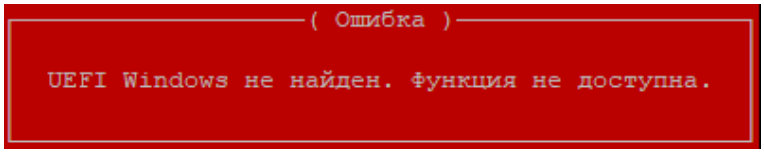

Рисунок 81 – UEFI Windows не найден

4.6.4.1.13. Просмотр контроля целостности

Меню «Просмотр» позволяет выполнить просмотр контролируемых элементов реестра. На рисунке 82 представлено окно просмотра контролируемых элементов реестра Windows.

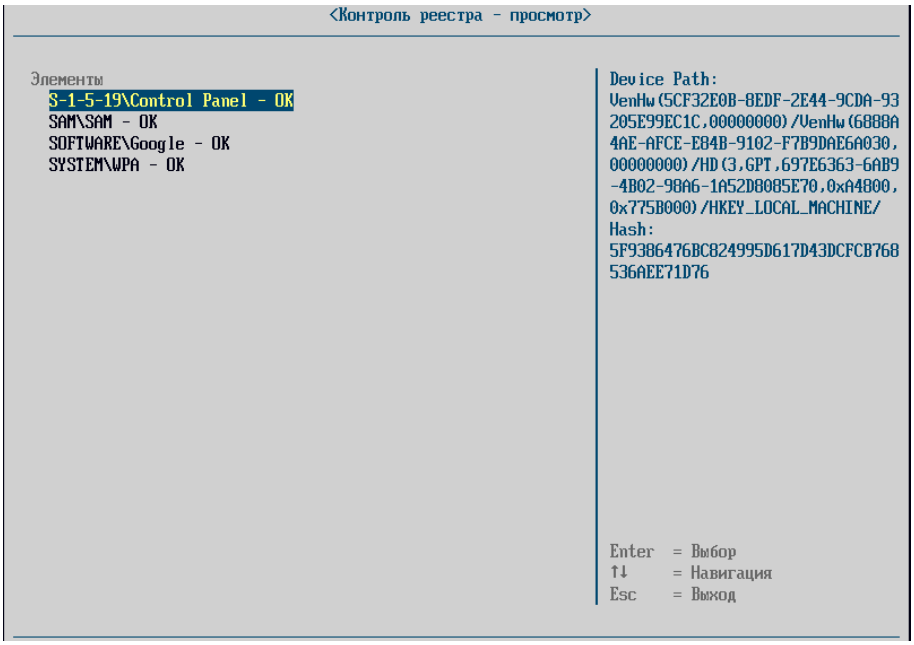

Рисунок 82 – Окно просмотра контролируемых элементов реестра Windows

При входе в меню просмотра у всех элементов, взятых на контроль, автоматически проверяется целостность. Если целостность хотя бы одного контролируемого элемента нарушена, то при входе в меню просмотра будет отображено сообщение об ошибке (см. рисунок 83). В конце имени элементов, целостность которых нарушена, добавляется строка «Ошибка».

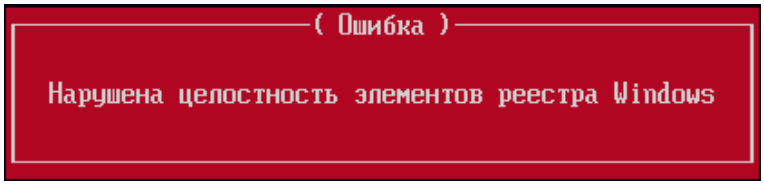

Рисунок 83 – Сообщение об ошибке при нарушении целостности элементов реестра Windows

4.6.4.1.14. Добавление элементов реестра в список контроля целостности

Меню «Редактирование» позволяет управлять списком контролируемых элементов реестра Windows. На рисунке 84 представлено окно редактирования элементов.

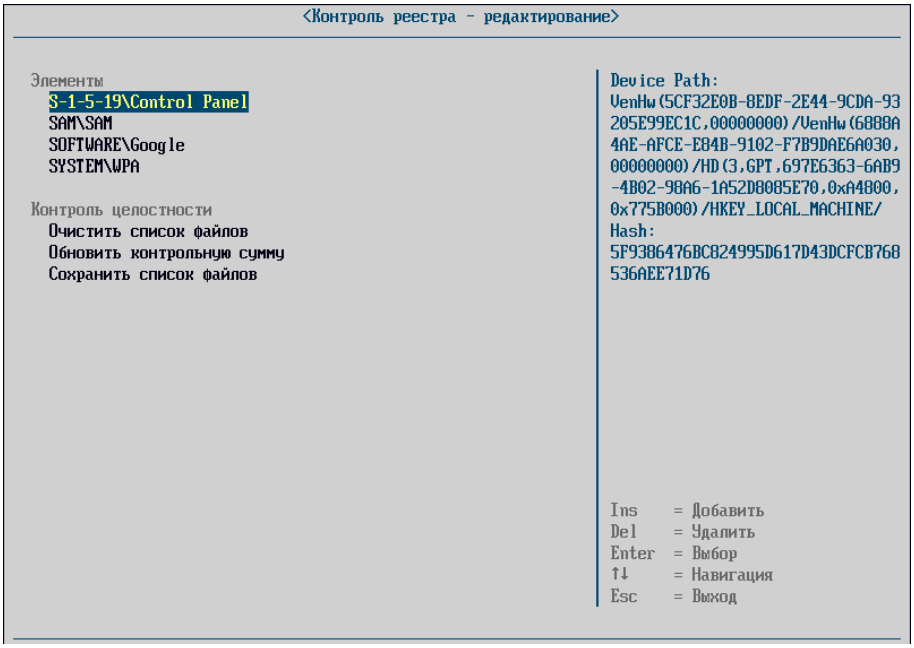

Рисунок 84 – Окно редактирования списка контролируемых элементов реестра Windows

При нажатии клавиши «Ins» появляется окно файлового браузера для добавления элементов реестра в контроль целостности. В окне файлового браузера отображается список разделов жесткого диска, формирующих реестр Windows. Окно файлового браузера представлено на рисунке 85.

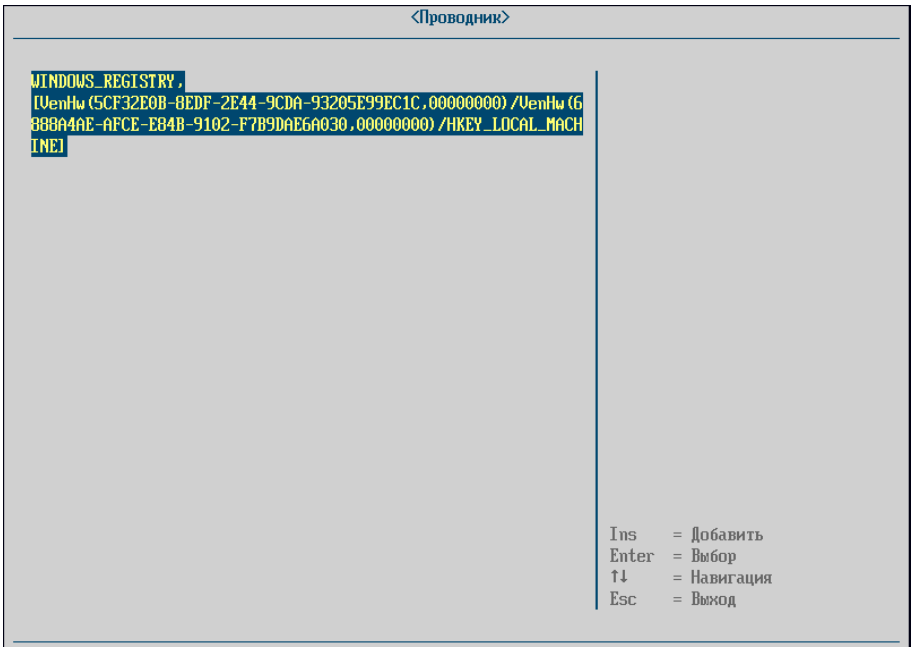

Рисунок 85 – Окно файлового браузера

После выбора устройства, содержащего реестр, становится доступен выбор разделов и параметров реестра для постановки их на контроль. Окно файлового браузера с разделами реестра представлено на рисунке 86.

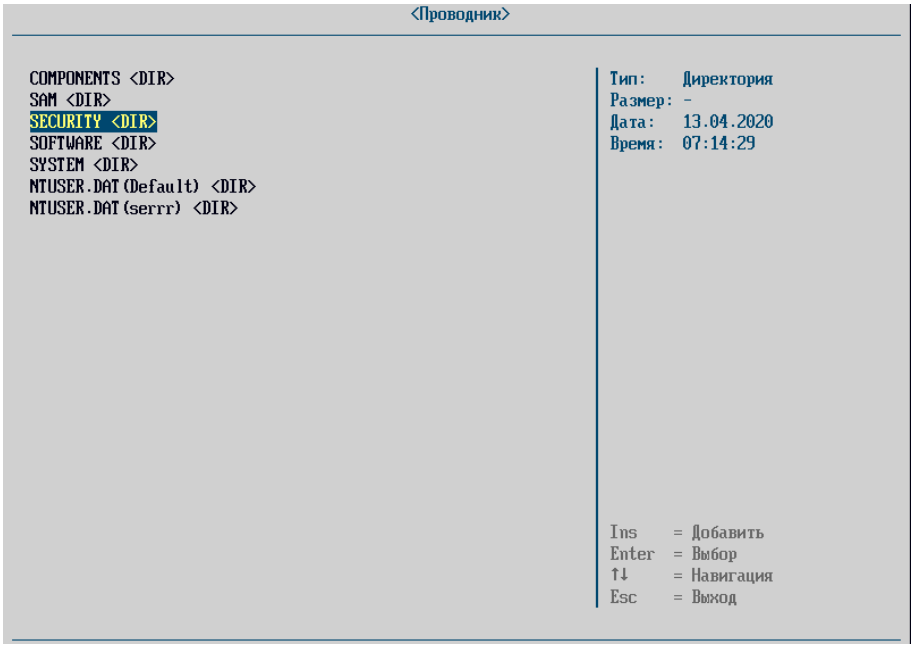

Рисунок 86 – Окно файлового браузера с разделами реестра

Контроль целостности возможен для следующих системных разделов реестра Windows:

- COMPONENTS (расположение \Windows\System32\config\COMPONENTS);
- SAM (расположение \Windows\System32\config\SAM);
- SECURITY (расположение \Windows\System32\config\SECURITY);
- SOFTWARE (расположение \Windows\System32\config\SOFTWARE);
- SYSTEM (расположение \Windows\System32\config\SYSTEM);

– DEFAULT (расположение \Windows\System32\config\DEFAULT);

– S-1-5-19 (расположение \Windows\ServiceProfiles\LocalService\NTUSER.DAT) при наличии. Относится к учётной записи "LocalService";

– S-1-5-20 (расположение \Windows\ServiceProfiles\NetworkService\NTUSER.DAT) при наличии. Относится к учётной записи «NetworkService».

