Общество с ограниченной ответственностью «Нума Технологии»

УТВЕРЖДЕН

643.АМБН.00022-01 32 01–ЛУ

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Руководство администратора

643.АМБН.00022-01 32 01

Листов 100

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

2020

Литера

АННОТАЦИЯ

Данное руководство предназначено для администраторов Изделия модуль доверенной загрузки Numa Arce 643.АМБН.00022-01 (далее – Изделие или Numa Arce).

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

Перед началом работы с Изделием администратор должен ознакомиться с настоящим руководством.

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.

1.2. Функциональные возможности Изделия

Изделие обеспечивает выполнение следующих функциональных возможностей

- возможность генерации и регистрации возникновения событий, относящихся к безопасности и контролируемых средством доверенной загрузки;
- возможность реагирования на обнаружение событий, указывающих на возможное нарушение безопасности;
- возможность блокирования пользователя при превышении неуспешных попыток аутентификации пользователя;
- возможность проверки соответствия аутентификационной информации определенной метрике качества;
- идентификация и аутентификация пользователя до выполнения действий по загрузке операционной системы или администратора до выполнения действий по управлению средством доверенной загрузки;
- возможность идентификации и аутентификации с помощью логина и пароля или носителя ключевой информации или при совместном использовании носителя ключевой информации и пароля;
- исключение отображения действительного значения

аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе путем отображения условных знаков типа «*»;

– возможность контроля целостности загружаемой операционной системы, файлов, поставленных на контроль администратором Изделия, путем вычисления контрольных сумм по ГОСТ Р 34.11-2012 (256 бит);

– возможность контроля целостности загружаемой операционной системы при загрузке с использованием технологии HTTP Boot путем вычисления цифровой подписи по алгоритму ГОСТ Р 34.10-2012;

– возможность со стороны администраторов управлять режимом выполнения функций безопасности средства доверенной загрузки;

– возможность со стороны администраторов управлять данными (данными средства доверенной загрузки), используемыми функциями безопасности средства доверенной загрузки;

– возможность установления ограничений на время действия аутентификационной информации (пароля), вводимой (вводимого) пользователем в диалоговом интерфейсе при идентификации/аутентификации и блокирования доступа пользователя при превышении ограничений;

– поддержка определенных ролей (возможность создания учетных записи пользователей с ролями администратор, пользователь, аудитор) для средства доверенной загрузки и их ассоциации с конкретными администраторами средства доверенной загрузки и пользователями информационной системы;

– возможность тестирования (самотестирования) функций безопасности средства доверенной загрузки, проверки целостности программного обеспечения средства доверенной загрузки и целостности данных средства доверенной загрузки;

– блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы;

– реализация сценариев блокировки (по длительности блокировки)

Изделия при превышении порога неуспешных попыток аутентификации пользователя;

– блокирование загрузки операционной системы при нарушении целостности средства доверенной загрузки;

– блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды;

– блокирование загрузки операционной системы при критичных типах сбоев и ошибок;

– возможность контроля состава компонентов аппаратного обеспечения средства вычислительной техники, основываясь на их идентификационной информации;

– блокирование загрузки операционной системы при обнаружении несанкционированного изменения состава аппаратных компонентов;

– обеспечение недоступности информационного содержания ресурсов средств вычислительной техники, использовавшихся в процессе работы средства доверенной загрузки программным обеспечением и данными средства доверенной загрузки после завершения работы средства доверенной загрузки.

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 – пользователь, наделенный правами по просмотру контроля целостности Изделия, файлов, поставленных на контроль администратором, а также имеющий возможность просмотр и выгрузку на USB-флеш-накопитель журнала аудита.

1.4. Режимы функционирования Изделия

Изделие поддерживает следующие режимы работы

1.4.1. Режим администрирования

Переход в режим администрирования осуществляется пользователем, наделенным полными правами и привилегиями по администрированию Изделия (далее – Администратор).

1.4.2. Штатный режим функционирования Изделия

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

1.4.3. Режим работы для аудитора

Режим работы для пользователя с ролью аудитор предназначен для пользователей с ролью «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:

– просмотр целостности Изделия, файлов и объектов, поставленных на контроль администратором Изделия;

– действия с журналом аудита: просмотр, выгрузка.

1.4.4. Аварийный режим

При аварийном режиме работы Изделия предусматривается блокировка СВТ, на которое установлено Изделие. Дальнейшая работ Изделия возможна только после переустановки Изделия в режиме начально инициализации.

1.4.5. Режим начальной инициализации

Режим инициализации доступен только при первом запуске Изделия, или при восстановлении из-за нарушения контроля целостности Изделия. При режиме инициализации все установленные администратором данные стираются, Изделие возвращается к заводским настройкам.

1.5. Дополнительные требования

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

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

Для обновления Изделия требуется USB-флеш-накопитель с файловой системой FAT32.

Для осуществления доверенной загрузки операционной системы по технологии HTTP Boot необходимо развернуть удостоверяющий центр и инфраструктуру открытых ключей в ОС Astra Linux версии 1.6 и выше. Разворачивание удостоверяющего центра, построение инфраструктуры открытых ключей должно осуществляться администратором безопасности с помощью библиотеки OpenSSL.

Для осуществления доверенной загрузки операционной системы по технологии HTTP Boot необходимо развернуть WEB-сервер с поддержкой протокола TLS, например, Защищенный комплекс программ гипертекстовой обработки данных из состава ОС Astra Linux версии 1.6 и выше.

1.6. Требования к аппаратным средствам

Изделие может функционировать на материнских платах СВТ следующего типа:

Таблица 1 – Соответствие серии чипсетов и исполнения Изделия

Исполнение Изделия	Серия чипсетов
Numa Arce 643.АМБН.00022-01 Исполнение 1	Baytrail (Atom E38xx)
Numa Arce 643.АМБН.00022-01 Исполнение 2	KabyLake/CoffeLake (NS565, NS685, H310C, B365)
Numa Arce 643.АМБН.00022-01 Исполнение 3	ApolloLake (Atom E39xx/N4200)
Numa Arce 643.АМБН.00022-01 Исполнение 4	CoffeeLake (H246)

Исполнение Изделия	Серия чипсетов
Numa Arce 643.АМБН.00022-01 Исполнение 5	SkyLake (H170)
Numa Arce 643.АМБН.00022-01 Исполнение 6	Denverton (Atom C300)

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 идентификаторов (имен) и паролей (кодов) администратора Изделия.

Обновление Изделия должно осуществляться только с использованием файла-прошивки, полученной от изготовителя, в т.ч. скачанной с его официального сайта, с соблюдением соответствующих Инструкций изготовителя.

Изменение версии Изделия на другую версию возможно только в том случае, если изготовителем подтверждено соответствие данной версии Изделия требованиям безопасности информации путем проведения анализа уязвимостей и периодических испытаний Изделия.

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

Запрещается модифицировать, реконструировать или видоизменять Изделие.

Установка, конфигурирование и управление Изделием должны производиться только администратором в соответствии с данным руководством.

2. УСТАНОВКА ИЗДЕЛИЯ

2.1. Установка Изделия

Установка и активация Изделия осуществляется Изготовителем устройства, на которое устанавливается Изделие, при его производстве. Идентификационная и аутентификационная информация (логин-пароль) администратора установленного Изделия должна быть получена от Изготовителя устройства, на которое установлено Изделие.

Для обновления Изделия необходимо выполнить действия по обновлению описанные в разделе 4.7.2.1.

В случае полной переустановки Изделия на СВТ необходимо выполнить полную настройку Изделия, для этого:

Примечание. Для установки Изделия требуется USB-флеш-накопитель с файловой системой FAT32.

Внимание! Процедура безопасной установки Изделия должна начинаться с проверки контрольной суммы полученного Изделия на соответствие сертифицированной версии! Процедура выполняется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00022-01 94 01.

1) скопировать файловый архив, содержащий файл-прошивку с компакт-диска, входящего в комплект поставки, на USB-флеш-накопитель с файловой системой FAT32;

2) распаковать содержимое архива в корневую папку подготовленного USB-флеш-накопителя;

3) подключить подготовленный USB-флеш-накопитель с файлом-прошивкой к СВТ и произвести загрузку в EFI-режиме;

4) в автоматической режиме после загрузки запустится скрипт установки файла-прошивки (см. рисунок 1);

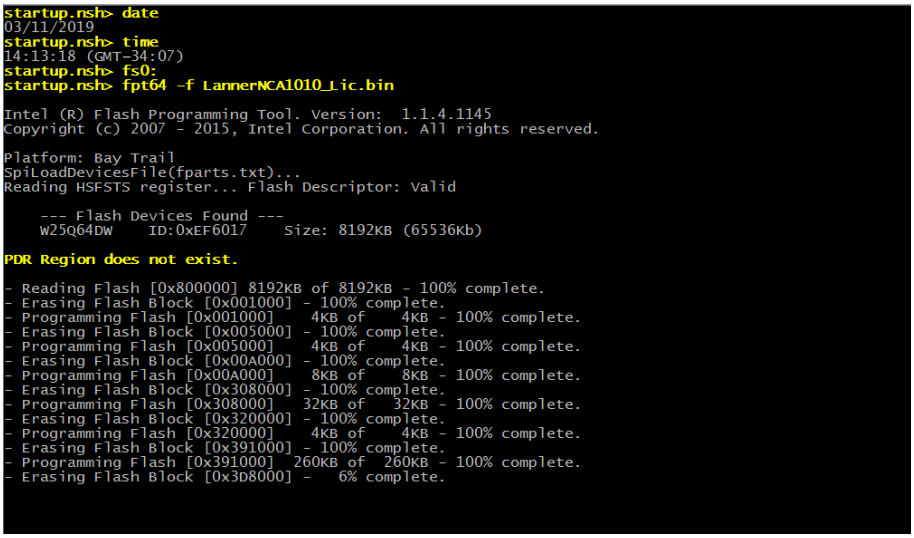

Рисунок 1 – Работа скрипта прошивки

Примечание. В конце работы скрипта возможны сообщения об ошибках верификации, данные ошибки необходимо проигнорировать.

После окончания работы скрипта необходимо нажать клавишу «Enter» для перезагрузки СВТ.

Также доступна установка Изделия с использованием программатора.

2.2. Запуск Изделия

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

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

2.3. Подготовка к работе

При первом включении Изделия в консоль могут выводиться сообщения об ошибках «DebugAssert...», ошибки такого типа следует игнорировать.

При первом включении Изделия необходимо создать учётную запись администратора.

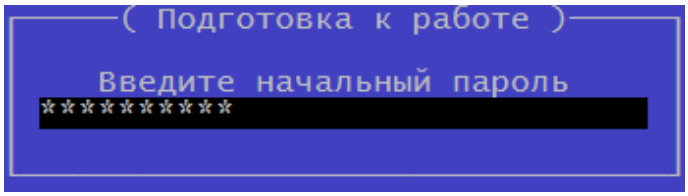

Рисунок 2 – Диалог ввода пароля для меню «Подготовка к работе»

Для этого в режиме «Подготовка к работе» (см. рисунок 2) необходимо ввести начальный пароль «**capitolium**» для дальнейшей первоначальной настройки Изделия.

После ввода пароля будет доступно меню (см. рисунок 3), состоящее из пунктов:

– «Создать Администратора» – создание учетной записи администратора СВТ;

– «Загрузить с USB» – загрузка подготовленного списка пользователей, включая администратора;

– «Дата и время» – настройка системных часов;

– загрузить сертификаты (см. п. 4.6.2 «Сертификаты»).

Для дальнейшей работы необходимо создать учетную запись администратора. Для этого в меню, представленном на рисунке, выбрать раздел «Создать администратора». В форму, представленную на рисунке 4, необходимо ввести параметры администратора. После создания администратора вход в меню администрирования Изделия будет осуществляться с его учетными записями.

После успешного создания администратора следует перезагрузка Изделия.

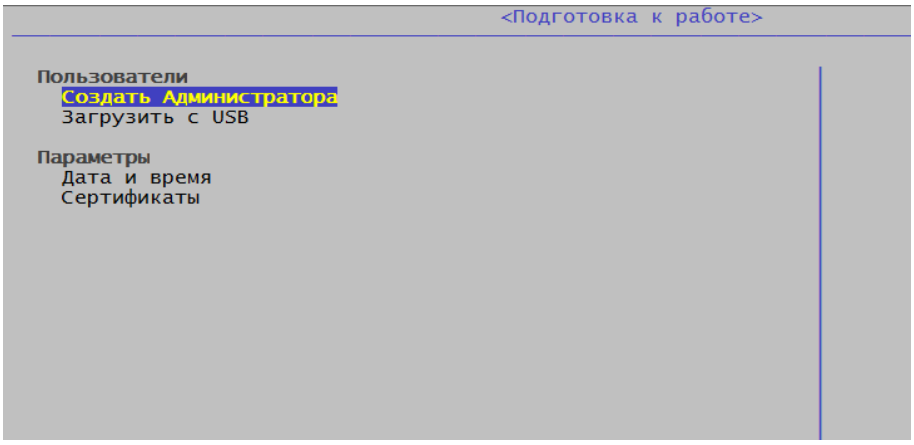

Рисунок 3 – Меню режима «Подготовка к работе»

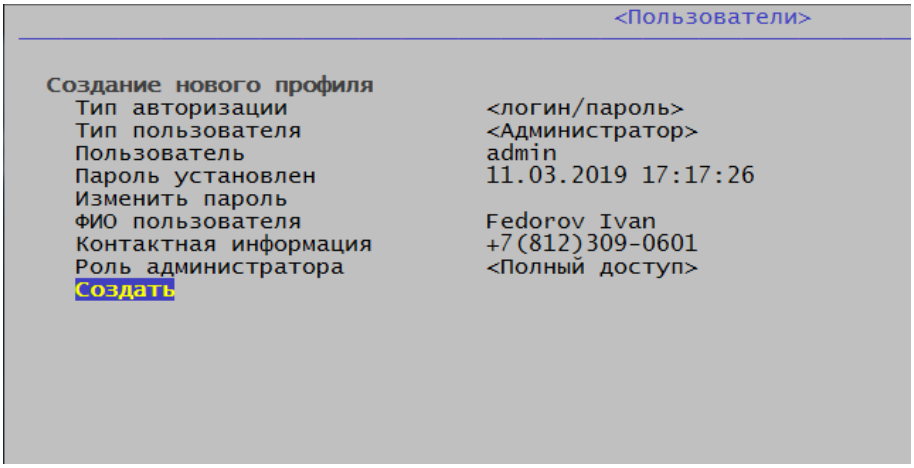

Рисунок 4 – Меню «Создать администратора»

Загрузка ОС СВТ из режима Подготовки к работе Изделия не предусмотрена.

2.4. Ввод лицензии

Примечание. Данный пункт не доступен для Изделия в исполнении 1,исполнении 3, исполнении 5. После режима «Подготовка к работе» Изделие переходит в режим «Администрирования» для дальнейшей настройки Изделия.

После перезагрузки Изделия активизируется режим проверки лицензии на Изделие. Для отображения меню «ручной режим запроса лицензий» нажмите «Esc» (см. рисунок 5):

– «Сохранить файл запроса» – сохраняет файл с уникальным

идентификатором на USB-флеш-накопитель. В дальнейшем этот файл должен быть передан в компанию-изготовитель СВТ, на которое установлено Изделие для создания файла лицензии;

– «Загрузить файл лицензии» – загрузить полученный файл лицензии;
– «Настройка даты и времени» – настройка системных часов.