Дополнительно в список контролируемых объектов могут быть добавлены пользовательские разделы реестра Windows (NTUSER.DAT). Данные разделы находятся в каталогах пользователей ОС Windows (каталог \Users\Test\ для пользователя с именем Test).

Так как файлов NTUSER.DAT может быть несколько, то к имени раздела добавляется в скобках имя пользователя для создания уникального имени раздела.

Добавление файлов (параметров) реестра в список контроля целостности осуществляется путем нажатия клавиши «Enter». В случае если выбран каталог (раздел) реестра, то нажатие клавиши «Enter» приводит к отображению списка дочерних элементов (разделов и параметров) выбранного каталога.

Добавление разделов (каталогов) в список контроля целостности осуществляется путем нажатия клавиши «Insert». При этом в выбранном разделе просматриваются все параметры реестра.

В случае контроля каталога (раздела) реестра нарушение целостности наступает в следующих случаях:

– добавление/удаление файлов (параметров) из каталога, добавленного в список контроля целостности;

– модификация существующих файлов (параметров) в каталоге, добавленном в список контроля целостности.

Внимание:

1. Не рекомендуется добавлять в список контроля целостности корневые разделы (COMPONENTS, SOFTWARE, SYSTEM и т.д.) целиком, так как число файлов в разделе может достигать сотен тысяч. При этом добавление корневого раздела нецелесообразно, так как в процессе работы ОС Windows в раздел с большой вероятностью будут записаны данные, что приведет к нарушению целостности.

2. Максимальное число отображаемых элементов в файловом браузере ограничено 2000. При входе в каталог, содержащий большее число дочерних элементов будет показано предупреждение, представленное на рисунке 87.

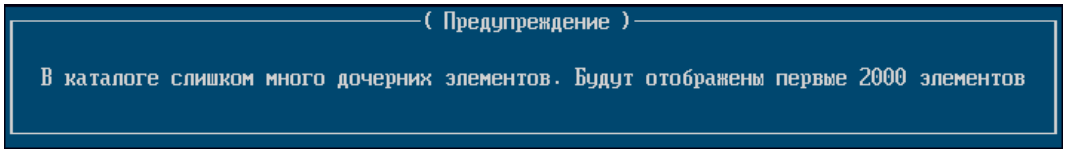

Рисунок 87 – Сообщение, отображаемое при большом числе дочерних элементов раздела реестра Windows

В случае если необходимо добавить неотображаемые элементы каталога, следует воспользоваться функцией импорта списка контроля целостности (см. раздел 4.6.4.1.16).

После выбора элемента реестра выполняется вычисление контрольной суммы элемента, а затем добавление элемента в список контроля целостности. При этом происходит возврат из файлового браузера в меню редактирования списка контроля целостности.

4.6.4.1.15. Редактирование списка контролируемых элементов

Нажатие клавиши «Delete» приводит к удалению выбранного элемента из списка контроля целостности.

Выбор пункта «Очистить список файлов» полностью очищает список контроля целостности.

Выбора пункта «Обновить контрольную сумму» пересчитывает контрольную сумму для каждого элемента из списка контроля целостности.

Выбор пункта «Сохранить список файлов» выполняет сохранение списка контроля целостности в NVRAM.

Максимальное число элементов, которые могут быть добавлены в список контроля целостности: 1024.

4.6.4.1.16. Импорт/экспорт списка контроля целостности элементов реестра Windows

Импорт/экспорт списка контроля целостности осуществляется из главного окна управления контролем целостности реестра Windows.

Для экспорта настроек необходимо подключить USB-носитель, на который будет осуществляется экспорт, перейти в меню «Контроль реестра Windows» выбрать пункт «Сохранить на USB». Список контроля целостности экспортируется в формате JSON в виде:


```
{
  "RegControlObjects": [
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SYSTEM\\CurrentControlSet",
      "HashType": 5,
      "Hash":
"DACC4A629C0E39F186DA19C9A77D1A5548B147E99C432CC36921A3E846616C9F"
    },
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SOFTWARE\\Intel",
      "HashType": 5,
      "Hash":
"F0579F6AA21128777E1A863363D0E26E0B8DC01E9B5BE6156F454B5F9E512455"
    },
    {
      "DevPath": "VenHw(5CF32E0B-8EDF-2E44-9CDA-
93205E99EC1C,00000000)/VenHw(6888A4AE-AFCE-E84B-9102-
F7B9DAE6A030,00000000)/HKEY_LOCAL_MACHINE/",
      "File": "SYSTEM\\RNG",
      "HashType": 5,
      "Hash":
"F840B896DEED410D322C2DBCC75E03FF3C8D698E99B298D9940B9BA89BE28C42"
    }
  ]
}
```

где

– DevPath – путь до раздела, содержащего реестр,
– File – путь до контролируемого элемента внутри реестра,
– HashType – тип контрольной суммы,
– Hash – контрольная сумма (параметр 5 указывается на хеш по алгоритму ГОСТ Р 34.11-2012, 256 бит).

Для импорта необходимо подключить USB-носитель с файлом типа JSON. Выбрать пункт «Загрузить с USB», в открывшемся проводнике выбрать файл. Во время импорта список контроля целостности формируется из входного файла JSON. При это происходит сохранение сформированного списка в NVRAM.

Файл для импорта может быть сформирован вне Изделия. При этом для каждого элемента обязательным будет являться только поле File.

Если поле DevPath не указано, то будет выполняться проверка первого найденного реестра.

Если поле HashType не указано, то будет взят алгоритм по умолчанию (ГОСТ 2012, 256 бит). В целях безопасности HashType со значениями меньше 5 запрещены. Если указано некорректное значение, то будет использоваться алгоритм по умолчанию.

Если поле Hash не указано, то контрольная сумма будет вычислена в процессе построения списка контроля целостности.

Например, корректным будет являться следующий файл JSON:

```
{
  "RegControlObjects": [
    {
      "File": "SYSTEM\\CurrentControlSet"
    },
    {
      "File": "SOFTWARE\\Intel"
    },
    {
      "File": "SYSTEM\\RNG"
    }
  ]
}
```

4.6.4.1.17. Контроль целостности элементов реестра Windows при загрузке ОС

Контроль целостности элементов осуществляется при каждой загрузке ОС. Если целостность элементов реестра нарушена, то выдается сообщение об ошибке:

```
«Ошибка! Нарушена целостность реестра Windows!»
```

Загрузка ОС при этом прекращается, а в журнал аудита добавляется запись.

4.6.4.1.18. Сопоставление содержимого реестра в Windows и в NumaArce

Представление реестра, отображаемое в утилите «regedit.exe» формируется из множества файлов, расположенных на системном разделе ОС Windows.

Физические файлы, участвующие в контроле целостности отображаются в реестре Windows по следующим правилам:

– раздел COMPONENTS недоступен для редактирования с помощью regedit;
– раздел SAM соответствует ветке реестра HKEY_LOCAL_MACHINE\SAM\;

– раздел SECURITY соответствует ветке реестра HKEY_LOCAL_MACHINE\SECURITY\;
– раздел SOFTWARE соответствует ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\;
– раздел SYSTEM соответствует ветке реестра HKEY_LOCAL_MACHINE\SYSTEM\. При формировании раздела SYSTEM создается каталог CurrentControlSet, который является ссылкой на один из каталогов \SYSTEM\ControlSet00x, где x - число, записанное в файле \SYSTEM\Select\Current;
– раздел DEFAULT соответствует ветке реестра HKEY_USERS\.DEFAULT;
– раздел S-1-5-19 соответствует ветке реестра HKEY_USERS\S-1-5-19;
– раздел S-1-5-20 соответствует ветке реестра HKEY_USERS\S-1-5-20.

4.6.4.2. Secure Boot

Параметр Secure Boot включает проверку загрузки только подписанных образов ОС (EFI-модулей), т.е. при включенном значении параметра при попытке загрузить неподписанный образ ОС на экран выводится сообщение. И процесс загрузки завершается.

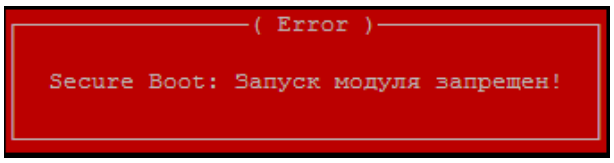

Рисунок 88 – Окно ошибки

Примечание. Для включения параметра Secure Boot необходимо отключить параметр CSM-модуль в меню «Компоненты».

Secure Boot поддерживает 2 режима: «Стандартный» и «Настраиваемый» (Custom Mode) (см. рисунок 89).

При включении стандартного режима устанавливаются все ключи и базы, предустановленные в прошивке. В данном режиме недоступна модификация ключей.

В настраиваемом режиме доступна модификация ключей PK, KEK, DB и DBX. Можно как расширять базы, так и, удалив все стандартные значения, добавлять свои ключи (см. рисунок 90).