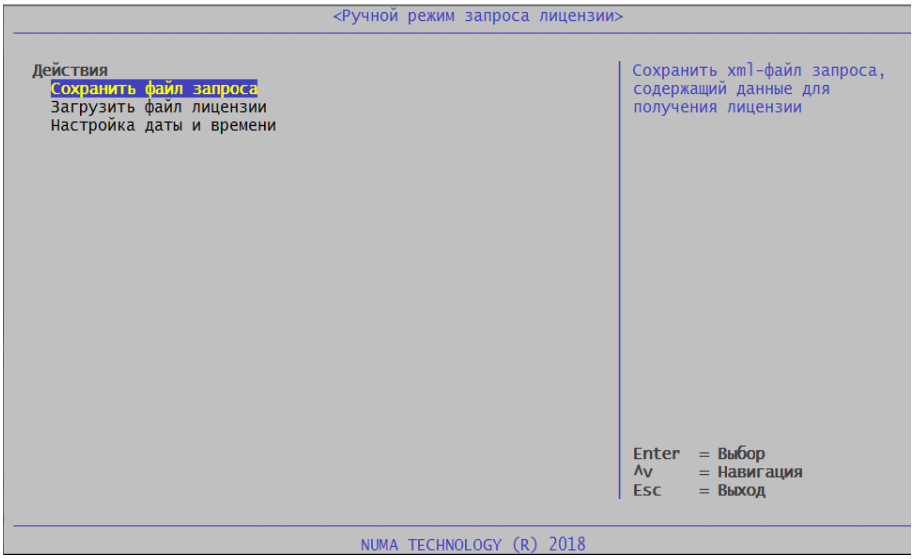

Рисунок 5 – Ручной режим запроса лицензии

Для создания файла запроса для получения лицензии необходимо в меню «Ручной ввод лицензии» необходимо выбрать пункт «Сохранить файл запроса». Необходимые данные будут сохранены на USB-флеш-накопитель в файл с именем «numa_license_req_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.xml» (см. рисунок 6).

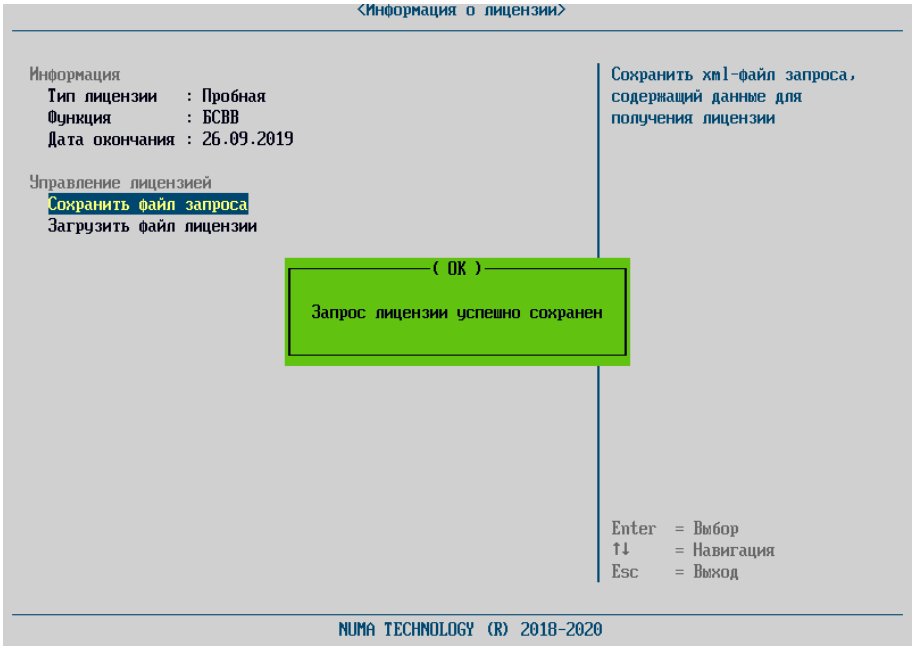

Рисунок 6 – Создание файла запроса лицензии

Созданный файл необходимо отправить в службу технической поддержки изготовителя устройства, на которое установлено Изделие.

На основе файла запроса лицензии будет создан файл лицензии («XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.p12»).

Для активации лицензии необходимо полученный файл лицензии загрузить через пункт меню «Загрузить файл лицензии». После проверки лицензии работа Изделия будет разблокирована, Изделие будет доступно для дальнейшей настройки и использования.

В случае если выбран файл от неверной платформы, 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 службу технической поддержки Изготовителя устройства, на которое устанавливается Изделие.

2.5. Режим производства

После ввода лицензии и перезагрузке СВТ будет осуществлён

автоматический вход в режим производства.

В данном режиме в главном меню доступны дополнительные пункты (см. рисунок 7):

a. загрузить настройки БСВВ;

b. сохранить настройки БСВВ;

c. выход из режима производства.

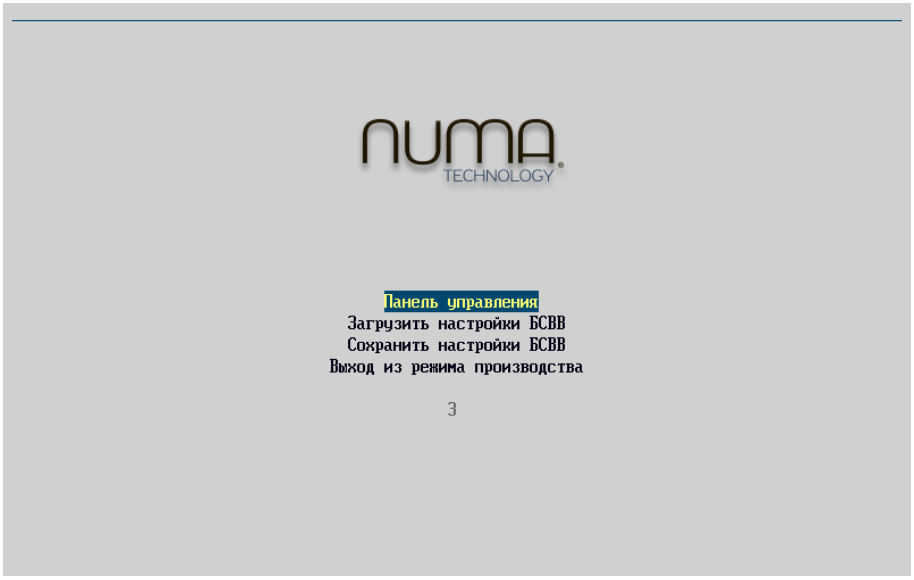

Рисунок 7 – Главное меню «Режима производства»

Выход из режима производства производится вручную – через пункт меню.

2.5.1. Создание файла настроек

Для создания файла настроек необходимо выполнить следующие действия:

– войти в меню «Панель управления»;

– внести необходимые изменения в настройки, например, создать загрузочный профиль, список пользователей и настройки портов SATA/USB;

– перезагрузиться (выход из панели управления в главное меню невозможен);

– выполнить пункт «сохранить настройки БСВВ» – файл настроек будет сохранен на USB-флеш-накопитель в папку \BIOS;

– выйти из режима производства через соответствующий пункт меню.

2.5.2. Применение файла настроек:

Для применения файла-настроек необходимо выполнить следующие действия:

– установить USB-флешку с сохраненным файлом настроек и включить изделие;

– если файл настроек существует, автоматически будет предложено загрузить его (см. рисунок 8);

– в случае согласия файл будет загружен и будет осуществлен автоматический выход из режима производства;

– в случае отказа пользователю предоставляется возможность выбрать файл вручную, выбрав пункт «Загрузить настройки БСВВ».

Выход из режима производства также производится вручную – через пункт меню.

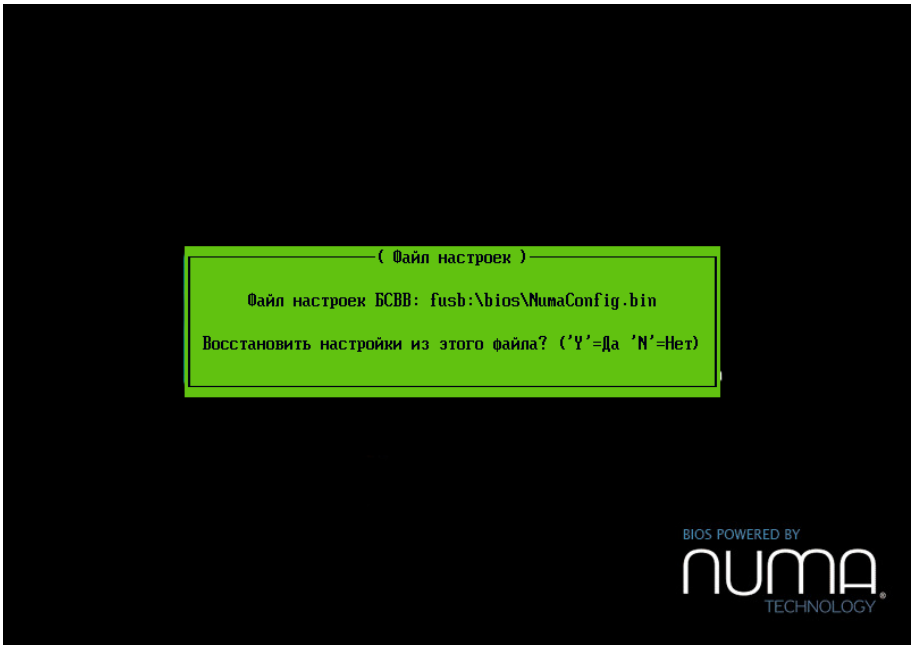

Рисунок 8 – Установка файла настроек

3. ОПИСАНИЕ ПРОЦЕДУР ПРОВЕРКИ ЦЕЛОСТНОСТИ

3.1. Контроль целостности в штатном режиме

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

- ПО Изделия (ГОСТ Р 34.11-2012);
- модули БСВВ (ГОСТ Р 34.11-2012);
- конфигурационных параметров (ГОСТ Р 34.11-2012);
- ПО СВТ (MBR и ОС, поставленные на контроль), файлы, поставленные на контроль администраторам (ГОСТ Р 34.11-2012).

В случае нарушения контроля целостности образа Изделия (ПО Изделия), Изделие осуществляет переход в аварийный режим работы, который сопровождается сообщением об ошибке и блокировкой загрузки СВТ.

В случае нарушения контроля целостности локальных файлов MBR и ОС, файлов, поставленных на контроль администратором Изделия (объекты загружаемой операционной системы), осуществляется блокировка работы СВТ, выдача сообщения об ошибке, звуковой сигнал (только при наличии технической возможности), запись в журнал аудита.

Примечание. Дальнейшая блокировка требует снятие блокировки администратором Изделия путем перерасчета контрольных сумм.

В случае нарушения контроля целостности конфигурационных параметров осуществляется блокировка загрузки СВТ, выдача сообщения об ошибке и предложение сохранить отладочный дамп для дальнейшего расследования инцидента.

3.2. Проверка целостности вручную

Функция проверки целостности вручную 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 9).

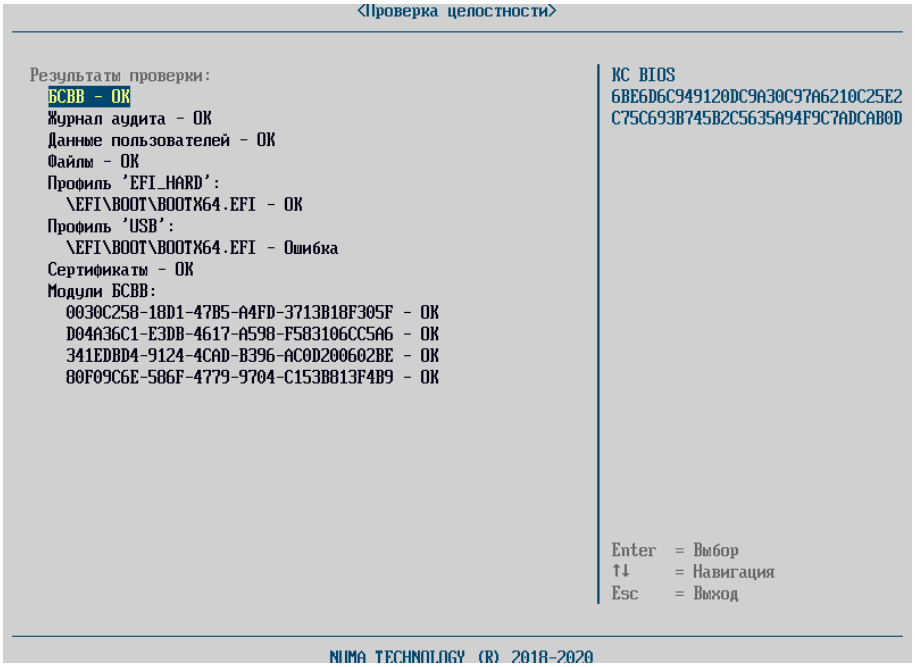

Рисунок 9 – Результат контроля целостности вручную

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

Контрольная сумма рассчитывается на основании алгоритма ГОСТ Р 34.11-2012 с ключом в 256 бит.

Управление списком файлов, для которых осуществляется контроль целостности, доступно из раздела «Редактирование профиля» пункта «Конфигуратор» меню «Панель управления» (п. 4.4.2.6).

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

4.1. Авторизация

После загрузки Изделия появляется окно с приглашением выбрать тип авторизации пользователя (см. Рисунок 10):

– по имени пользователя;

– с помощью АНП.

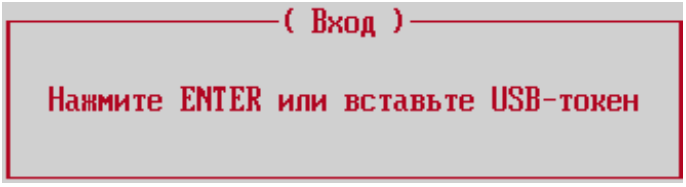

Рисунок 10 – Внешний вид окна с приглашением для выбора типа авторизации

Чтобы авторизоваться по имени пользователя (с помощью логина и пароля), необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, нажать «Enter»;

– в окне «Имя пользователя» (см. рисунок 11) ввести имя пользователя;

– в появившемся окне «Пароль пользователя» (см. рисунок 12) ввести пароль и нажать «Enter».

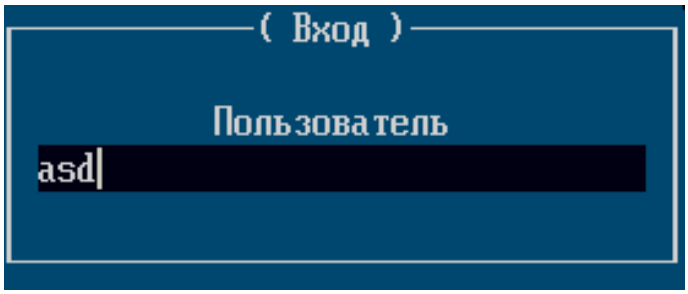

Рисунок 11 – Внешний вид авторизационного окна «Имя пользователя»

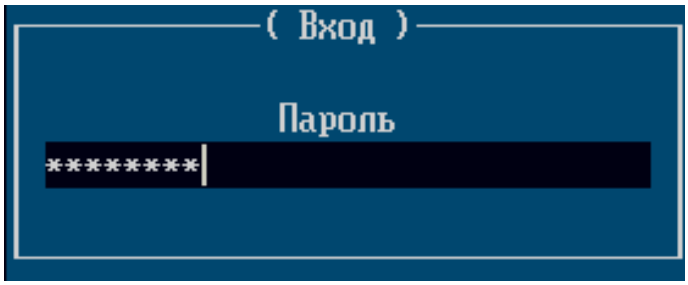

Рисунок 12 – Внешний вид авторизационного окна «Пароль пользователя»

Чтобы авторизоваться с помощью АНП, необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, вставить АНП в USB–разъем СВТ;

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

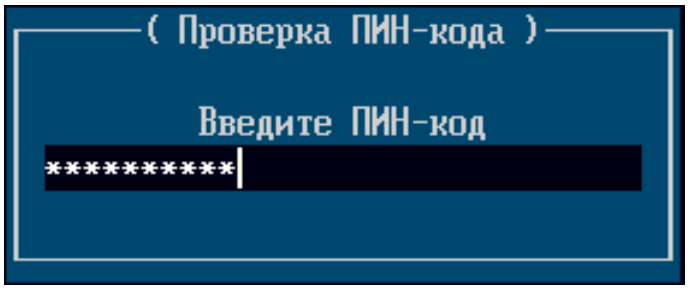

Рисунок 13 – Внешний вид окна при авторизации с помощью АПН

Если задан тип авторизации «АНП + логин и пароль», необходимо выполнить следующие действия:

– после появления окна с приглашением к авторизации, вставить АНП в USB–разъем СВТ;

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

– в появившемся окне «Имя пользователя» ввести имя пользователя;

– в появившемся окне «Пароль пользователя» ввести пароль и нажать «Enter».

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

Примечание. В случае если предварительно в Изделие не был загружен сертификат, при попытке авторизации об этом будет выведено сообщение «СА не загружен!». После извлечения АНП или нажатия клавиши «Enter» в этом случае пользователю в доступе будет отказано с выводом сообщения «Ошибка! доступ запрещен!».

Примечание. Количество попыток ввода PIN-кода для АНП ограничивается администратором организации при инициализации АНП.

В Изделии реализован механизм блокирования работы пользователи при превышении установленных администратором Изделия параметров. По умолчанию в Изделии установлены следующие параметры для защиты от несанкционированного доступа:

– количество неуспешных попыток ввода пароля – 3;

– время блокировки пользователи при превышении установленного количества неуспешных попыток ввода пароля – 15 минут.

Подробная информация о способах настройки парольной политик описана в разделе 4.6.1.4.

Любые действия по администрированию Изделием доступны только после успешной процедуры авторизации.

Для исполнения 1, исполнения 3, исполнения 5 загрузка полезной нагрузки (например, ОС) осуществляется после подачи питания на СВТ при условии успешного прохождения контроля целостности настроенного Изделия, в том числе файлов, поставленных на контроль целостности администратором, без запроса авторизации пользователя.

4.2. Главное меню

После успешной авторизации администратора или аудитора на экране появляется меню, которое содержит список профилей загрузки (при условии, если профили были созданы заранее) и пункт «Панель управления» (см. рисунок 14).

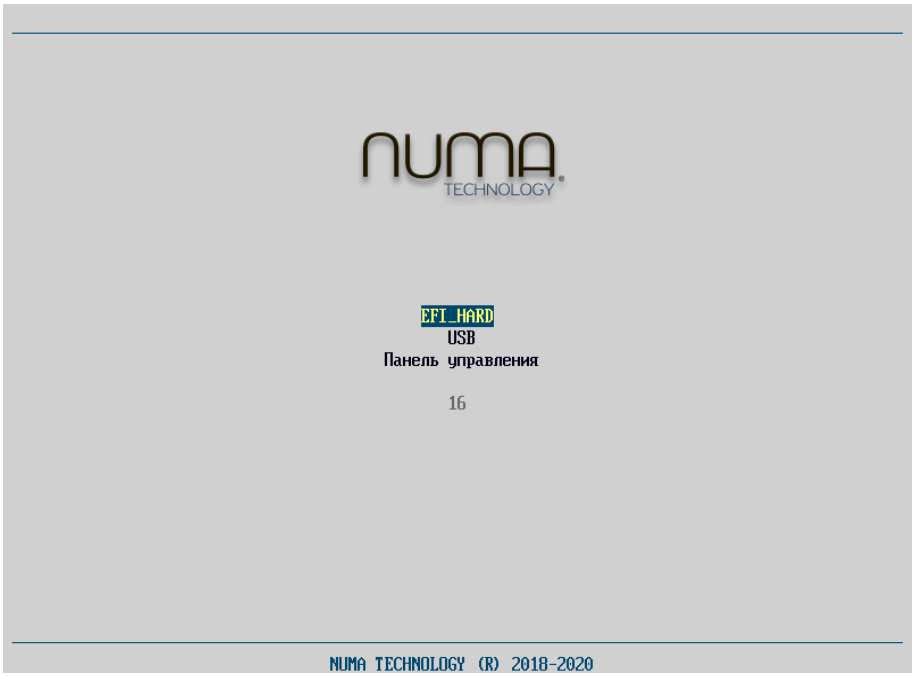

Рисунок 14 – Главное меню

По умолчанию меню на экране отображается в течение 7 сек., после чего происходит запуск профиля загрузки СВТ если он один или первого из списка профилей, если их более одного. Если была нажата какая-либо клавиша, меню будет отображаться на экране вплоть до выбора соответствующего пункта.

Настроить тайм-аут можно в пункте меню «Конфигуратор».

Обычный пользователь после авторизации получает доступ к списку профилей загрузки, пункт – «Панель управления» для него не доступен. Если заведен всего один профиль загрузки, система сразу переходит к загрузке ОС, соответствующей профилю.

Примечание. Для исполнения 1, исполнения 3, исполнения 5 загрузка полезной нагрузки (например, ОС) осуществляется после подачи питания на СВТ при условии успешного прохождения контроля целостности настроенного

Изделия, в том числе файлов, поставленных на контроль целостности администратором, без запроса авторизации пользователя.

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 ОС, создать конфигурацию загрузки и настроить параметры Изделия.

В режиме управления пользователю с правами администратора доступно 13 пунктов меню, сгруппированных в 4 секции.

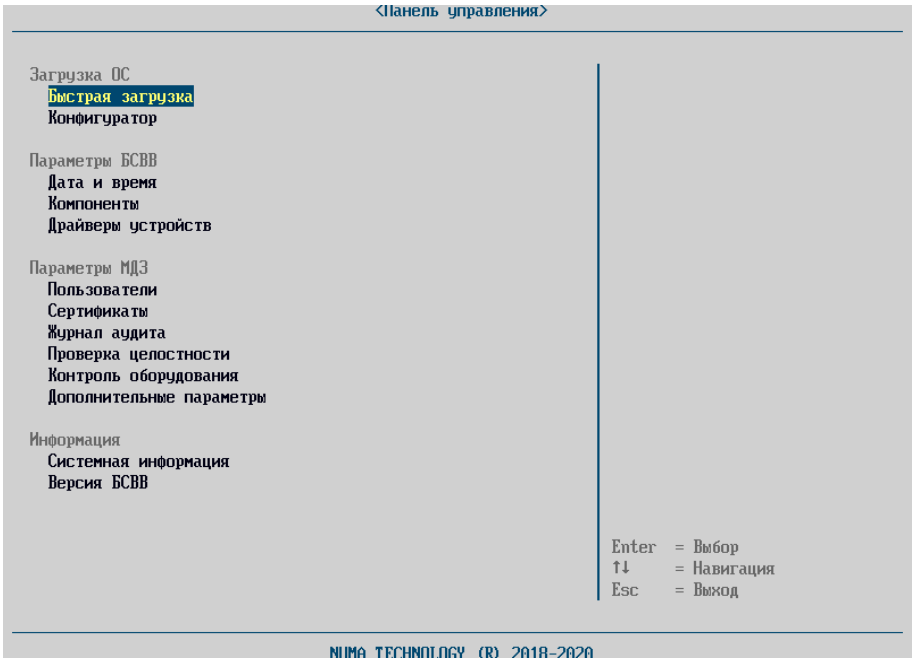

Рисунок 15 – Меню «Панель управления». Вид администратора

Администратору с правами аудитора доступны только два пункта меню (см. Рисунок 16):

– «Журнал аудита»;

– «Проверка целостности».

Остальные пункты меню выводятся серым шрифтом и недоступны для выбора.

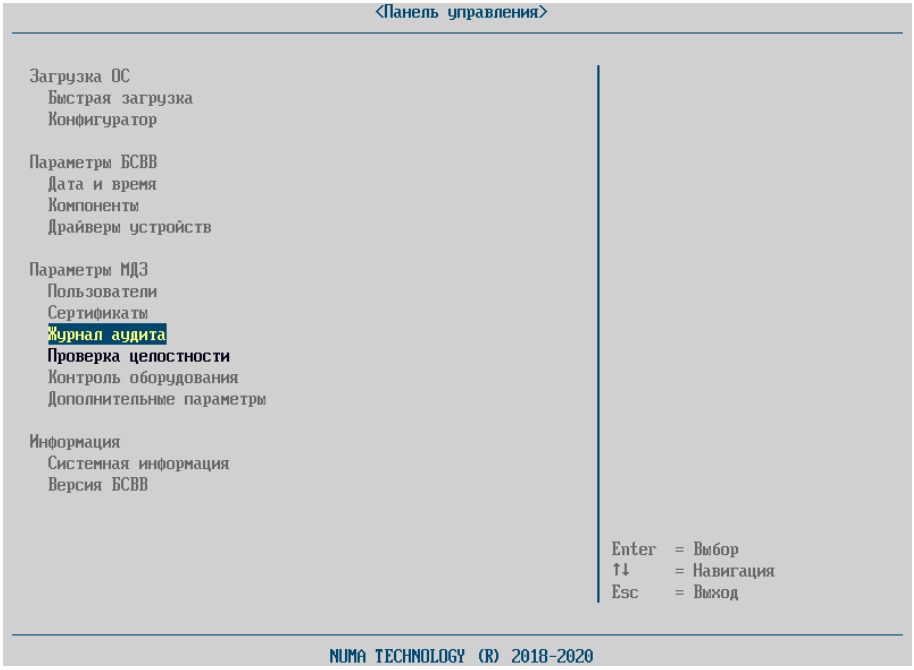

Рисунок 16 – Меню администратора с правами аудитора

4.4. Раздел «Загрузка ОС»

4.4.1. «Быстрая загрузка»

Пункт «Быстрая загрузка» (см. рисунок 17) 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-флеш-накопителей определяется настройкой в подразделе «Компоненты» параметром «Драйвер USB Legacy».

– «Профили загрузки» – показывает существующие профили.

– «Сканировать носители» позволяет обновлять список загрузочных устройств. Необходим для отображения только что подключенных USB-носителей

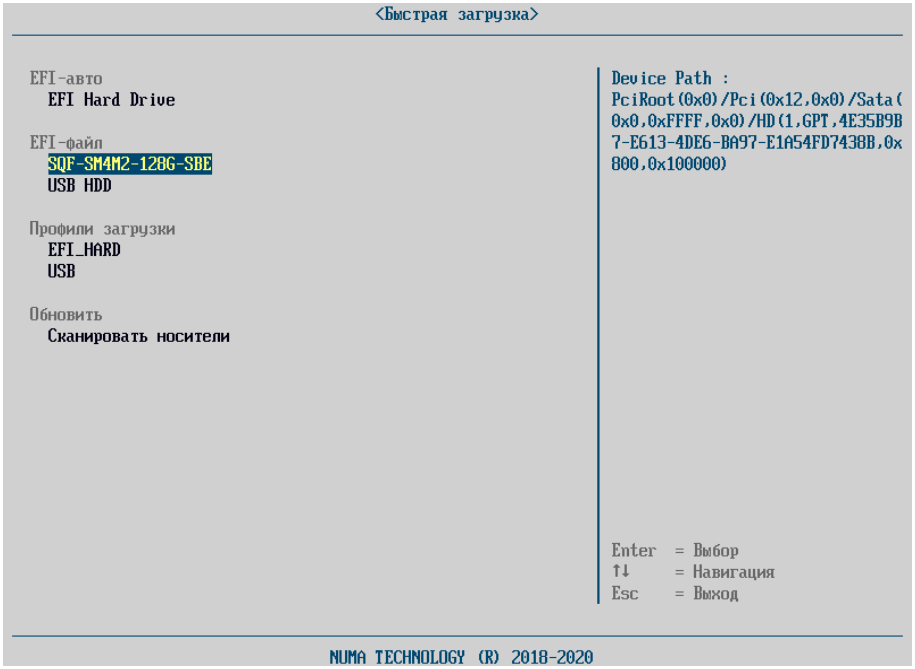

Рисунок 17 – Меню «Быстрая загрузка»

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

4.4.2. «Конфигуратор»

Настройка конфигурации загрузки (набора параметров, задающих режим и источник загрузки) осуществляется из пункта «Конфигуратор» меню «Панель управления» (см. рисунок 18).

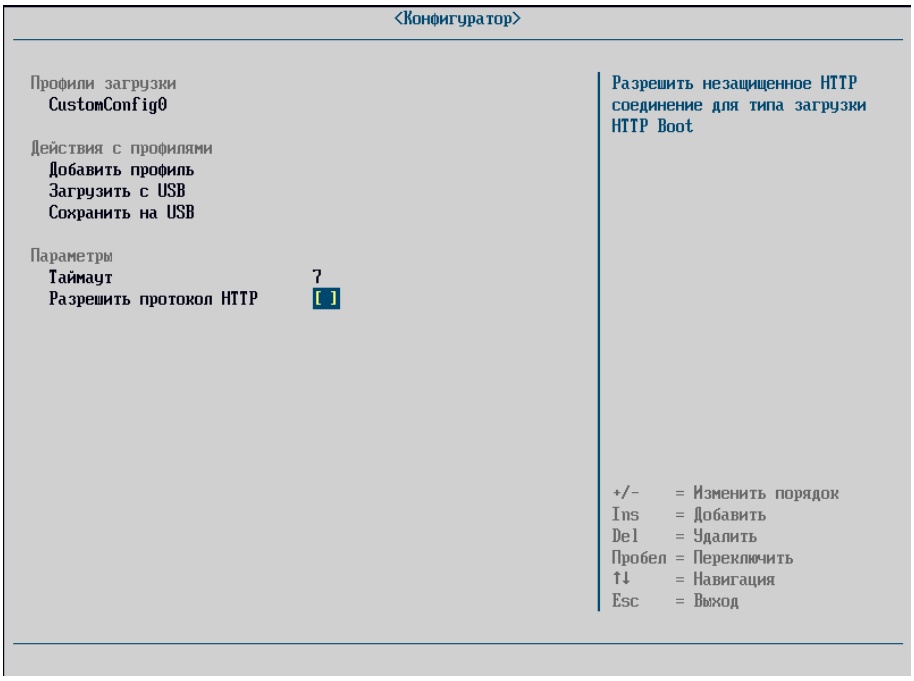

Рисунок 18 – Меню «Конфигуратор»

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

Операции управления конфигурациями загрузки осуществляются из основного пункта меню «Конфигуратор», которое содержит три секции (см. рисунок 18): «Профили загрузки», «Действия с профилями», «Параметры».