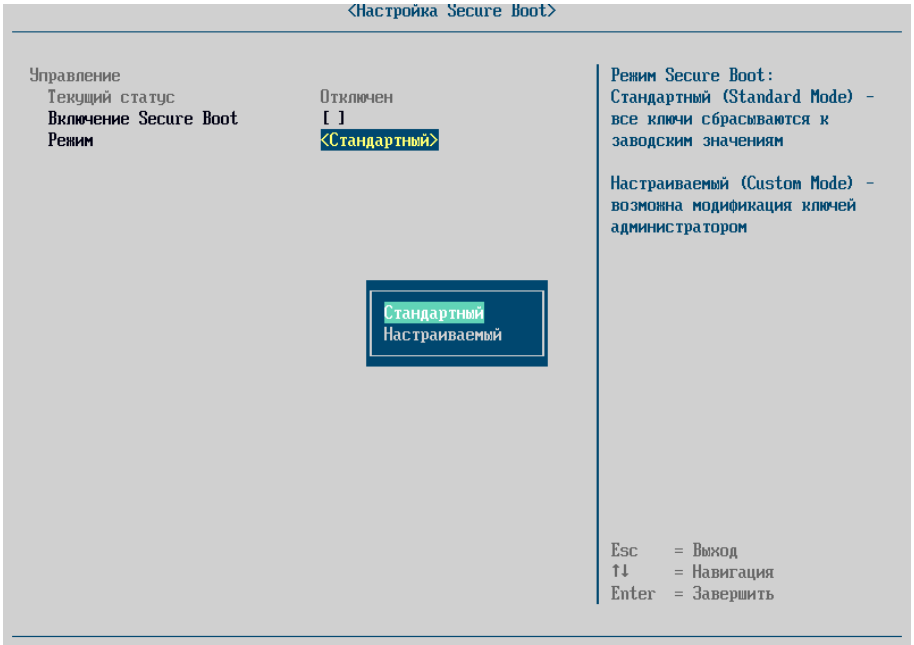

Рисунок 89 – Настройка режима Secure Boot

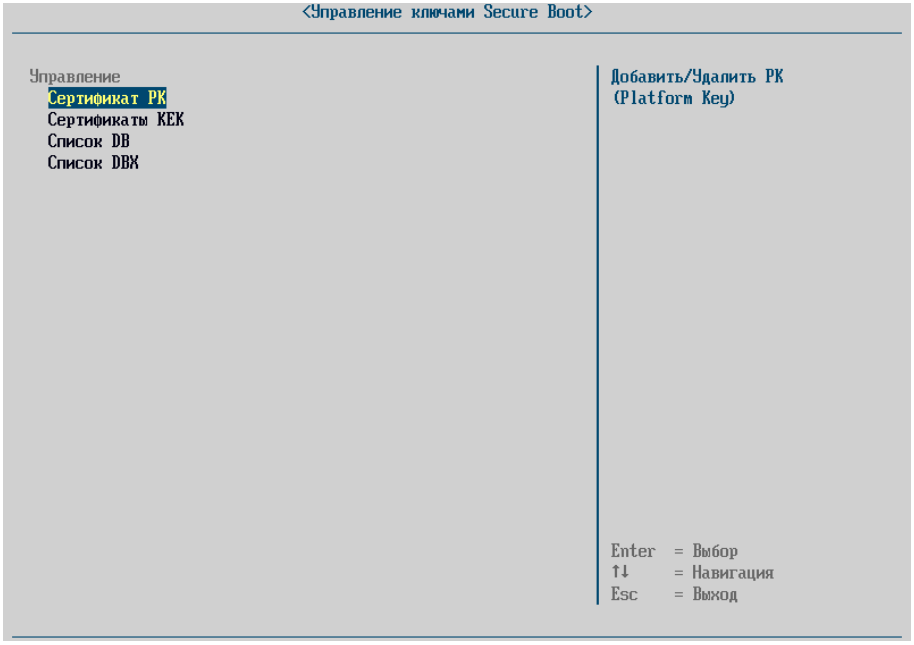

Рисунок 90 – Управление ключами Secure Boot

При выборе настраиваемого режима появляется кнопка входа в форму управления ключами:

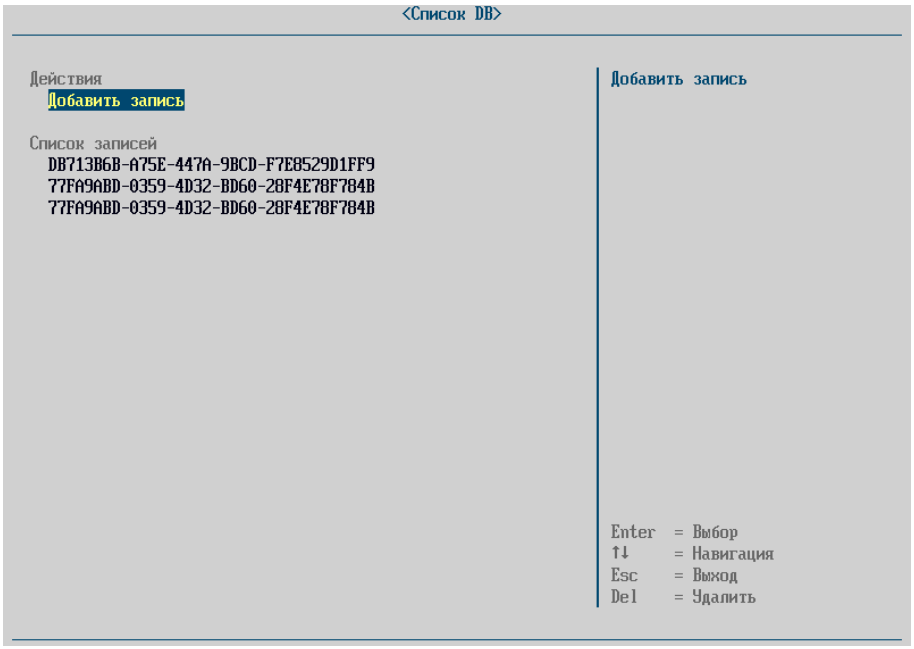

Рисунок 91 – Управление ключами Secure Boot. Список DB

4.6.4.3. Защита EFI-переменных

Параметр включает защиту EFI-переменных от изменений в ОС.

4.6.4.4. Контроль транзакций Ext4

Функция обеспечивает эмуляцию работы сервиса jbd2. При включенном параметре файловая система ext4 будет находиться в восстановленном состоянии.

4.6.4.5. Контроль целостности транзакций NTFS

Функция обеспечивает проверку файловой системы и настройку поведения Изделия при обнаружении незавершенных транзакций файловой системы NTFS. Изделие поддерживает следующие реакции:

– «Отключено» – проверка файловой системы не производится;

– «Предупреждение» – выводится предупреждающее сообщение;

– «Блокировка» – выводится предупреждающее сообщение, блокируется загрузка ОС. Дальнейшая загрузка доступна только после проверки администратором Изделия контрольных сумм.

4.6.5. «Проверка целостности»

Функция проверки целостности вручную предназначена для запуска принудительного контроля целостности бинарного образа Изделия, загружаемых компонент операционной среды, журнала аудита, карточек пользователей.

Для запуска проверки необходимо выполнить следующие действия:

– авторизоваться под учётной записью административного пользователя;

– выбрать пункт основного меню «Проверка целостности».

На экран будет выведено сообщение с результатами проверки всех компонентов (см. рисунок 92).

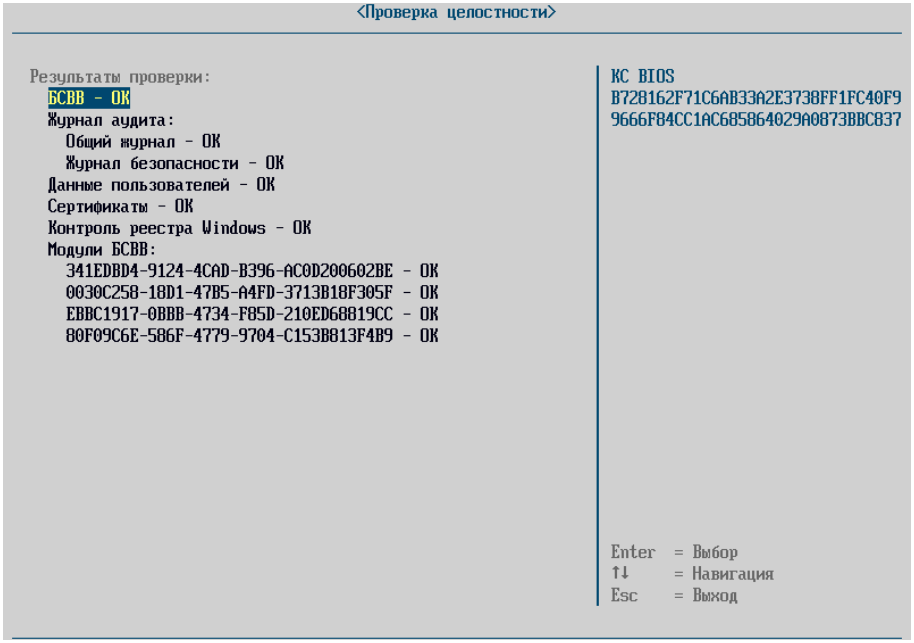

Рисунок 92 – Результат контроля целостности вручную

При наведении клавишами «↓» и «↑» в правой части окна синим шрифтом выводится хеш-сумма выделенной строки.

Управление списком файлов, для которых осуществляется контроль целостности профиля загрузки, доступно из раздела «Редактирование профиля» пункта «Конфигуратор» меню «Панель управления».

Настройка контроля целостности реестра Windows осуществляется согласно разделу 4.6.4.1.17.

4.6.6. «Контроль оборудования»

Контроль оборудования проверяет добавление, удаление, замену аппаратных компонент. Перестановка однотипных устройств в местах подключения (слоты памяти, SATA-порты) также считается нарушением контроля.

Контроль оборудования может функционировать в следующих режимах:

– контроль отключен;

– полный контроль;

– базовый контроль;

– настраиваемый контроль.

В режиме отключения контроля замена/добавление/удаление аппаратных компонентов не проверяется.

При полном контроле проверяется целостность CPU, RAM, HDD, PCI, PCI OpRoms, регионов ME/GBE (при наличии).

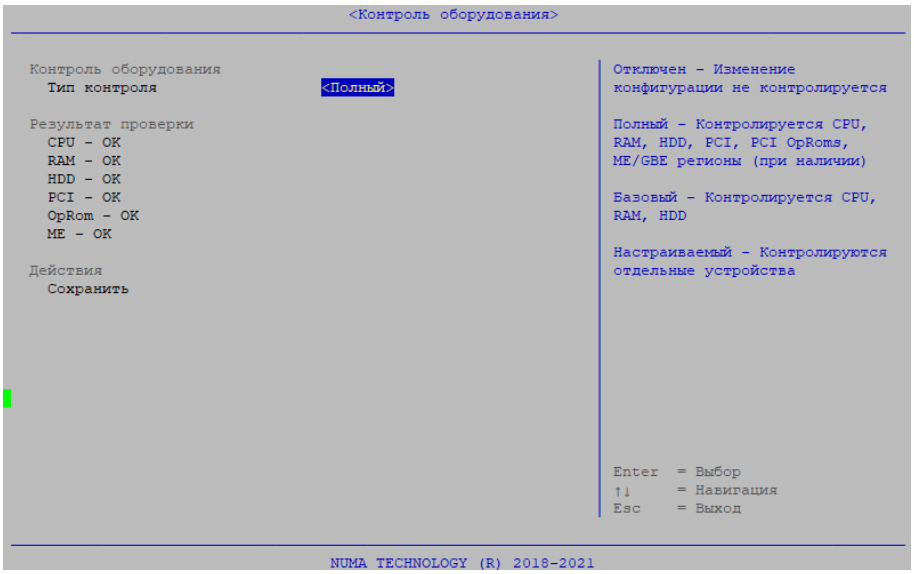

Рисунок 93 – Тип контроля оборудования «Полный»

В режиме базового контроля проверяется целостность CPU, RAM, HDD. Устройства PCI, OpRoms и регионы ME/GBE отключаются от контроля.