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

«Действия с профилями» содержит следующие подпункты:

– «Добавить профиль»;

– «Загрузить с USB»;

– «Сохранить на USB».

Пункт «Профили загрузки» содержит информацию о созданных профилях, и дают возможность изменять настройки профилей.

Параметр «Таймаут» предназначен для управления времени отображения главного меню, до начала старта загрузки ОС из первого профиля – минимум 1 секунда, максимум 30. При попытке ввода значения, не

попадающего в данный интервал, автоматически восстановится текущее значение таймаута. Величина этого параметра отображается в счетчике обратного отсчета на форме «Главного меню». Работа счетчика останавливается при нажатии на любую клавишу. После этого выбор и загрузка может осуществиться только вручную администратором.

Параметр «Разрешить протокол HTTP» позволяет осуществлять загрузку по сети при помощи незащищенного протокола http. Данный параметр необходимо включать только для тестирования HTTP Boot. По умолчанию загрузка ОС при профиле загрузки с HTTP Boot будет осуществляться по защищенному протоколу https.

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 возможное загрузочное устройство (см. рисунок 19);

Доступно:

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

EFI-загрузка (присутствует файл efi\boot\bootx64.efi), отображается строкой "USB Hard Drive" или "EFI USB Device";

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

– «Контроль целостности» – добавления нового файла в список проверяемых перед загрузкой ОС. Пункт меню доступен для настройки после первичного сохранения создаваемого профиля загрузки;

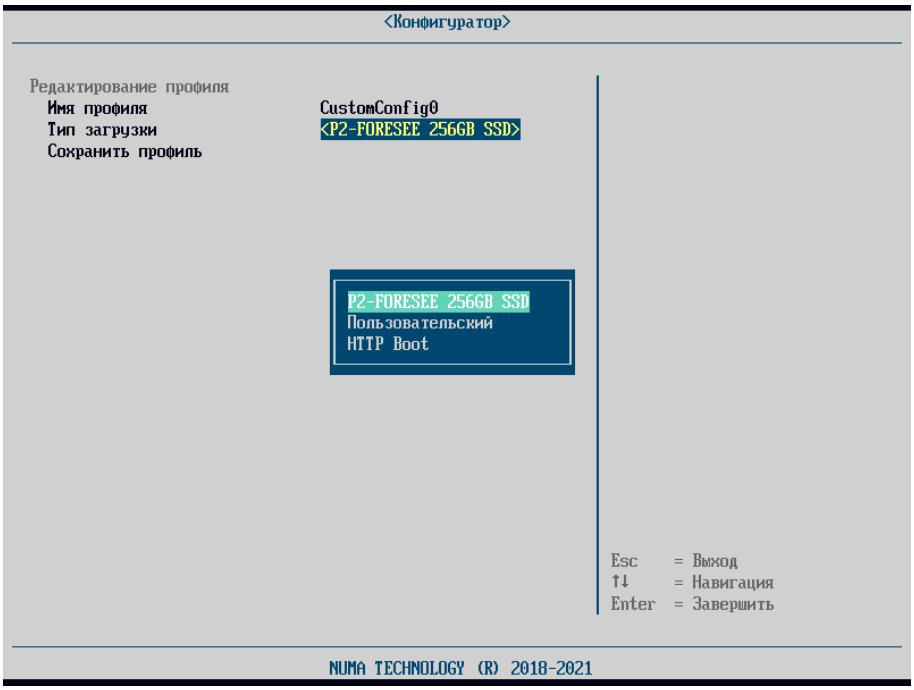

Рисунок 19 – Выбор типа загрузки

– «Сохранить профиль» – сохранение настроек профиля загрузки (см. рисунок 20).

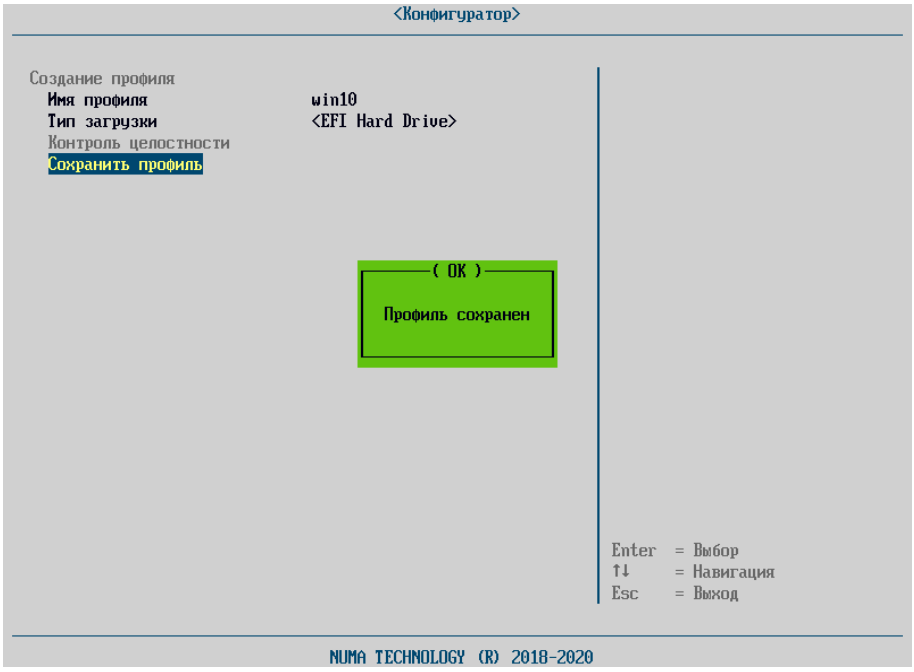

Рисунок 20 – Созданный профиль загрузки

Для управления существующими профилями необходимо перейти в пункт «Профили загрузки» меню «Конфигуратор».

4.4.2.2. Настройка профиля загрузки с типом загрузки HTTP Boot

Для возможности загрузки по HTTP Boot необходимо создать профиль загрузки. Для этого необходимо выполнить следующие действия:

1) для работы с HTTP Boot необходимо включить драйвера сетевого стека UEFI в разделе меню «Компоненты» → «Сетевой стек».

2) в меню «Конфигуратор» ввести имя профиля загрузки (произвольное);

3) в качестве типа загрузки выбрать «HTTP Boot»;

4) выбрать сетевой контролер, с помощью которого будет выполняться загрузка. Символом «*» отмечены устройства, к которым подключён сетевой кабель (см. рисунок 21).

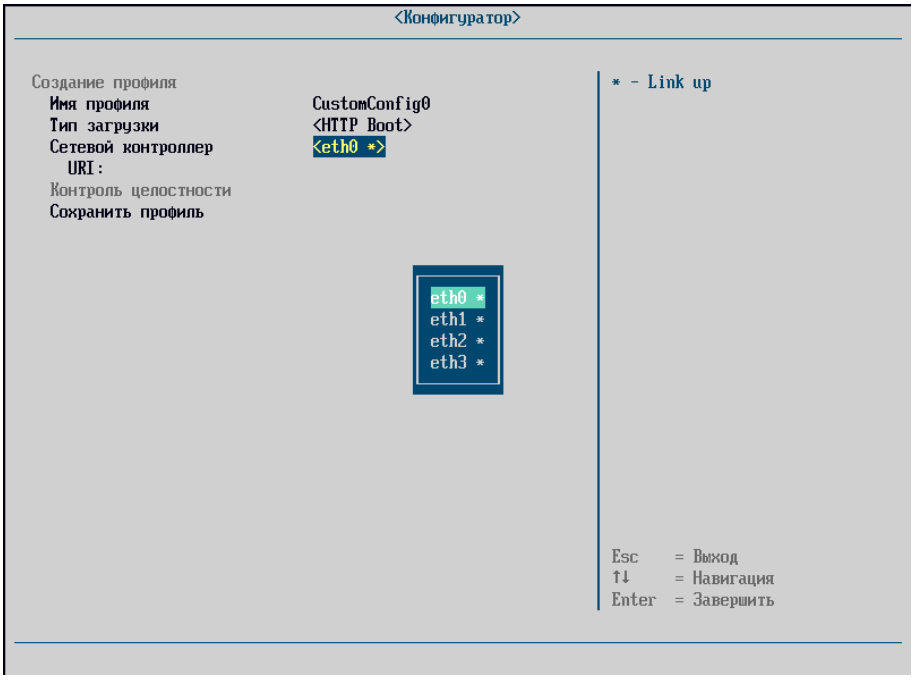

Рисунок 21 – Настройка HTTP Boot. Выбор сетевых контроллеров

5) в поле «URL» указать полный адрес загружаемого образа ОС (см. рисунок 22);

Примечание. В случае если порт отличается от стандартных (http – 80, https – 443), необходимо указать порт через двоеточие.

6) загружаемый образ должен иметь цифровую подпись для проверки его целостности и подлинности. Файл цифровой подписи должен храниться на

сервере в том же каталоге, что и загружаемый образ, и иметь имя и расширение <Filename.iso>.sign, где Filename.iso – имя загружаемого файла ОС.

Сертификат администратора безопасности для проверки цифровой подписи может быть добавлен в локальное хранилище Изделия (см. раздел 4.6.2.2.2) или же располагаться на сервере в том же каталоге, что и загружаемый образ и иметь наименование и расширение <Filename.iso>.crt, где Filename.iso – имя загружаемого файла ОС.

Корневой сертификат удостоверяющего центра должен быть заранее загружен в локальное хранилище сертификатов, после чего появится возможность загрузки локальных сертификатов администратора безопасности (см. раздел 4.6.2.2.1).

Пример построения удостоверяющего центра и инфраструктуры открытых ключей, а также процесс подписи загружаемого образа с генерацией всех необходимых для загрузки элементов приведен в Приложении 4.

*Примечание. Поддерживается форматы *.efi, *.iso, *.img для загружаемого образа ОС. Файл иного типа загружаться не будут!*

Подпись образа загружаемого файла ОС генерируется администратором на предприятии самостоятельно в доверенной ОС Astra Linux версии 1.6 и выше.

Генерация сертификатов, подписей и ключей, включая TLS – являются средствами обеспечения целостности загружаемого образа операционной системы.

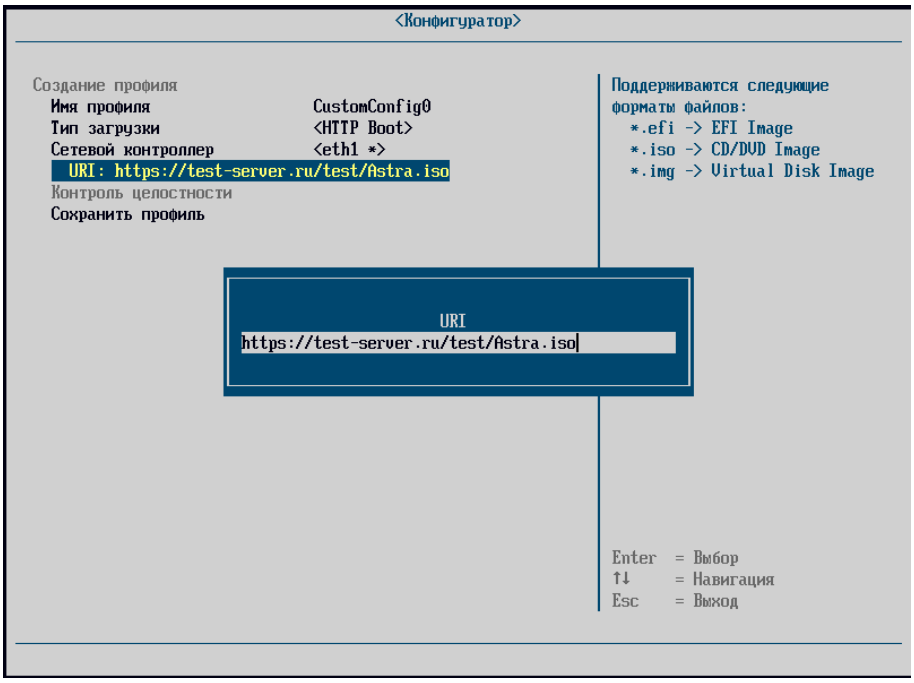

Рисунок 22 – Настройка HTTP Boot. Ввод адреса загрузки

5) По умолчанию разрешено только защищенное https соединение. В отладочных целях доступно незащищённое соединение http. Для этого необходимо включить параметр «Разрешить протокол HTTP» в меню «Конфигуратор» в разделе «Параметры».

Использование http соединения не в отладочных целях ЗАПРЕЩЕНО.

6) сохранить профиль загрузки;

7) запустить созданный профиль.

Во время загрузки с созданного профиля, сначала выполняется последовательное скачивание файлов образа, подписи и сертификата (файл сертификата загружается при необходимости).

Проверка цифровой подписи осуществляется в два этапа:

– с использованием локальных сертификатов, загруженных в «Сертификаты для HTTP Boot». Проверка будет выполняться, пока цифровая подпись не будет успешно проверена;

– если ни один локальный сертификат не подошел, будет загружен и использован сертификат с удаленного сервера (CRT-файл).

После успешного выполнения всех процедур будет выполнена загрузка

ОС.

При возникновении ошибок необходимо проверить, что сетевой кабель подключён в разъем, указанный при создании профиля загрузки, включен параметр «Сетевой стек» меню «Компоненты», убедиться в наличии и правильности всех элементов для загрузки: подписанный файл-образа ОС, файл цифровой подписи, файл сертификата для проверки цифровой подписи.

4.4.2.3. Удаление профилей загрузки

Для удаления профиля загрузки необходимо перейти на профиль загрузки и нажать кнопку «Del» (см. рисунок 23).

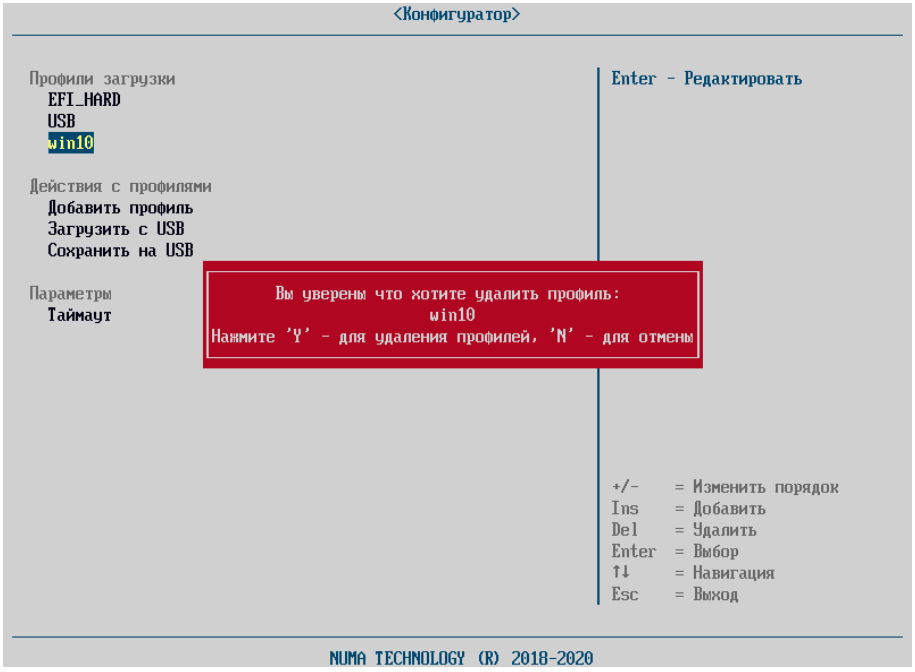

Рисунок 23 – Удаление профиля загрузки

Настройка порядка профилей загрузки в меню «Конфигуратор» осуществляется кнопками + (плюс) и – (минус).