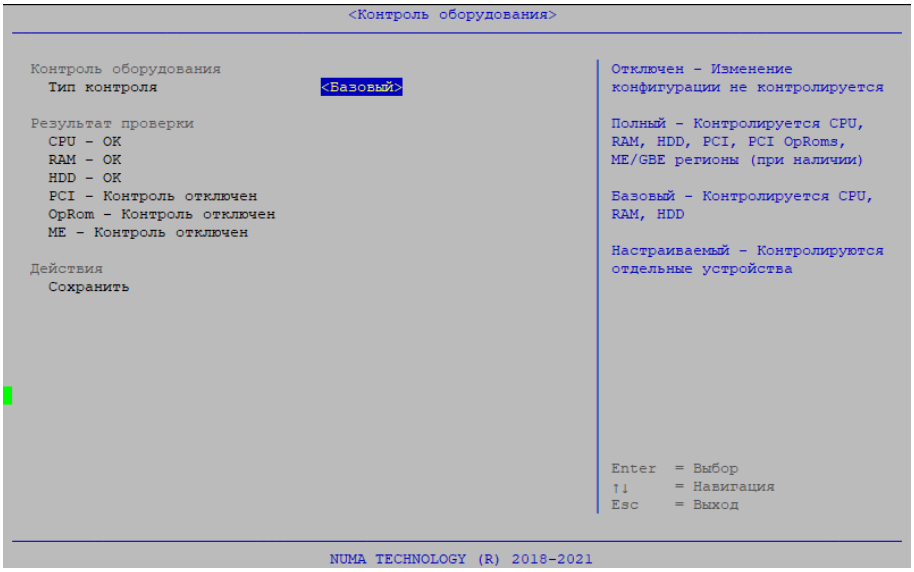

Рисунок 94 – Тип контроля оборудования «Базовый»

Настраиваемый контроль имеет возможность включать/выключать отдельные типы устройств и отдельные устройства из контроля оборудования. В режиме базового и полного контроля такие возможности отсутствуют.

В данном режиме доступна настройка отдельных типов устройств. На рисунке 97 представлено окно настройки параметров устройств PCI.

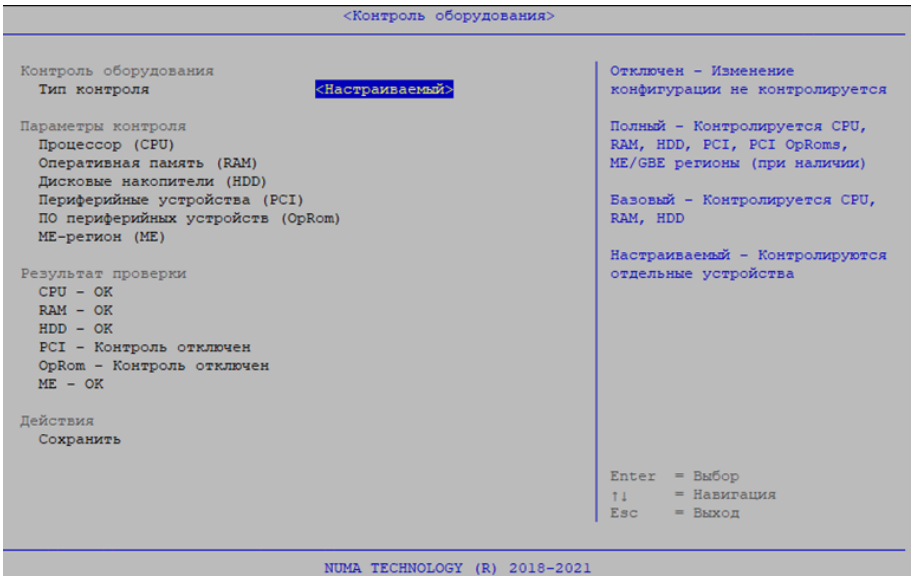

Рисунок 95 – Тип контроля оборудования «Настраиваемый»

Добавление, удаление или перестановка контролируемых устройств приводит к нарушению контроля целостности. При нарушении контроля целостности невозможна загрузка ОС из профилей загрузки.

При попытке загрузки выдается сообщение об ошибке, и загрузка ОС прекращается:

«Ошибка! Нарушена целостность оборудования!»

В режиме администрирования проверка целостности оборудования выполняется при каждом входе в меню контроля оборудования. Если конфигурация аппаратной конфигурации не совпадает с сохраненной, то выдается сообщение об ошибке (см. рисунок 96).

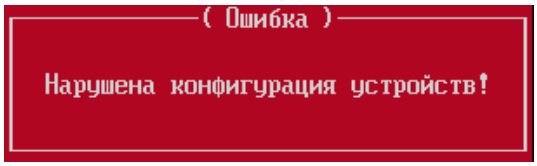

Рисунок 96 – Сообщение об ошибке контроля целостности аппаратной платформы

После входа в меню контроля оборудования можно посмотреть какой тип устройств привел к нарушению целостности.

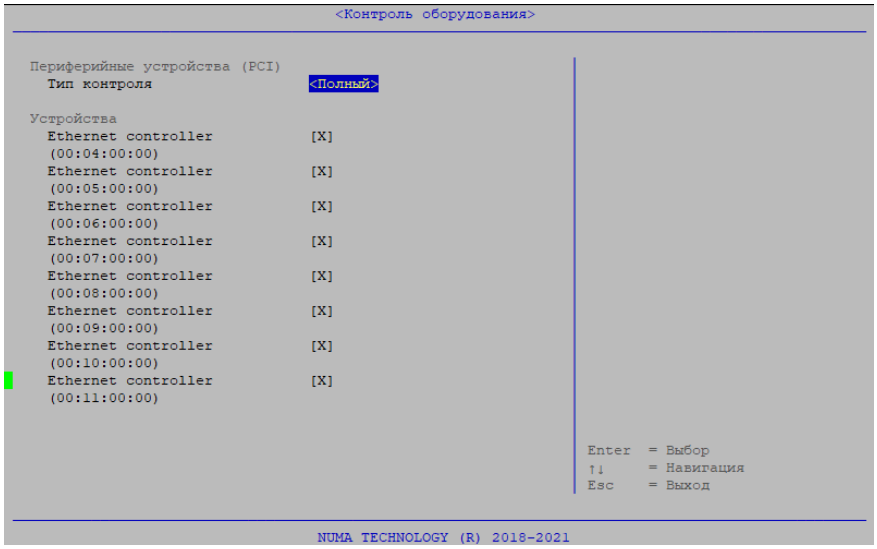

Рисунок 97 – Настройка параметров контроля устройств PCI

Настройка параметров контроля ПО периферийных устройств (OpRom) зависит от настройки параметров периферийных устройств (PCI). Контроль OpRom осуществляется по следующим правилам:

1) если выключен контроль устройств PCI, то устройства OpRom также не контролируются. При этом пункт настройки контроля OpRom недоступен для выбора;

2) если из контроля выключены отдельные устройства PCI, то их OpRom также не проверяется;

3) если устройство PCI проверяется, то при этом можно выключить контроль его OpRom. Для этого необходимо выбрать в пункте настройки OpRom настраиваемый режим и исключить целевое устройство из контроля.

В процессе контроля PCI также проверяются устройства на нулевой шине (устройства PCH). При этом администратору доступны для настройки только внешние устройства PCI (PCI-шина 1 и выше). При проверке целостности PCI игнорируется локация устройства (BUS, DEV, FUNC), так как список шин при подключении/отключении периферийных устройств формируется динамически. Это приводит к ситуации, когда при подключении внешнего устройства меняются BUS уже подключенных ранее устройств. Это делает невозможным реализацию выключения отдельных устройств из контроля целостности PCI. По этой же причине не проверяются устройства типа PCI BRIDGE, так как данные устройства включаются/отключаются динамически (в том числе на нулевой шине) при подключении внешних устройств PCI. Таким образом, в процессе контроля PCI неявно проверяются PCI-устройства Intel, расположенные на нулевой шине. Администратор может выключать из контроля только PCI-устройства, расположенные выше нулевой шины. При подключении/отключении внешних PCI-устройств может меняться BUS, DEV для уже подключенных устройств. Поэтому полная локация устройства носит справочный характер, а фактически устройства сравниваются по Vendor ID, Device ID ClassCode – данные отображаются в области справки при выборе PCI-устройства в контроле оборудования.

После завершения ввода параметров администратор должен выбрать пункт «Сохранить» на главной странице контроля оборудования. При этом будет выполнена запись параметров в NVRAM SPI-flash.

При сохранении контрольная сумма конфигурации пересчитывается и записывается в NVRAM. При каждом входе в настройки контроля оборудования и при каждой загрузке ОС из конфигурации вычисляется текущая КС аппаратной конфигурации и сравнивается с расположенной в NVRAM.

4.6.7. «Дополнительные параметры»

В меню Дополнительные параметры можно настроить параметры отзыва сертификатов (см. рисунок 98).

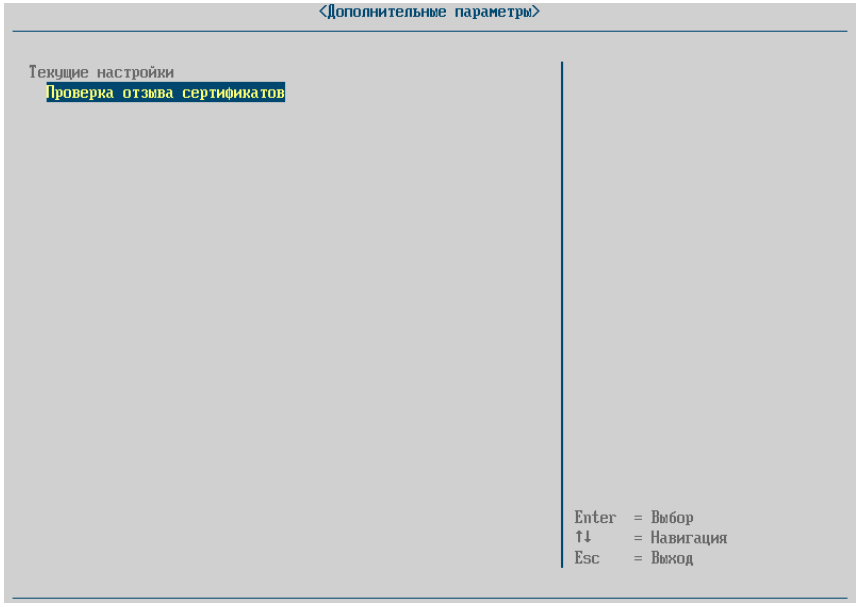

Рисунок 98 – Меню дополнительные параметры

Проверка отзыва сертификата осуществляется с загруженного списка отзыва сертификатов. В зависимости от настроек доступна проверка всей цепочки или только пользовательского сертификата (см. рисунок 99).