4.4.2.4. Импорт профилей загрузки

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

– подключить USB–флеш-накопитель с файлом конфигурации;

– выбрать пункт меню «Конфигуратор» → «Загрузить с USB»;

– выбрать требуемый файл из каталога файлов устройства и нажать «Enter».

В случае успешной загрузки конфигурации будет выдано соответствующее сообщение:

`Конфигурация успешно сохранена!`

В случае выбора неподходящего файла будет выдано сообщение:

`Ошибка! Неизвестный формат файла!`

4.4.2.5. 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–флеш-накопитель (с файловой системой формата FAT32);

– выбрать пункт меню «Конфигуратор» → «Сохранить на USB».

В случае успешной выгрузки файла конфигурации будет выдано соответствующее сообщение

`Сохранение профилей завершён успешно!`

Файл с конфигурацией будет сохранен в корневом каталоге устройства с именем, соответствующим шаблону

`BootProfiles[YY-MM-DD].csv,где YYMMDD – текущая дата`

4.4.2.6. Настройка контроля целостности

Настройка контроля целостности производится в отдельном меню «Конфигуратор» → «Редактирование профиля» → «Контроль целостности» (см.рисунок 24).

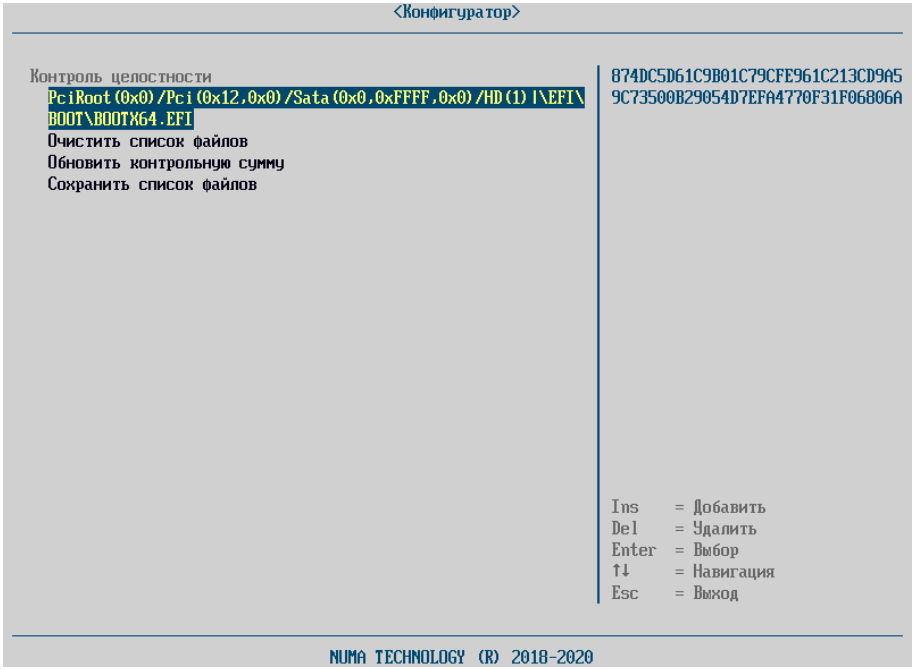

Рисунок 24 – Настройка контроля целостности

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

– выбрать пункт меню «Добавить файл в список»;

– выбрать устройство, с которого необходимо добавить файл;

– выбрать требуемый файл и нажать «Enter» – файл появится в списке добавляемых файлов, справа будет выведена его контрольная сумма (см. рисунок 24);

– для удаления файла из этого списка необходимо выделить его и нажать «Enter» (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 перечислению);

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

```
Список файлов сохранён!
```

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 системную дату и время необходимо выполнить следующие действия (см. рисунок 25):

– 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.

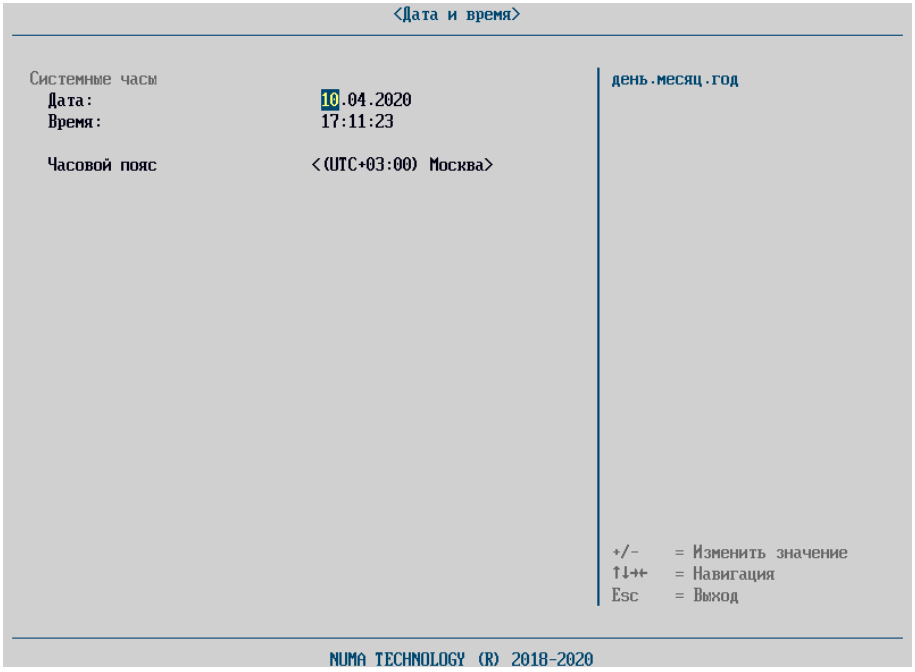

Рисунок 25 – Установка даты и времени

4.5.2. «Компоненты»

Меню «Компоненты» предоставляет возможность изменения значений следующих параметров (см. рисунок 26):

– «Удаленный терминал» – параметр для разрешения вывода информации в терминал через COM-порт;

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

– «Сетевой стек» – параметр для включения/отключения драйверов сетевого стека UEFI для загрузки по сети;

– CSM-модуль – поддержка Legacy-загрузки. Отключение ускоряет запуск БСВВ и ОС, в меню «Быстрой загрузки» перестает появляться секция Legacy-загрузки. Включение-выключение параметра позволяет включать/выключать параметр <Драйвер USB-Legacy(CSM)>;

– Драйвер USB Legacy (CSM) – подключает возможность использовать USB устройства для в режиме Legacy. Переключение значения параметра проявляется на отображение USB-устройств в секции <Legacy загрузка> в меню «Быстрой загрузки».

Примечание:

1. Исполнение 1 Изделия поддерживает неотключаемый CSM-модуль, отображение параметра отсутствует в меню «Компоненты».

2. Исполнение 3 Изделия не поддерживает CSM-модуль.

3. Для исполнения 4, 5 Изделия для активации пункта «Драйвер USB Legacy (CSM)» необходимо сначала включить пункт «CSM-модуль», только после этого пункт «Драйвер USB Legacy (CSM)» будет доступен.

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

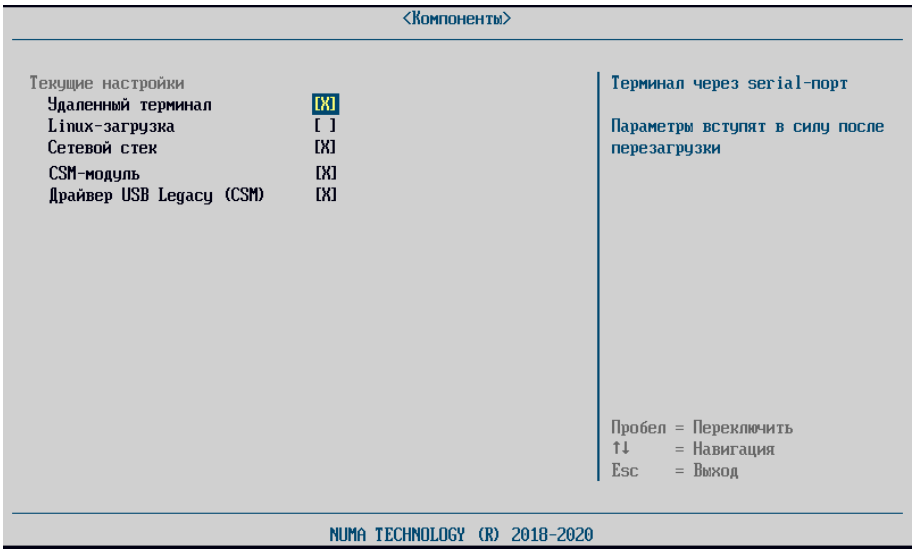

Рисунок 26 – Пункт меню «Компоненты»

Примечание. Доступные для настройки параметры меню «Компоненты» могут отличаться в зависимости от технических свойств аппаратной платформы, на которую устанавливается Изделие.

4.5.3. «Драйверы устройств»

Данный пункт позволяет просматривать драйверы устройств, установленные на СВТ, проверять правильность их работы и изменять параметры.

Список устройств, отображаемых в диспетчере, зависит от платформы, используемой в СВТ.

Список драйверов по умолчанию (независимо от платформы) включает MISC настройка платформы.

Для того чтобы настроить параметры платформы, необходимо выполнить следующие действия:

– выбрать пункт меню;
– выбрать пункт меню, соответствующий требуемому устройству;
– задать необходимые параметры;
– сохранить изменения.

4.5.3.1. ETH: настройка IPv4

Данный пункт предназначен для настройки работы сетевых протоколов (TCP/UDP) IPv4.

Изделие поддерживает автоматический режим настройки, с использование DHCP – Dynamic Host Configuration Protocol, протокол динамической настройки хостов.

4.5.3.2. MISC: настройка платформы

Настройка платформы включает в себя возможность настройки следующих параметров (см. рисунок):

– «Яркость LCD дисплея» – настройка яркости возможна в пределах: 0-25-50-75-100;

– «Разрешение LVDS» – доступные для установки разрешения: 640*480, 800*480, 1024*768, 1920*1080;

– «Поведение при потере питания» – доступные поведения «Оставить выключенным», «Включить»;

– «Скорость SATA» – доступные для установки параметры: Gen1, Gen2, Gen3.

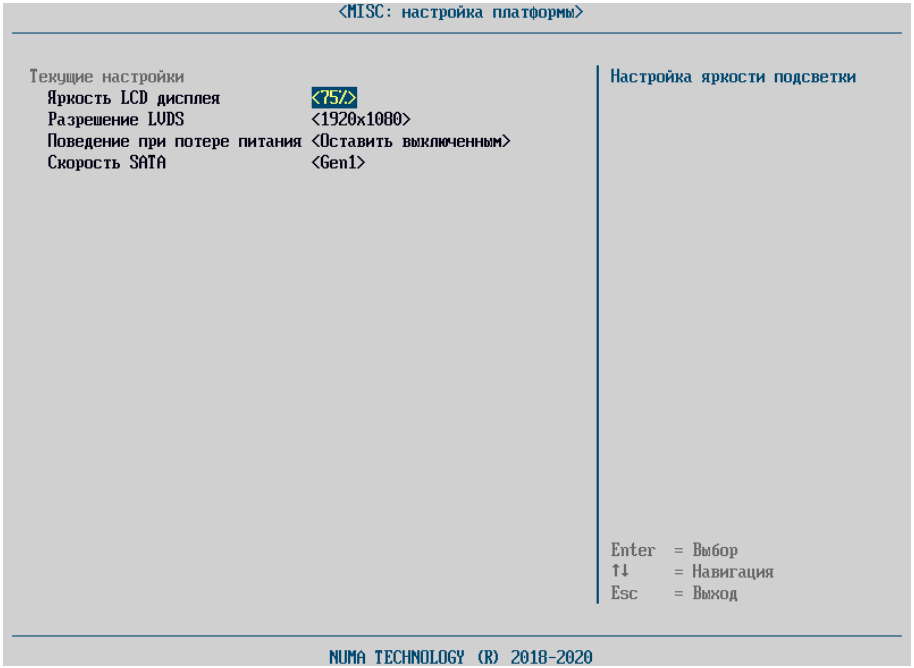

Рисунок 27 – Доступные параметры настройки платформы

4.6. Раздел «Параметры МДЗ»

4.6.1. «Пользователи»

Операции управления пользователями Изделие осуществляются из основного пункта меню «Пользователи», которое содержит три подпункта: «Профили пользователей», «Действия с пользователями», «Настройка» (см. рисунок 28). Подменю «Действия с пользователями» следующие подпункты:

– «Создать пользователя»;

– «Сохранить информацию на USB».

Подменю «Настройка» содержит подпункт «Парольная политика».

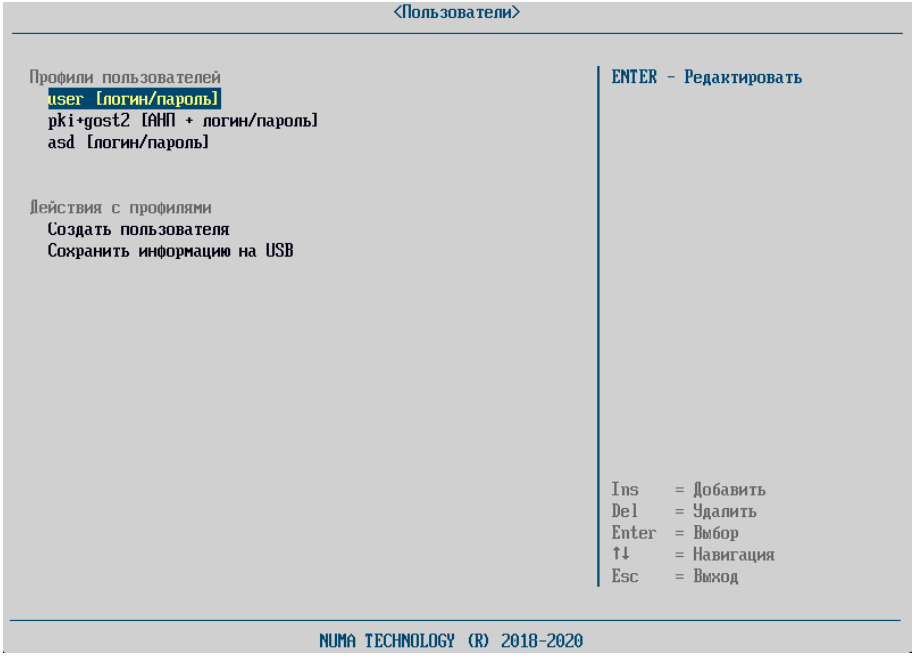

Рисунок 28 – Подпункты меню «Управление пользователями»

4.6.1.1. Создание профиля пользователя

Для создания пользователя необходимо выполнить следующие действия (см. рисунок 29):

– выбрать пункт меню «Создать пользователя» или нажать клавишу Ins (указанную в списке допустимых в правом нижнем углу экрана);

– заполнить атрибуты пользователя:

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

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

в) «Имя пользователя» – задать в окне ввода данных имя пользователя (логин). Текущие ограничения на имя пользователя: не менее 3 символов и не более 25 символов;

г) «Ф.И.О. пользователя»;

д) «Контактная информация»;

е) «Флаг блокировки» – задать при необходимости;

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

Примечание. Рекомендуется добавлять не более одного Администратора и не присваивать право «Полный доступ» без необходимости.