Параметр «Отсутствие CRL» контролирует политику проверки сертификатов токена пользователей при включенной проверке сертификата пользователя по CRL. Если данный чекбокс включен, то в случае отсутствия подходящего CRL сертификат пользователя будет считаться доверенным.

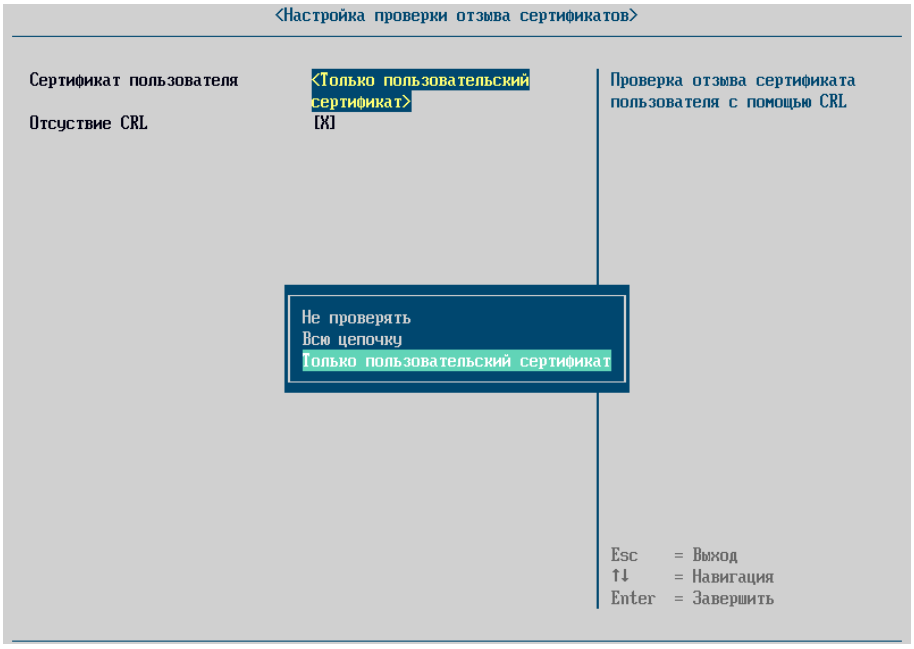

Рисунок 99 – Настройка проверки отзыва сертификатов

4.7. Раздел «Информация»

4.7.1. «Монитор состояний»

Примечание. Данное меню отображается в зависимости от типа СВТ, на которое установлено Изделие.

Данное меню позволяет отслеживать состояние и скорость оборотов датчиков вентилятора, а также определять значение температуры центрального процессора, температуру материнской платы, подключаемых внешний датчиков и уровень заряда СВТ (см. рисунок 100).

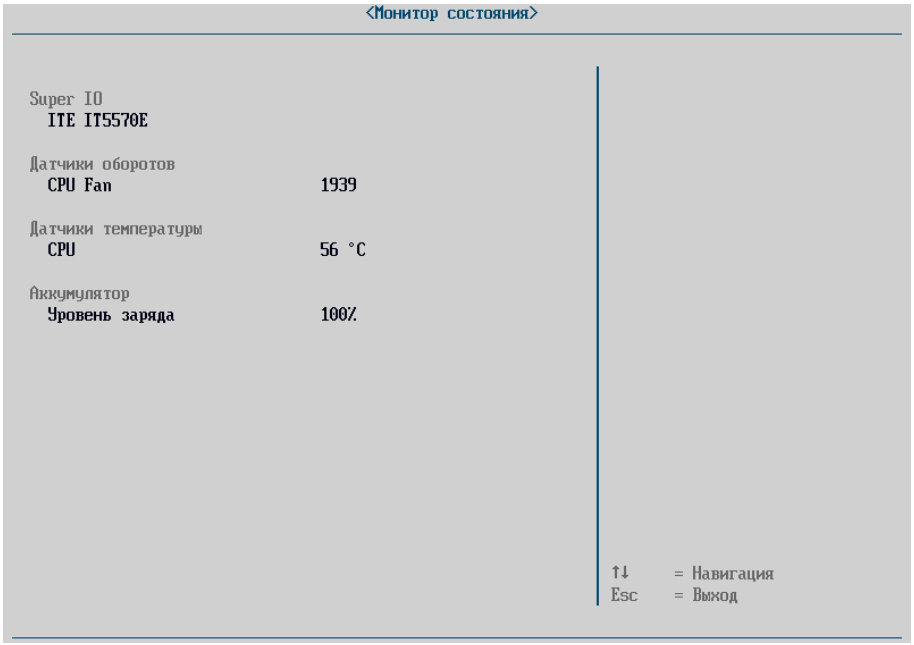

Рисунок 100 – Меню «Монитор состояний»

4.7.2. «Системная информация»

Выбрав пункт меню «Системная информация», можно получить сведения о платформе, параметрах процессора, устройствах в SATA портах, уникальном идентификаторе, адресах сетевых адаптеров (см. рисунок 101).

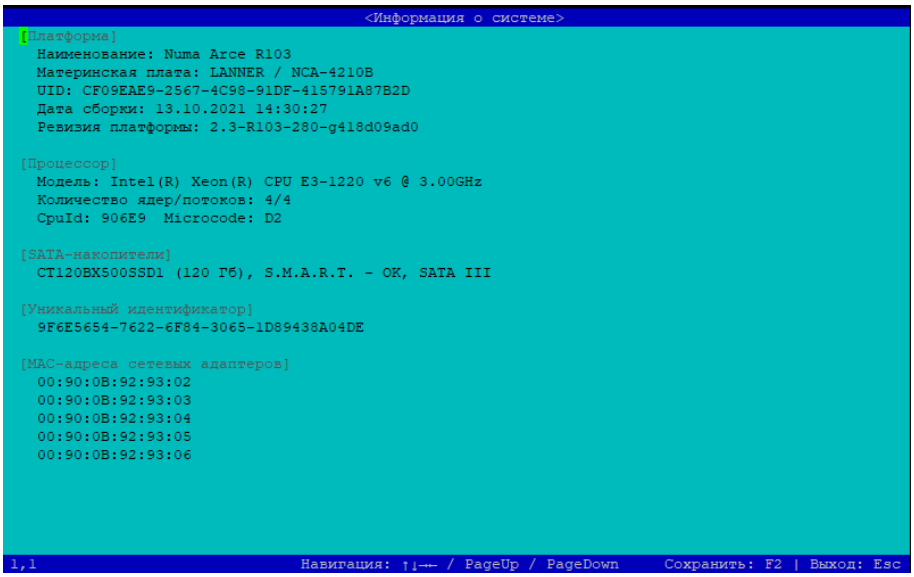

Рисунок 101 – Информация о системе

4.7.3. «Версия ПО»

Меню «Версия ПО» показывает текущую версию ПО, лицензионное соглашение, информацию о лицензии и позволяет обновить версию ПО с USB-носителя (см. рисунок 102).

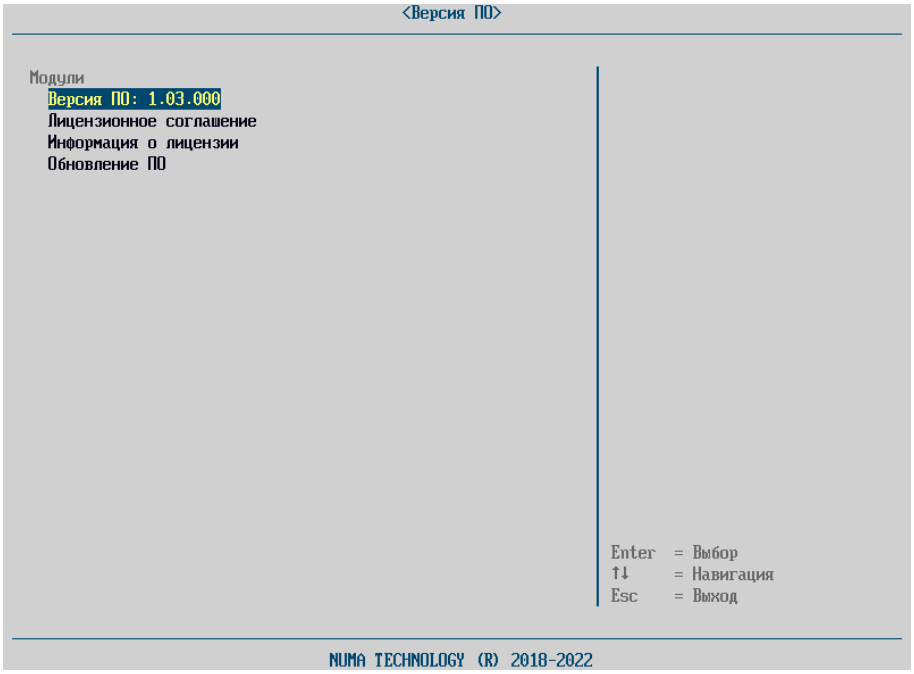

Рисунок 102 – Раздел «Версия ПО»

При просмотре версии ПО (см. рисунке 103) отображается следующая информация:

– информация о платформе;
– информация о среде функционирования Изделия;
– информация об Изделии.

Данная информация необходима для обращения в сервисную службу.

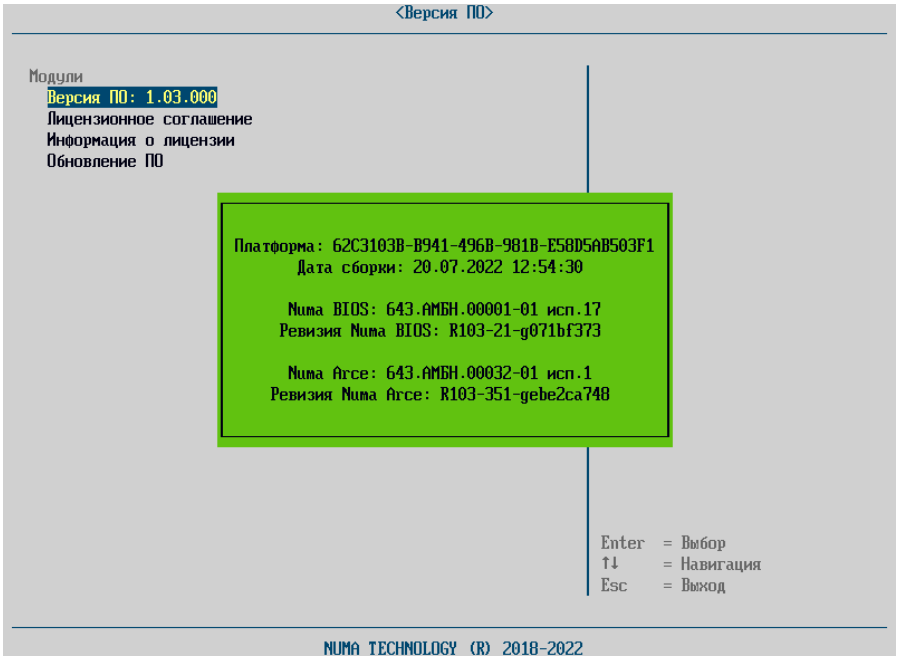

Рисунок 103 – Версия ПО

4.7.3.1. Лицензионное соглашение

При выборе этого пункта на экран выводится текст лицензионного соглашения. Пролистывание текста доступно как построчно, с помощью клавиш «↑↓», так и постранично, с использованием клавиш «PgUp/ PgDown».

4.7.3.2. Информация о лицензии

Форма имеет вид, представленный на рисунке 104, и выполняет функции:

– отображения текущего состояния лицензии;

– управления лицензией.

Раздел «Информация» отображает поля:

– «Тип лицензии» с допустимыми значениями: Обычная (бессрочная) или Пробная (ограниченный срок действия);

– «Функция»: МДЗ;

– «Поддержка LDAP»: Нет.

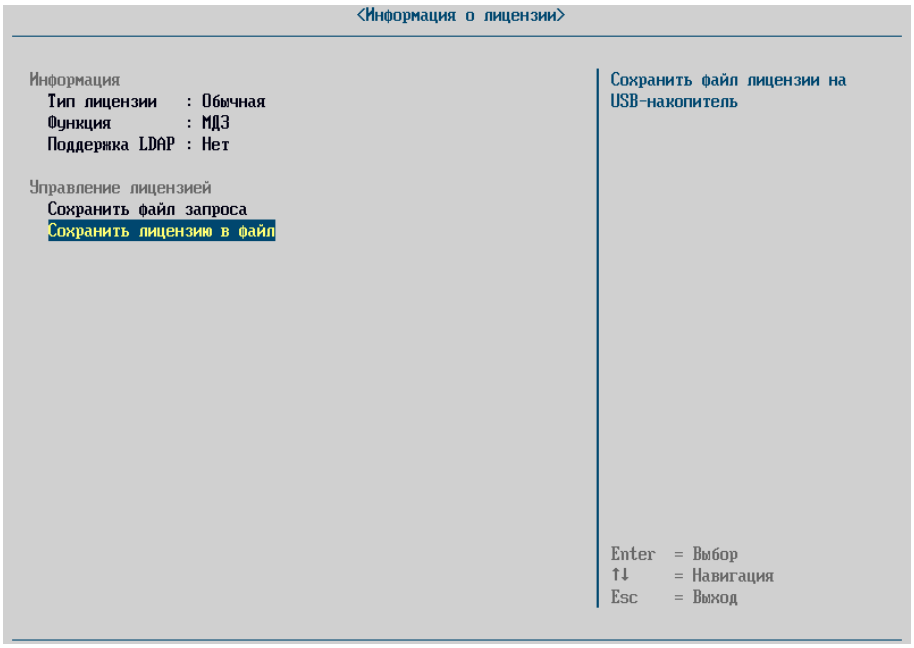

Рисунок 104 – Меню информация о лицензии

В разделе «Управление лицензией» можно сформировать xml-файл запроса для получения лицензии, например, при замене пробной лицензии на постоянную.

О необходимости такой замены, Изделие информирует таким сообщением:

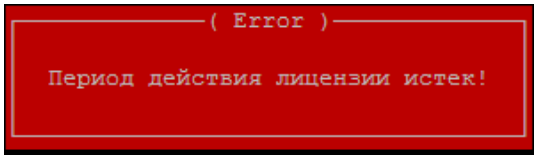

Рисунок 105 – Окно ошибки истекшей лицензии

Для этого необходимо предварительно подключить USB-носитель, выбрать пункт «Сохранить файл запроса», нажав клавишу «Enter». Изделие сформирует файл вида numa_license_req_xxx.xml, где xxx – уникальный идентификатор платформы, отображаемый в «Информации о системе».

Файл запроса содержит всю необходимую информацию о конкретном экземпляре платформы для формирования лицензии. По завершении формирования файла, Изделие информирует пользователя следующим сообщением:

```
Запрос лицензии успешно сохранен
```

Сохраненный файл запроса необходимо отправить в сервисную службу ООО «НумаТех».

На основе файла запроса формируется файл лицензии вида – XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.p12. Данный файл помещается на USB-носитель, подключаемый к СВТ. В меню «Информация о системе» необходимо выбрать пункт «Загрузить файл лицензии». В случае отсутствия USB-носителя, Изделие проинформирует об ошибке «USB-носитель не найден».

После подключения USB-носителя необходимо перейти в меню «Панель управления» → «Версия ПО» → «Информация о лицензии» и выбрать пункт «Загрузить файл лицензии». В появившемся проводнике выбрать файл лицензии для данной платформы и нажать клавишу «Enter». В случае успеха выводится сообщение об успешной установке лицензии:

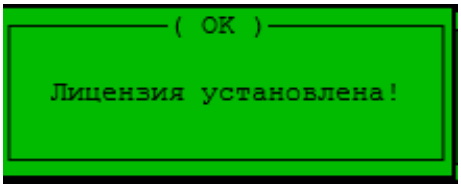

Рисунок 106 – Успешная установка лицензии

В случае если выбран файл от неверной платформы, появляется сообщение об ошибке:

```
Проверка лицензии завершилась с ошибкой!
```

4.7.3.3. Обновление БСВВ

Внимание! Не допускается выключение питания во время обновления.

Для обновления необходимо выполнить следующие действия:

1) выгрузить журнал аудита согласно пункту 4.6.3. Изделие не позволит начать обновление до выгрузки всего журнала аудита на USB-носитель;
2) записать бинарный файл прошивки на USB-носитель и подключить к СВТ;
3) включить СВТ;
4) в меню «Панель управления» выбрать пункт «Версия ПО» → «Обновление БСВВ»;
5) в открывшемся списке файлов выбрать файл прошивки и нажать «Enter»;
6) в появившемся окне подтвердить проведение обновления;
7) в появившемся окне «Обновить EFI-переменные?» нажать клавишу «N» для сохранения преднастроенных параметров БСВВ или клавишу «Y» для возврата Изделия к заводским настройкам;
8) подтвердить действия нажатием «Enter» в следующем окне;
9) начнется запись образа прошивки в флеш-память.

По окончании обновления будет показано сообщение (см. рисунок 107) и СВТ будет выключен.

Рисунок 107 – Сообщение об успешном обновлении Изделия

При выборе несоответствующего данной аппаратной платформе бинарного файла обновления Изделие выдаст сообщение об ошибке (см. рисунок 108).

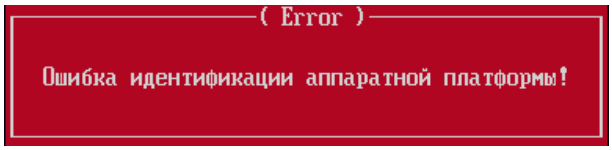

Рисунок 108 – Сообщение о некорректном файле обновления Изделия

5. СООБЩЕНИЯ АДМИНИСТРАТОРУ

5.1. Режим начальной инициализации

Сообщения, которые могут появиться при подготовке к работе Изделия, приведены в таблице 2.

Таблица 2 – Сообщения в режиме подготовке к работе Изделия

Сообщение	Описание	Действие
«Нарушена целостность БСВВ»	Произошло вмешательство извне в бинарный образ БСВВ	Уведомить администратора и ответственного за безопасность информации
«Введите начальный пароль»	Режим подготовки к работе	Ввести логин и пароль
«Пароль не верен»	Режим подготовки к работе	Повторно ввести пароль
«Создание карточки администратора»	Режим подготовки к работе	Задать карточку администратора
«Ошибка создания карточки администратора: не хватает данных»	При создании карточки администратора не были введены обязательные поля	Задать все поля данных
«Ошибка создания карточки администратора: данные сопоставления не верны»	Ошибка при задании данных сопоставления АНП	Задать верные данные
«Восстановление настроек с внешнего носителя»	Функция восстановления настроек	
«Ошибка восстановления: нет носителя»	Нет USB-носителя	Подключить USB-носитель в USB-порт
«Ошибка восстановления: неподдерживаемый носитель»	USB-носитель имеет неподдерживаемую файловую систему	Предъявить носитель с поддерживаемой файловой системой
«Ошибка восстановления»	При восстановлении настроек произошла ошибка	Повторить заново, либо обратиться в сервисный центр

5.2. Режим администрирования

Сообщения БСВВ, которые могут появиться в режиме администрирования, приведены в таблицах 3 и 4.

Таблица 3 – Сообщения при восстановлении настроек с внешнего носителя

Сообщение	Описание	Действие
«Ошибка восстановления: нет носителя»	Нет USB-носителя	Подключить USB-носитель в USB-порт
«Ошибка восстановления: неподдерживаемый	USB-носитель имеет неподдерживаемую	Предъявить носитель с поддерживаемой файловой

Сообщение	Описание	Действие
носитель»	файловую систему	системой
«Ошибка восстановления»	При восстановлении настроек произошла ошибка	Повторить заново либо обратиться в сервисный центр
Введите PIN код	Авторизация на АНП	Ввести PIN-код
«PIN код не верен»	Предъявлен неверный PIN код	Предъявить верный PIN-код
«Ошибка выгрузки: нет носителя»	Нет USB-носителя	Подключить USB-носитель USB-порт
«Ошибка выгрузки: неподдерживаемый носитель»	USB-носитель имеет неподдерживаемую файловую систему	Предъявить носитель с поддерживаемой файловой системой
«Данные инсталляционного носителя не верны»	Носитель не является доверенным и содержащим ПО	Обратиться к администратору безопасности
«Ошибка контроля целостности инсталляционного носителя»	Носитель не является доверенным и содержащим ПО	Обратиться к администратору безопасности

Таблица 4 – Сообщения при загрузке/обновлении сертификатов УЦ

Сообщение	Описание	Действие
«Ошибка! Неизвестный формат PKCS7 цепочки CA!»	Файл не является файлом цепочки сертификатов, или формат цепочки не DER	Выбрать файл формата DER
«Ошибка! Неизвестный формат CRL»	Файл не является файлом цепочки сертификатов, или формат цепочки не DER	Выбрать файл цепочки сертификатов формата DER
«Сертификат еще не вступил в действие»	Срок действия загружаемого сертификата еще не наступил.	Выбрать сертификат с корректным сроком действия

5.3. Штатный режим

Сообщения БСВВ, которые могут появиться в штатном режиме, приведены в таблице 5.