– для пользователя с типом авторизации «АНП» или «АНП+логин/пароль» (см. рисунок 29) требуется задать следующие поля:

– «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» или «АНП+логин/пароль»;

– «Данные сопоставления» – могут быть заданы из текстового файла с внешнего USB–носителя или с АНП. Для того чтобы ввести данные сопоставления с внешнего USB–носителя, необходимо выбрать пункт меню «Данные сопоставления» и выбрать файл с данными. Данные сопоставления необходимо задать согласно типу следующим образом:

CN (Common Name) – согласно стандарту X.509 в следующем формате: `/C= <код страны, RU>/ST = <кодсубъекта>/L = <Город>/O = <Имя организации>/OU = <Имя подразделения>/CN`

= <Имя пользователя>/emailAddress = <адрес электронной почты>;

– MAIL – по полному адресу электронной почты формата <username>@<domain.fqdn>;

– DIGEST – подпись X.509-сертификата – в формате 16-теричного числа, в форме <байт_0>:<байт_1>: … :<байт_n>;

– сохранить изменения, выбрав пункт меню «Создать».

Примечание. Для работы с АНП необходимо загрузить корневой сертификат АНП в раздел 4.6.2.

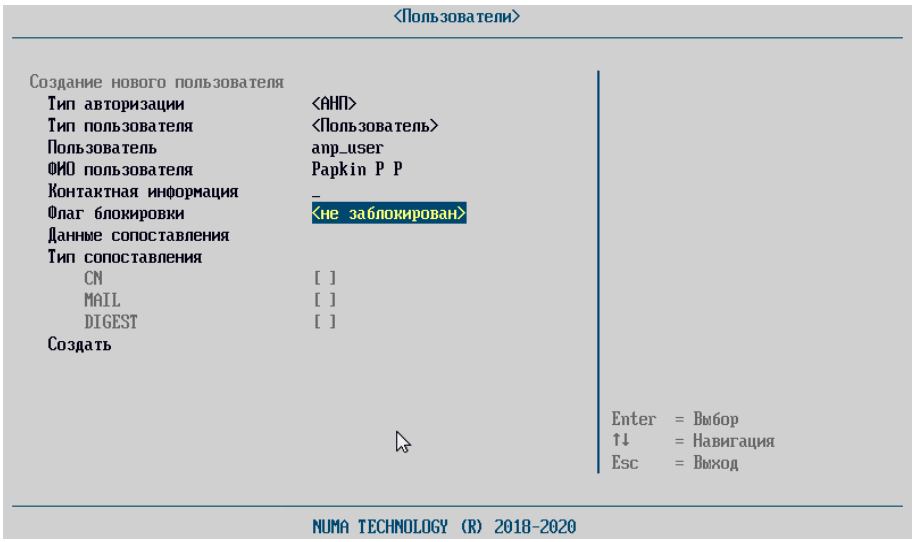

Рисунок 29 – Пример заполнения карточки пользователя с типом авторизации «АНП»

Если при заполнении карточки пользователя указаны не все атрибуты, то Изделие выдаст сообщение об ошибке и укажет поля, обязательные к заполнению (см. рисунок 30).

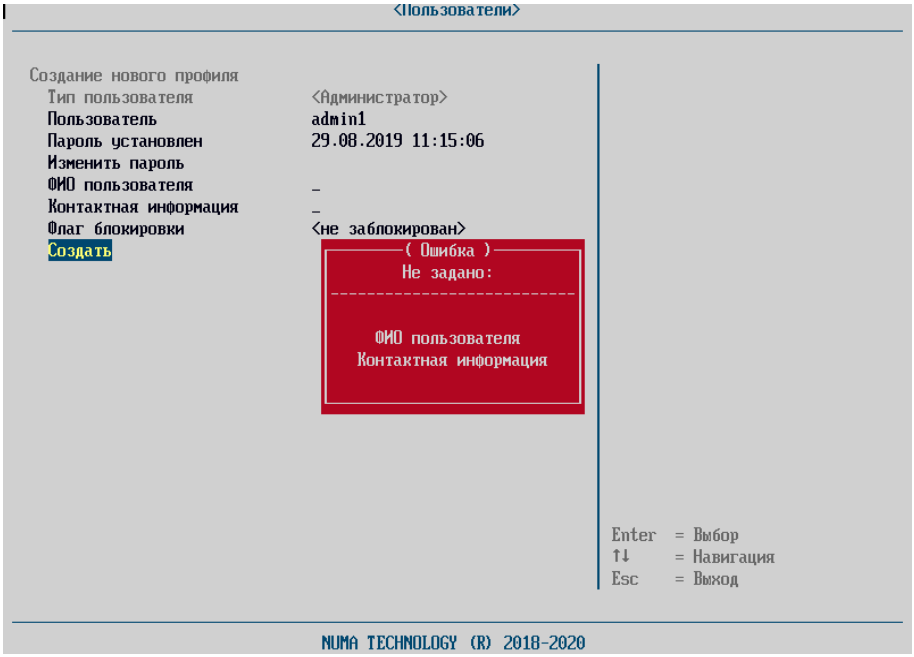

Рисунок 30 – Ошибки создания пользователей

При вводе логина уже существующего пользователя Изделие также выдаст сообщение об ошибке и не создаст пользователя (см. рисунок 31).

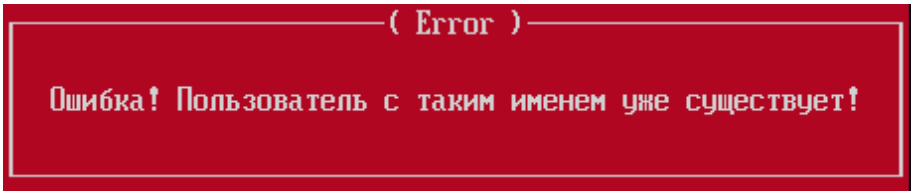

Рисунок 31 – Сообщение об ошибке при создании пользователя

При вводе пароля, не соответствующего действующей парольной политике, Изделие выдаст сообщение об ошибке и не позволит установить набранный пароль.

Примечание. Информацию о парольной политике смотрите в разделе 4.6.1.4.

4.6.1.2. Просмотр/редактирование/удаление профиля пользователя

Для просмотра/редактирования пользователей необходимо выполнить следующие действия:

– выбрать в подменю «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.

Примечание. При изменении пароля новый вариант необходимо будет ввести повторно для подтверждения (см. Рисунок 32). Если второй раз при вводе будет допущена ошибка, об этом будет выдано предупреждение:

```
Пароли не совпадают
нажмите ENTER для продолжения
```

Пароль в этом случае заменён не будет.

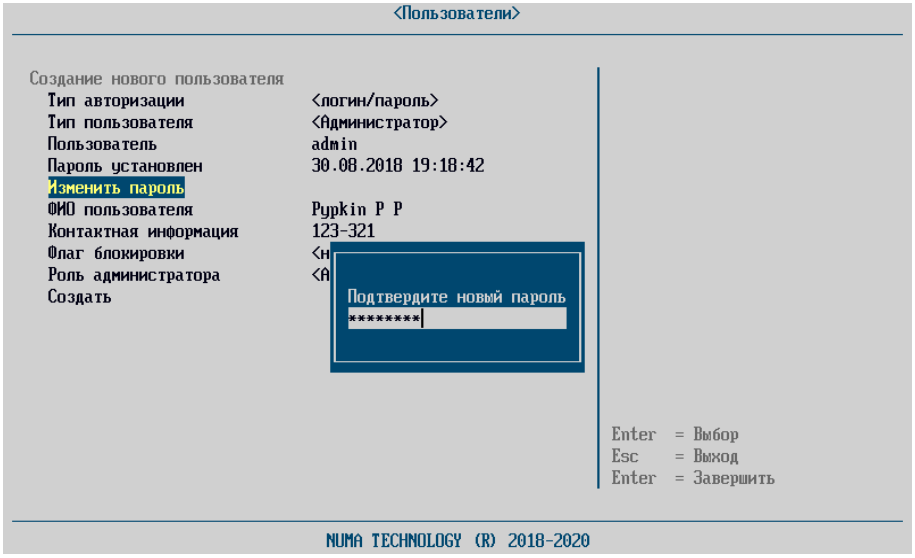

Рисунок 32 – Запрос на повторный ввод нового пароля

При успешном сохранении изменений будет выведено сообщение:

```
Пользователь успешно обновлен
```

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

```
Профиль текущего пользователя была изменен! Перезагрузка!
```

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 33).

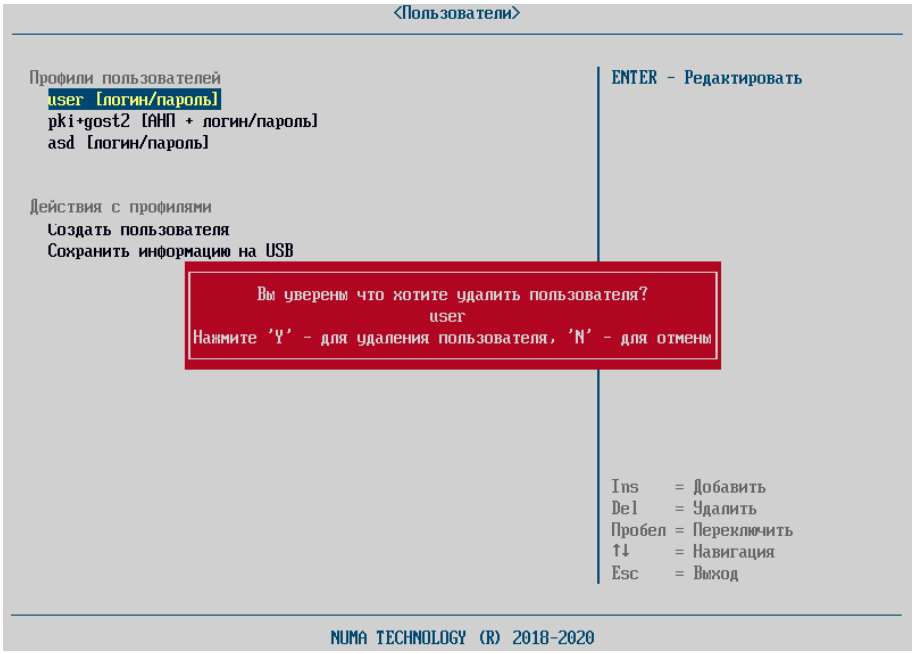

Рисунок 33 – Вид операции подтверждения удаления пользователя

4.6.1.3. Экспорт профилей пользователей

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

– подключить USB-флеш-накопитель;

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

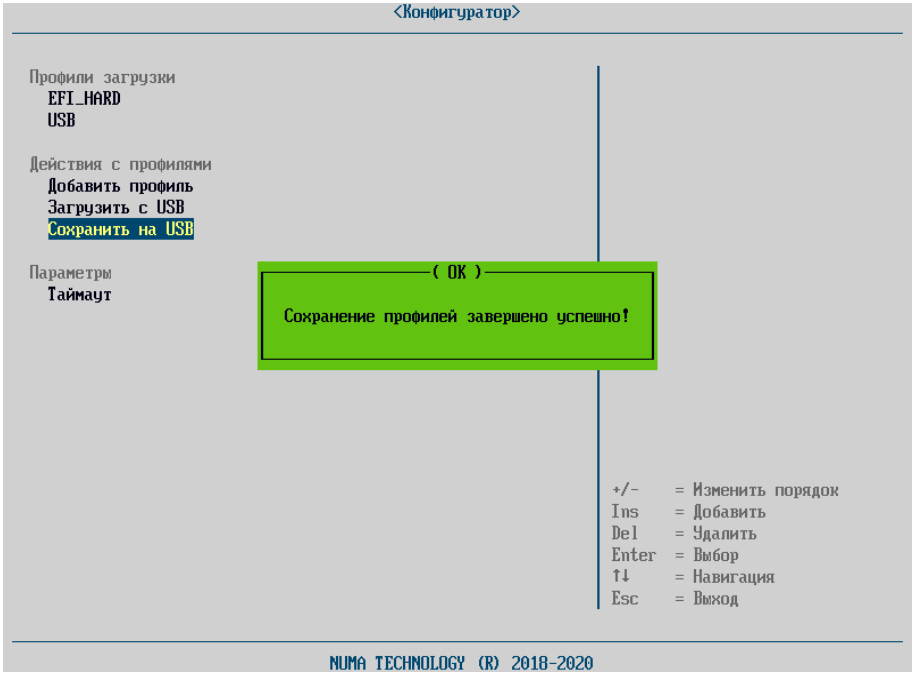

Рисунок 34 – Сообщение об успешном экспорте профилей пользователей

Примечание. При ошибке экспорта профилей пользователей на USB-флеш-накопитель необходимо проверить тип файловой системы USB-флеш-накопителя.

4.6.1.4. Политика паролей

Изделие поддерживает настраиваемую парольную политику. Для настройки парольной политики необходимо перейти в меню «Пользователи» → «Политика паролей» (см. рисунок 35).

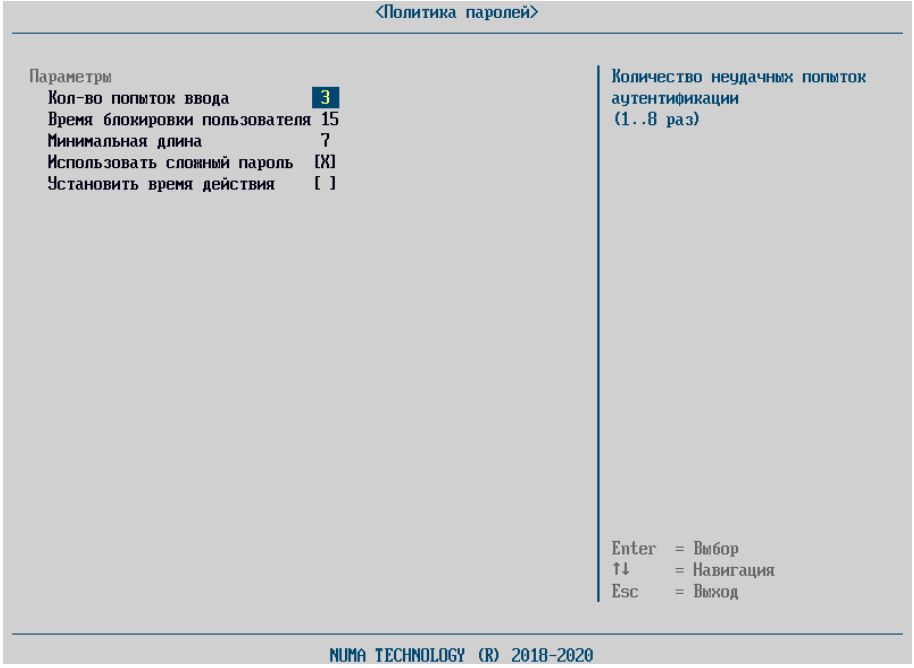

Рисунок 35 – Меню настройки парольной политики

«Количество попыток входа» – данный параметр указывает на количество неуспешных попыток аутентификации пользователя. Параметр может принимать значения от 1 до 8. При превышении числового параметра, учетная запись пользователя блокируется на время, установленное в параметре «Время блокировки».