Таблица 5 – Сообщения в штатном режиме

Сообщение	Описание	Действие
«Нарушена целостность БСВВ»	Произошло вмешательство извне в бинарный образ БСВВ	Срочно уведомить администратора комплекса и ответственного за безопасность

Сообщение	Описание	Действие
«Введите PIN код»	Авторизация на АНП	Ввести PIN-код
«PIN код не верен»	Предъявлен неверный PIN-код	Предъявить верный PIN-код

ПРИЛОЖЕНИЕ 1

Справочное

ДАННЫЕ СОПОСТАВЛЕНИЯ

Данные сопоставления задаются в текстовом файле в следующем виде:

```
тип данных сопоставления1=значение данных
тип данных сопоставления2=значение данных
```

Пример задания данных сопоставления:

```
CN=cn token user1
SUBJECT=subject for token user1
MAIL=token_user1@NUMA.ru
UID=1234
DIGEST=1122334455667788990011223344556677889900112233445566778899001122
```

Ограничения:

- обрабатывается не более 5 строк;
- при дублировании типов будет использован первый по порядку следования в файле.

ПРИЛОЖЕНИЕ 2

Справочное

ПОРЯДОК СЛЕДОВАНИЯ ПОЛЕЙ ПРИ СОЗДАНИИ КАРТОЧЕК ПОЛЬЗОВАТЕЛЕЙ

Карточки пользователей задаются в Unicode JSON-файле.

Формат выгружаемого файла *.json имеет следующий структурированный вид, описанный в таблице 6.

Таблица 6 – Описание формата выгружаемого файла

Поле	Значение	Описание
Name	UNICODE, от 3 до 25 символов	Логин
UserID	Число	Идентификатор пользователя
AuthType	«Token», «TokenAndPassword»	Тип аутентификации: Token – АНП, TokenAndPassword – АНП + логин/пароль
Flags	Число	Битовые флаги, объединенные по "или": 0x0040 - флаг блокировки пользователя; 0x0080 - тип пользователя: администратор. Если данный бит равен нулю, то тип пользователя: пользователь; 0x0100 - использовать счетчик аутентификаций; 0x0200 - использовать счетчик попыток входа
FullName	UNICODE, не более 25 символов	ФИО пользователя
ContactInfo	UNICODE, не более 50 символов	Контактная информация
TokenData	Массив полей	Поля данных сопоставления
Type	«SN», «Digest», «Mail»	Тип сопоставления: SN – Subject name, Digest - хеш, Mail – эл.почта
ComparisonData	Текстовое значение	Данные сопоставления
AccessType	0/1/2	Роль пользователя. Возможные значения: 0 – Пользователь, 1 – Аудитор, 2 - Администратор
PasswordCreationTime	Дата и время в UNICODE	Время создания пароля

Примечание. Должно быть указано хотя бы одно значение данных для сопоставления токена (SN, Mail, Digest).

Пример содержимого файла:

```
{
  "UsersList": [
    {
      "Name": "admin",
      "UserID": 1,
```

```
      "AuthType": "Token",
      "Flags": 128,
      "FullName": "uks",
      "ContactInfo": "666",
      "TokenData": [
        {
          "Type": "SN",
          "ComparisonData": "0000000035824752"
        },
        {
          "Type": "DIGEST",
          "ComparisonData":
"EA7195B32F929397CF8DAF180DC19EEF8C7FDD9361331E15C37742C4723D906B"
        }
      ],
      "PasswordCreationTime": "2021-11-22_17:49:03",
      "PasswordHash":
"CCE01BC759820155312E16243835DC2124900C00B9D4CC8671B07100F0A34C33",
      "AccessType": 2
    }
}
```

ПРИЛОЖЕНИЕ 3

СПИСОК СОБЫТИЙ, РЕГИСТРИРУЕМЫХ В ЖУРНАЛЕ

Код события	Мнемоника	Уровень критичности		Описание события
0x0002	HEVENT_USER_LOGIN	6/3	Информация (info) Ошибка (error)	Авторизация пользователя, событие заносится в журнал при каждой попытке авторизации с результатом «успех» или «ошибка» в зависимости от результата прохождения авторизации
0x0003	HEVENT_ADD_NEW_USER	6/3	Информация (info)	Создание (добавление) нового пользователя, заносится в журнал при каждой записи во флеш новой карточки пользователя
0x0004	HEVENT_DELETE_USER	6/3	Информация (info)	Удаление пользователя из системы БСВВ, заносится в журнал при удалении карточки пользователя
0x0005	HEVENT_LOAD_CA	6	Информация (info)	Загрузка сертификата удостоверяющего центра, заносится при записи во флеш данных сертификата
0x0006	HEVENT_LOAD_CRL	6	Информация (info)	Загрузка списка отозванных сертификатов, заносится при записи во флеш данных сертификата
0x0009	HEVENT_FORCE_CHECK_INTEGRITY	6/3	Информация (info) Ошибка (error)	Принудительный контроль целостности, заносится в журнал при выполнении контроля целостности из меню
0x000A	HEVENT_START_TO_LOAD_OS	6/3	Информация (info) Ошибка (error)	Старт запуска ОС, событие заносится в журнал перед каждой загрузкой ОС с результатом «успех» и в случае если загрузка ОС не прошла, т. е. вернулись из загрузчика в БСВВ с

Код события	Мнемоника	Уровень критичности		Описание события
				результатом «Ошибка»
0x000B	HEVENT_REGULAR_LOADING_MODE	7	Отладочная (debug)	Выбран режим штатной загрузки, заносится при выборе в «Главном меню» профиля загрузки
0x000C	HEVENT_ADMIN_MODE	7	Отладочная (debug)	Вход в меню режима администрирования, заносится при входе в меню «Панель управления»
0x000D	HEVENT_USER_UPDATE_DATA	6/3	Информация (info) Ошибка (error)	Обновление данных учетной записи пользователя
0x000E	HEVENT_CHECK_MODULE	3	Ошибка (error)	Проверка целостности модуля перед загрузкой ОС, заносится при проверке списка контроля целостности для выбранного способа загрузки (например, «Загрузка профиля» в Главном меню)
0x000F	HEVENT_EXPORT_USERS	6/3	Информация (info) Ошибка (error)	Экспорт учетных записей пользователей на USB носитель
0x0010	HEVENT_ADMIN_MODE_EXIT	7	Отладочная (debug)	Выход из меню "Панель управления", заносится в журнал при нажатии ESC в меню администрирования
0x0011	HEVENT_CERT_MODE_ENTER	7	Отладочная (debug)	Вход в меню управления сертификатами
0x0012	HEVENT_CERT_MODE_EXIT	7	Отладочная (debug)	Выход из меню управления сертификатами
0x0013	HEVENT_USR_CTRL_MODE_ENTER	7	Отладочная (debug)	Вход в меню управления пользователями
0x0014	HEVENT_USR_CTRL_MODE	7	Отладочная	Выход из меню

Код события	Мнемоника	Уровень критичности		Описание события
	_EXIT		(debug)	управления пользователями
0x0015	HEVENT_DATE_TIME_MODE_ENTER	7	Отладочная (debug)	Вход в меню дата/время
0x0016	HEVENT_DATE_TIME_MODE_EXIT	7	Отладочная (debug)	Выход из меню дата/время
0x0017	HEVENT_RESET_SYSTEM	7	Отладочная (debug)	Перезагрузка системы
0x0019	HEVENT_ADM_MODE_EXIT	5	Уведомление (notice)	Завершение режима администрирования
0x001A	HEVENT_TOKEN_EJECTED	5	Уведомление (notice)	Уведомление об извлечении токена
0x001B	HEVENT_BIOS_UPDATE_MODE_ENTER	7	Отладочная (debug)	Вход в пункт меню «ВерсияПО\обновление БСВВ»
0x001C	HEVENT_BIOS_UPDATE_MODE_EXIT	7	Отладочная (debug)	Выход в пункт меню «ВерсияПО\обновление БСВВ»
0x001F	HEVENT_HISTORY_MENU_ENTER	7	Отладочная (debug)	Вход в меню «Управления журналом аудита»
0x0020	HEVENT_HISTORY_MENU_EXIT	7	Отладочная (debug)	Выход из меню «Управления журналом аудита»
0x0021	HEVENT_USR_PASS_CHANGE	6	Информация (info)	Смена пароля пользователя
0x0022	HEVENT_TOKEN_INSERT_NOTIFY	5	Уведомление (notice)	Подключен токен
0x0023	HEVENT_USER_NAME_FAIL	3	Ошибка (error)	Неверное имя пользователя, заносится в журнал при вводе неверного имени пользователя
0x0024	HEVENT_WRONG_PIN	3	Ошибка (error)	Введен неверный PIN -код, заносится в журнал при вводе неверного PIN-кода, при авторизации по токену

Код события	Мнемоника	Уровень критичности		Описание события
0x0026	HEVENT_DEV_MANAGER_MODE_ENTER	7	Отладочная (debug)	Вход в меню «Драйверы устройств»
0x0027	HEVENT_DEV_MANAGER_MODE_EXIT	7	Отладочная (debug)	Выход из меню «Драйверы устройств»
0x003C	HEVENT_LDAP_START_TLS	3	Ошибка (error)	Ошибка инициализации TLS соединения
0x003D	HEVENT_LDAP_ERROR_TO_GET_PERMIT	3	Ошибка (error)	Ошибка определения прав пользователя для рабочей станции
0x003F	HEVENT_UNKNOWN_FORMAT_OF_CRL	3	Ошибка (error)	Неизвестный формат CRL
0x0040	HEVENT_UNKNOWN_FORMAT_OF_CERT	3	Ошибка (error)	Неизвестный формат сертификата
0x0041	HEVENT_UNKNOWN_KEY_FORMAT	3	Ошибка (error)	Неизвестный формат ключа
0x0042	HEVENT_ERR_CA_SIGN	3	Ошибка (error)	Ошибка при проверке подписи CA
0x0043	HEVENT_ERR_CERT_REVOKED	3	Ошибка (error)	Сертификат отозван
0x0044	HEVENT_ERR_GET_CA_PUBKEY	3	Ошибка (error)	Ошибка при извлечении открытого ключа CA
0x0045	HEVENT_ERR_CRL_VERIFY	3	Ошибка (error)	Ошибка при проверке подписи CRL
0x0046	HEVENT_PKCS7_NOT_SIGNED	3	Ошибка (error)	PKCS7 цепочка CA не подписана
0x0047	HEVENT_VERIFY_ERROR	3	Ошибка (error)	Ошибка верификации структуры данных
0x0048	HEVENT_ERROR_TO_LOAD_CRL	3	Ошибка (error)	CRL не загружен
0x0049	HEVENT_ERROR_TO_LOAD_ISSUER_CERT	3	Ошибка (error)	Цепочка CA не полная. Не найден сертификат Issuer
0x004A	HEVENT_ERROR_TO_LOAD_ISSUER_CERT_LOCALLY	3	Ошибка (error)	Отсутствует сертификат CA, подписавший сертификат пользователя