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от доступного промежутка, Изделие автоматически установит значение числового параметра равного 3.

«Время блокировки пользователя» – параметр регламентирует время блокировки учетной записи пользователя при превышении неуспешных попыток аутентификации.

Числовой параметр времени блокировки может принимать значения от 3 минут до 60 минут.

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение

числового параметра равного 15.

«Минимальная длина» – параметр, указывающий минимально допустимую длину пароля пользователя. Числовой параметр, устанавливающий длину пароля, находится в диапазоне от 1 до 20 символов.

Для изменения числового параметра необходимо нажать клавишу «Enter» и ввести числовой параметр. При попытке ввода числового параметра отличного от допустимого, Изделие автоматически установит значение числового параметра равного 7.

«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».

«Установить время действия пароля» – параметр, отвечающий за срок действия пароля. При включении данного параметра в поле «Время действия пароля» устанавливается числовой параметр действия пароля. Числовой параметр может принимать значение от 30 до 365 дней.

По истечении срока действия пароля выводиться сообщение об истечении срока действия и необходимости смены пароля и блокируется возможность загрузки ОС.

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

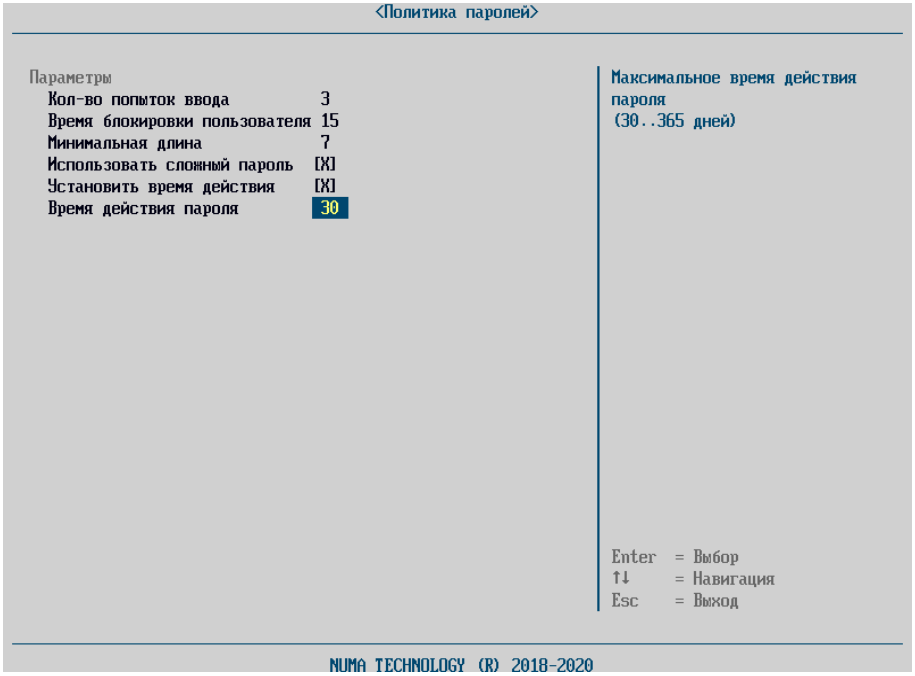

Рисунок 36 – Политика паролей. Время действия пароля

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

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.

Примечание. Значением по умолчанию являются:

- *количество попыток ввода пароля = 3;*
- *время блокировки пользователя = 15 мин;*
- *минимальная длина пароля = 7 символов;*
- *использовать сложный пароль = Вкл;*
- *ограниченное время действия = Выкл;*
- *время действия пароля = 30 дней (когда включен);*

4.6.2. «Сертификаты»

Раздел меню «Сертификаты» предназначен для работы с сертификатами для настройки процесса аутентификации типа «АНП» или

«АНП+логин/пароль» (см. п.4.6.1.1).

А также для работы с сертификатами для загрузки ОС с помощью технологии HTTP Boot.

4.6.2.1. Сертификаты для работы с АНП для аутентификации

Для возможности создания пользователя с типом аутентификации АНП или АНП+логин/пароль используются проинициализированные администратором безопасности АНП. Для данных АНП необходимо загрузить цепочку сертификатов удостоверяющего центра, а также список отозванных сертификатов.

4.6.2.1.1. Загрузка/обновление цепочки сертификатов удостоверяющего центра

Загрузка/обновления сертификата удостоверяющего центра поддерживается только с USB-флеш-накопитель. Для загрузки сертификата необходимо выполнить следующие действия:

– установить USB-флеш-накопитель в СВТ;

– выбрать в секции «Управление внутренними сертификатами», пункт меню «Текущая цепочка CA»;

– нажать клавишу «Enter» или «Ins», в запустившемся файловом обозревателе перейти в каталог, содержащий файл с цепочкой сертификатов удостоверяющего центра;

– выбрать файл цепочки сертификатов – будет выполнена загрузка сертификатов и в случае успешной загрузки/обновления цепочки сертификатов в строке меню «Текущая цепочка CA: <FILE_NAME>» будет отображено имя файла FILE_NAME, выбранного в качестве сертификата (см. рисунок 37).

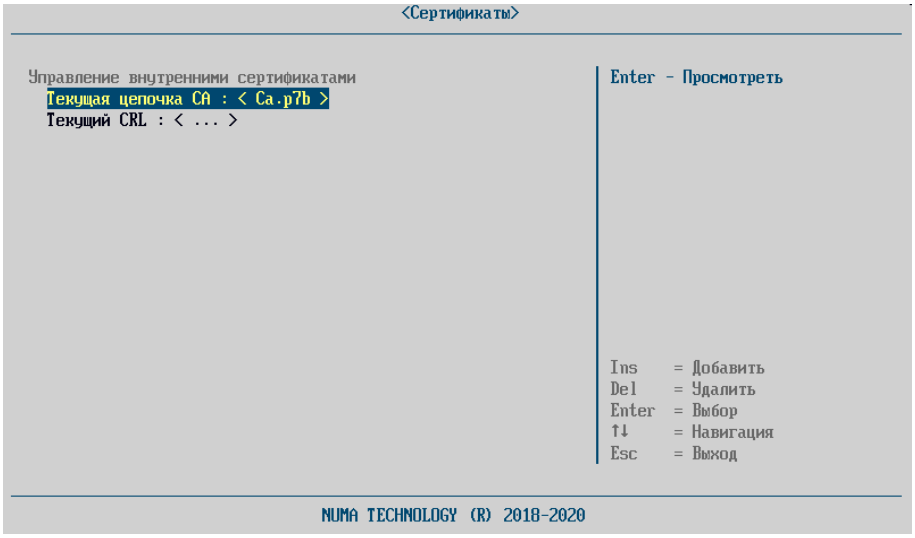

Рисунок 37 – Загрузка сертификата удостоверяющего центра

4.6.2.1.2. Загрузка/обновление списка отозванных сертификатов

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

– установить USB-флеш-накопитель в СВТ, на которое установлено Изделие;

– выбрать пункт меню «Текущий CRL»;

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

4.6.2.2. Сертификаты для загрузки ОС по технологии HTTP Boot

Для загрузки ОС по технологии HTTPBoot необходимо подготовить загружаемый образ ОС, а также корневой сертификат удостоверяющего центра, сертификат администратора безопасности, подписавшего образ загрузки. Пример построения удостоверяющего центра и инфраструктуры открытых ключей, а также процесс подписи загружаемого образа с генерацией всех необходимых для загрузки элементов приведен в Приложении 4.

4.6.2.2.1. Загрузка/обновление корневого сертификата удостоверяющего центра

Для работы с загрузкой типа HTTP Boot необходимо загрузить корневой сертификат удостоверяющего центра. Изделие поддерживает PEM и DER форматы сертификатов.

Изделие поддерживает только локальную загрузку корневого сертификата удостоверяющего центра.

Для загрузки корневого сертификата удостоверяющего центра в Изделие необходимо:

– установить USB-флеш-накопитель в СВТ, на которое установлено Изделие;

– выбрать в секции «Управление внутренними сертификатами», пункт меню «Текущая цепочка CA»;

– нажать клавишу «Enter» или «Ins», в запустившемся файловом обозревателе перейти в каталог, содержащий файл с корневым сертификатом удостоверяющего центра;

– выбрать файл корневого сертификата – будет выполнена загрузка сертификата и в случае успешной загрузки/обновления цепочки сертификатов в строке меню «Текущая цепочка CA: <FILE_NAME>» будет прописано имя файла FILE_NAME, выбранного в качестве сертификата.

После загрузки корневого сертификата удостоверяющего центра отобразится секция «Сертификаты для HTTP Boot».

4.6.2.2.2. Загрузка/обновление сертификата администратора безопасности

Сертификат администратора безопасности, подписавшего образ ОС, который должен быть загружен с помощью технологии HTTP Boot, может быть загружен локально в отобразившейся секции меню, для этого необходимо:

– установить USB-флеш-накопитель в СВТ, на которое установлено Изделие;

– перейти в секцию «Сертификаты для HTTP Boot»;

– нажать клавишу «Enter» или «Ins», в запустившемся файловом обозревателе перейти в каталог содержащий, файл сертификата;

– выбрать необходимый файл сертификата;

– после выбора сертификата наименование сертификата отобразится в секции «Сертификат для HTTP Boot». При навигации в информационном блоке справа отображается срок действия сертификата (см. рисунок 38).

Также данный сертификат администратора безопасности можно разместить на сервере, где будет расположен загружаемый образ ОС.

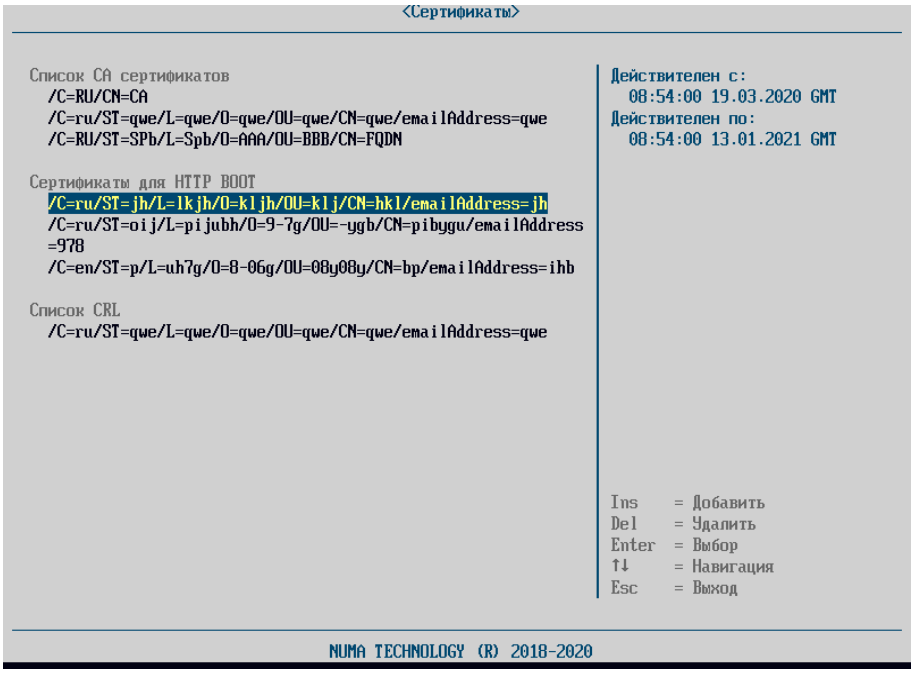

Рисунок 38 – Раздел сертификаты с указанными сертификатами для HTTP Boot

4.6.2.2.3. Загрузка/обновление списка отозванных сертификатов удостоверяющего центра

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

– установить USB-флеш-накопитель в СВТ, на которое установлено Изделие;

– выбрать пункт меню «Текущий CRL»;

– в файловом обозревателе выбрать файл, содержащий список

отозванных сертификатов – в случае успешной загрузки/обновления сертификата в строке меню «Текущий CRL: <FILE_NAME>» будет отображено имя выбранного файла FILE_NAME.

– выбрать пункт меню «Текущий CRL»;

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

4.6.3. «Журнал аудита»

Управление журналом аудита осуществляется из пункта «Журнал аудита» меню Панель управления (см. рисунок 39). Полный список регистрируемых событий приведен в Приложение 3.

Меню «Журнал аудита» содержит следующие пункты:

– «Очистить все выгруженные»;

– «Просмотр/Очистка записей»;

– «Управление журналом»;

– «Автоматическая перезапись»;

– «Сохранить на USB».

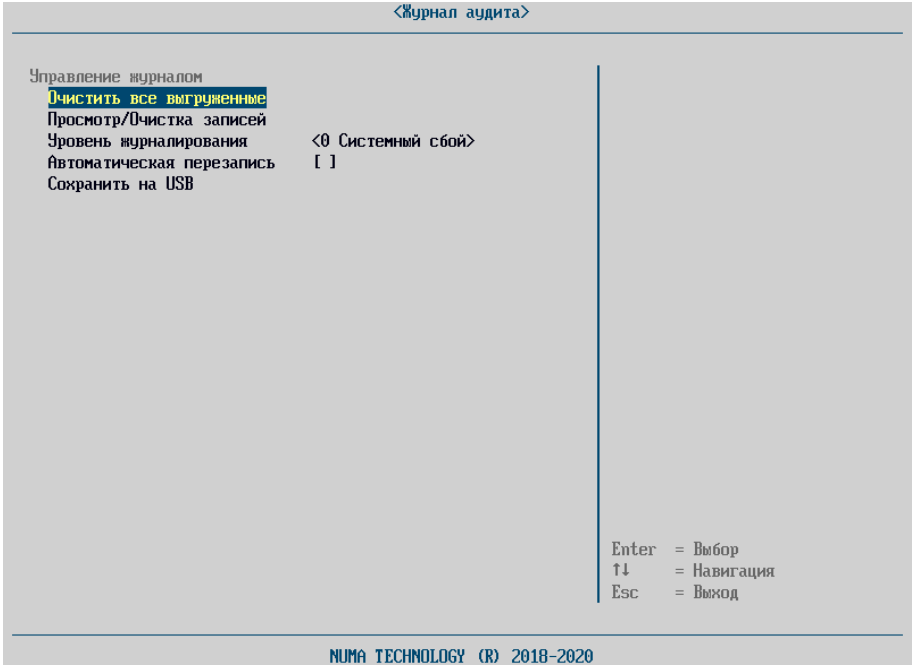

Рисунок 39 – Меню «Журнал аудита»

Команда «Очистить все выгруженные» выполняется при наличии предварительно выгруженных на внешний носитель записей. В противном случае выдаётся сообщение:

`Необходимо выгрузить журнал аудита!`

С записями в журнале можно ознакомиться, выбрав пункт «Просмотр/Очистка записей». Записи имеют следующий формат (см. рисунок 40):

– время наступления события;

– имя пользователя, действиями которого инициировано событие;

– тип события;

– код события;

– результат попытки осуществления действия (успешная или не успешная);

– описание события (произвольный текст).