Код события	Мнемоника	Уровень критичности		Описание события
0x004B	HEVENT_CANT_GET_TRUSTED_CERTS	3	Ошибка (error)	Не могу найти цепочку CA в структуре PKCS7
0x004C	HEVENT_CERT_NOT_YET_VALID	3	Ошибка (error)	Сертификат еще не вступил в действие
0x004D	HEVENT_CERT_HAS_EXPIRED	3	Ошибка (error)	Срок действия сертификата истек
0x004E	HEVENT_CRL_HAS_EXPIRED	3	Ошибка (error)	Срок действия CRL истек
0x004F	HEVENT_UNABLE_TO_GET_CRL	3	Ошибка (error)	Не найден CRL для проверки сертификата/цепочки CA
0x0050	HEVENT_BOOT_CFG_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение состава профилей загрузки
0x0051	HEVENT_BOOT_ICFL_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение списка контроля целостности для профиля загрузки
0x0052	HEVENT_PRIMARY_VIDEO_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение конфигурации чипсета: изменен первичный видеоадаптер
0x0053	HEVENT_USB_LEGACY_SUPPORT_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение конфигурации чипсета: изменен параметр поддержки USB-legacy
0x005B	HEVENT_HISTORY_SEVERITY_LVL_CHANGE	1	Тревога (alert)	Изменение уровня записи в лог
0x005C	HEVENT_HISTORY_AUTO_CLR_CHANGE	6	Информация (info)	Изменение параметра «автоматическая очистка» в меню «Управления журналом аудита»
0x005D	HEVENT_QUICK_BOOT_START	6	Информация (info)	Выполнение загрузки из «Быстрая загрузка»
0x005E	HEVENT_QUICK_BOOT_END	6/3	Информация (info) Ошибка (error)	Результат выполнения (завершения) загрузки из меню «Быстрая загрузка»
0x005F	HEVENT_REGULAR_BOOT	6	Информация	Выбран режим штатной

Код события	Мнемоника	Уровень критичности		Описание события
			(info)	загрузки
0x0060	HEVENT_ADMIN_BOOT	6	Информация (info)	Выбран режим административной загрузки
0x0061	HEVENT_RECOVER_BOOT	6	Информация (info)	Выбран режим загрузки с восстановлением
0x0062	HEVENT_INSTALL_BOOT	6	Информация (info)	Выбран режим инсталляции комплекса
0x0063	HEVENT_BOOT_MNGR_IMPORT_OPT	6	Информация (info)	Выбран пункт меню Конфигуратор - «Загрузка с USB»
0x0064	HEVENT_BOOT_MNGR_EXPORT_OPT	6	Информация (info)	Выбран пункт меню Конфигуратор - «Сохранить на USB»
0x0065	HEVENT_REVOKE_CERTS_CFG_CHANGED	6/3	Информация (info) Ошибка (error)	Изменение конфигурации настройки отзыва сертификатов
0x0066	HEVENT_AUTH_MODE_CFG_CHANGED	6/3	Информация (info) Ошибка (error)	Изменение конфигурации настройки режима авторизации
0x0068	HEVENT_OCPS_URL_ERROR	3	Ошибка (error)	Проверьте OCSP URL
0x0069	HEVENT_OCSP_RESPONSE_VERIFICATION	3	Ошибка (error)	Ошибка верификации OCSP ответа
0x006A	HEVENT_OCSP_RESPONDER_QUERY_FAILED	3	Ошибка (error)	Ошибка отправки OCSP запроса
0x006B	HEVENT_OCSP_CERT_UNKNOWN	3	Ошибка (error)	Неизвестный сертификат – информация о выдаче отсутствует
0x006C	HEVENT_CDP_ERROR	3	Ошибка (error)	Ошибка CDP
0x006D	HEVENT_ERR_INTERNAL	3	Ошибка (error)	Внутренняя ошибка, обратитесь к разработчику
0x006E	HEVENT_UNKNOWN_FORMAT_OF_CHAIN	3	Ошибка (error)	Неизвестный формат PKCS7 цепочки CA

Код события	Мнемоника	Уровень критичности		Описание события
0x006F	HEVENT_MULTIBOOT_START	5	Уведомление (notice)	Запуск модуля доверенной загрузки
0x0070	HEVENT_RESET_BIOS_TO_MII	0	Ошибка системы (emergency)	Сброс настроек БСВВ
0x0071	HEVENT_PCI_DEVS_MONITOR_FAIL	3	Ошибка (error)	Нарушена целостность оборудования
0x0076	HEVENT_PASSWD_GUESSING	1	Тревога (alert)	Подбор пароля
0x007C	HEVENT_BIOS_UPDATE	6	информация (info)	Обновление БСВВ с USB-носителя
0x0083	HEVENT_CRL_REFRESH_START	6	Информация (info)	Запуск процедуры обновления CRL
0x0084	HEVENT_CRL_REFRESH_RESULT	6/3	Информация (info) Ошибка (error)	Результат обновления CRL
0x008A	HEVENT_PCI_DEVS_MONITORING_ON	6	информация (info)	Включен контроль оборудования
0x008B	HEVENT_PCI_DEVS_MONITORING_OFF	6	информация (info)	Контроль оборудования отключена
0x008C	HEVENT_DISABLE_SERIAL_CON_CHANGE	6/3	Информация (info) Ошибка (error)	Изменена настройка разрешения вывода в serial-консоль
0x0090	HEVENT_ERR_SAVING_TO_CERT_STORAGE	3	Ошибка (error)	Ошибка записи сертификата в хранилище
0x0091	HEVENT_USER_BLOCKED	3	Ошибка (error)	Пользователь был заблокирован, заносится в журнал при блокировании пользователя
0x00A1	HEVENT_CANT_VERIFY_USER_WITH_PKEY	3	Ошибка (error)	Закрытый ключ, находящийся на токене, не соответствует открытому ключу из сертификата пользователя
0x00A2	HEVENT_ERR_RUTOKEN_SUPPORT_ERR	3	Ошибка (error)	Токен аппаратно не поддерживает заданный алгоритм шифрования

Код события	Мнемоника	Уровень критичности		Описание события
0x00A3	HEVENT_LANGUAGE_CHANGE	6/3	Информация (info) Ошибка (error)	Переключение языка интерфейса Русский/English
0x00AD	HEVENT_WINDOWS_REGISTRY_CONTROL_FAIL	3	Ошибка (error)	Нарушена целостность реестра Windows
0x00AE	HEVENT_WINDOWS_REGISTRY_CONTROL_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение списка контроля целостности для реестра Windows
0x00AF	HEVENT_SECURITY_MANAGER_MENU_ENTER	7	Отладочная (debug)	Вход в меню 'Параметры безопасности'
0x00B0	HEVENT_SECURITY_MANAGER_MENU_EXIT	7	Отладочная (debug)	Выход из меню 'Параметры безопасности'
0x00B1	HEVENT_EXT4_JOURNAL_RECOVERY_CHANGED	6/3	Информация (info) Ошибка (error)	Параметры безопасности: изменен параметр контроль транзакций Ext4
0x00B2	HEVENT_NTFS_LOGFILE_CHECK_CHANGED	6/3	Информация (info) Ошибка (error)	Параметры безопасности: изменен параметр контроль транзакций NTFS
0x00B3	HEVENT_FS_TRANSACTION_JOURNAL_NOT_EMPTY	3	Ошибка (error)	Журнал транзакций ФС не пуст
0x00B4	HEVENT_HISTORY_UNLOADED	5	Уведомление (notice)	Выгрузка журнала аудита
0x00B5	HEVENT_HISTORY_DELETED	5	Уведомление (notice)	Очистка раздела журнала аудита
0x00B6	HEVENT_TIME_SHIFTED	4	Предупреждение (warning)	Обнаружено несанкционированное изменение времени
0x00B7	HEVENT_FORCE_CHECK_MODULE	3	Ошибка (error)	Принудительный контроль целостности модуля
0x00B9	HEVENT_PLATFORM_TEST_SUCCESS	6	Информация (info)	Проверка платформы прошла успешно
0x00BA	HEVENT_PLATFORM_TEST_CPU_ERROR	3	Ошибка (error)	Обнаружена ошибка CPU
0x00BC	HEVENT_PLATFORM_TEST_MEMORY_ERROR	3	Ошибка (error)	Обнаружена ошибка памяти

ПРИЛОЖЕНИЕ 4

СПИСОК СОВМЕСТИМЫХ PCIE УСТРОЙСТВ

В качестве совместимых PCIe устройств могут выступать SATA-контроллеры.

ПРИЛОЖЕНИЕ 5

СПИСОК СОВМЕСТИМЫХ ТОКЕНОВ

В качестве токенов в Изделии должны использоваться АНП, сертифицированные по требованиям ФСБ России, предъявляемым к СКЗИ для класса КС3, поддерживающие алгоритм ГОСТ Р 34.10-2012.

ООО «НумаТех» рекомендует к использованию следующие АНП:

АНП производства ООО «АТ Бюро»:

– ESMART Token ГОСТ.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АНП	аутентифицирующий носитель персональный
АРМ	автоматизированное рабочее место
БСВВ	базовая система ввода-вывода
ГОСТ	государственный стандарт
КС	контрольная сумма
ИЗДЕЛИЯ	модуль доверенной загрузки
ОС	операционная система
ПО	программное обеспечение
СВТ	средство вычислительной техники
СКЗИ	средства криптографической защиты информации
ФСБ России	Федеральная служба безопасности
УЦ	удостоверяющий центр
AHCI	advanced host controller interface
BIOS	basic input/output system
CA	certification authority
CN	common name
CPU	central processing unit
CRL	certificate revocation list
DHCP	dynamic host configuration protocol
DNS	domain name server
HDD	hard disk drive
LAN	local area network
LDAP	lightweight directory access protocol
MBR	master boot record
NTFS	new technology file system
PCI	peripheral components interconnect
PID	product identifier
PIN	personal identification number
RAID	redundant array of independent disks
RAM	random-access memory
SATA	serial advanced technoilogy attachment
TLS	transport layer security
UEFI	unified extensible firmware interface
UID	user identificator
URL	uniform resource locator – адрес ресурса
USB	universal serial bus
VID	vendor identifier

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					