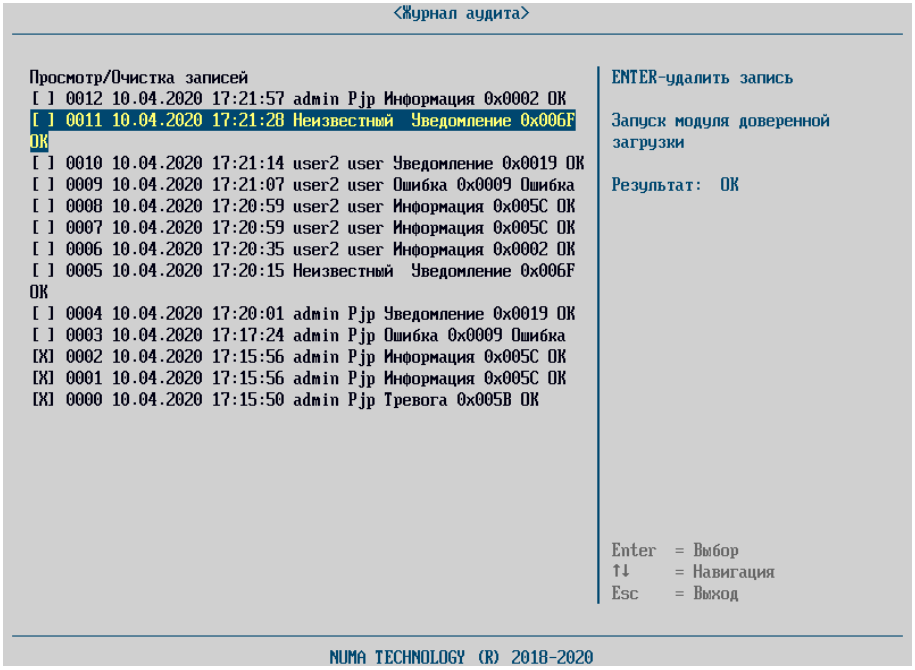

Рисунок 40 – Журнал аудита

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-флеш-накопитель, удаление будет заблокировано с выводом соответствующего сообщения:

`Невозможно удалить текущую запись!`

Для выгрузки журнала на внешний USB-флеш-накопитель необходимо вставить носитель в USB-порт ЭВМ и выбрать пункт меню «Сохранить на USB».

В случае успешной выгрузки данных будет выдано сообщение:

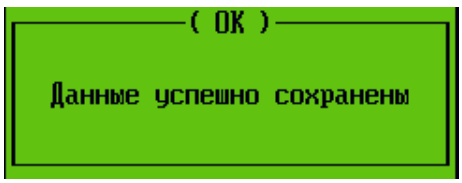

Рисунок 41 – Сообщение об успешном экспорте журнала аудита

В папке «\bios» появившейся на USB-флеш-накопителе будет создан файл с записями истории Изделия. Имя файла создается автоматически по шаблону:

`Journal[yy-mm-dd]`

где `yy-mm-dd` – текущая дата.

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

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

`Ошибка при сохранении данных`

Примечание. При ошибке экспорта на USB-флеш-накопитель необходимо проверить тип файловой системы USB-флеш-накопителя.

После успешного экспорта журнала Изделие предложит удалить уже выгруженные данные (см. рисунок 42).

Для удаление уже экспортированных данных из Изделия необходимо подтвердить их удаление путем нажатия клавиши «Y», в случае запрета необходимо нажать клавишу «Esc», которая вернет в меню «Журнал аудита».

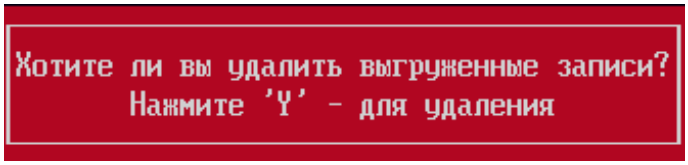

Рисунок 42 – Диалоговое окно удаление уже выгруженных данных

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

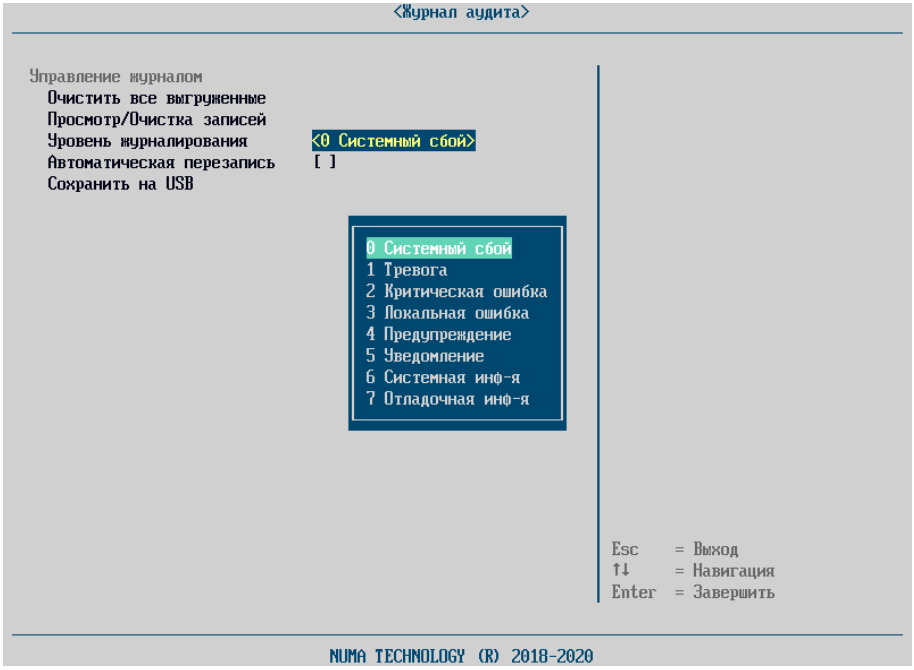

Рисунок 43 – Уровни журналирования

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

При достижении 500 записей в журнале БСВВ система блокируется, оставляя доступной только функцию выгрузки данных журнала. Выгрузку может осуществить администратор ил аудитор.

Для возможности автоматически перезаписывать невыгруженные записи при достижении предельного количества записей в журнале Изделия, можно включить функцию автоматической очистки. Для этого необходимо выставить флаг «On» в меню «Автоматическая очистка».

4.6.4. «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.

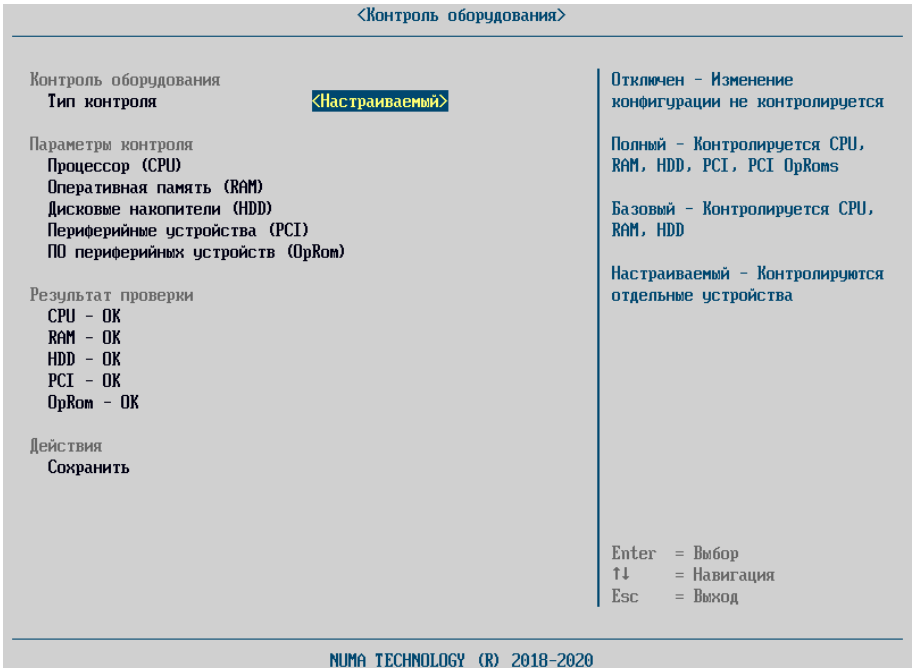

Рисунок 44 – Главное окно контроля оборудования

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

При полном контроле проверяется целостность CPU, RAM, HDD, PCI, PCI OpRoms, регион ME микросхемы SPIflash-памяти.

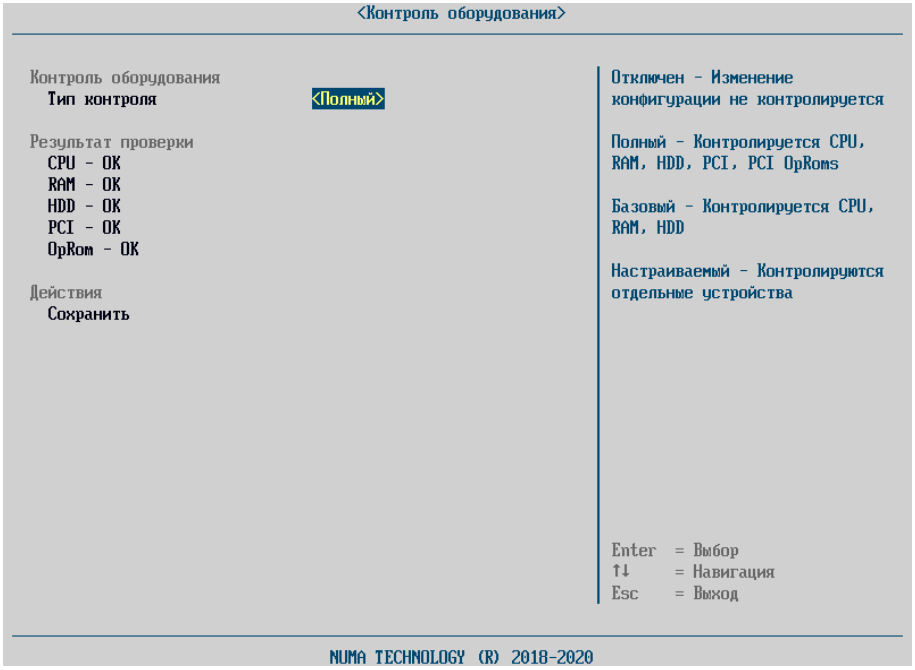

Рисунок 45 – Тип контроля оборудования «Полный»

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

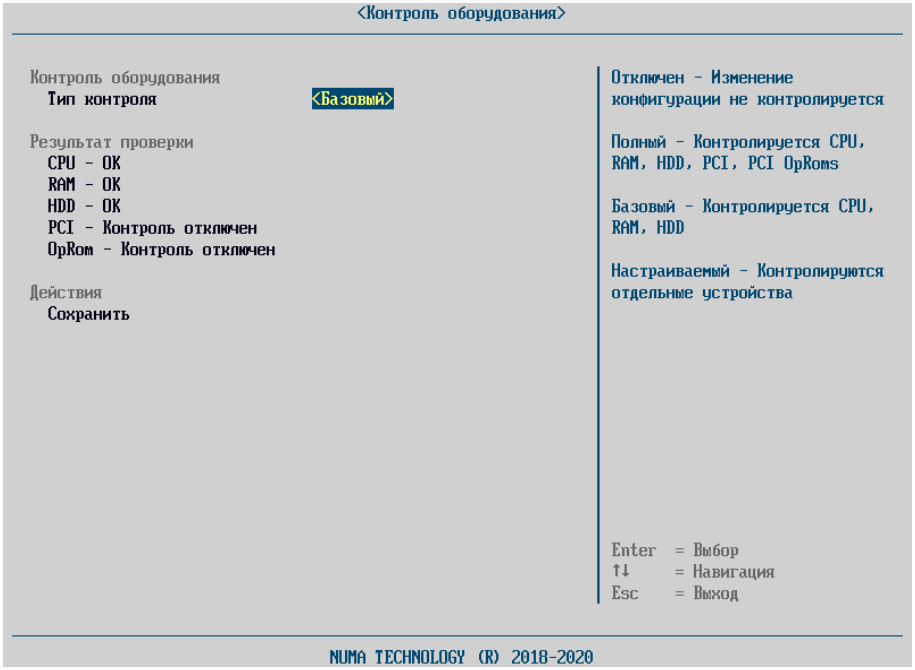

Рисунок 46–Тип контроля оборудования «Базовый»

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

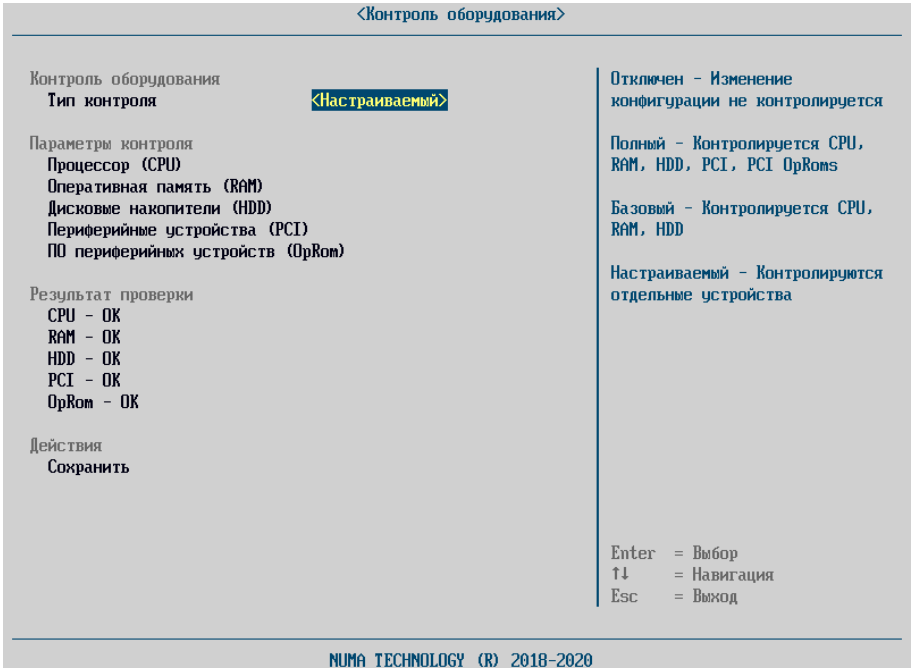

Рисунок 47 – Тип контроля оборудования «Настраиваемый»

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:

«Ошибка! Нарушена целостность оборудования!»

и загрузка ОС прекращается.

В режиме администрирования проверка целостности оборудования выполняется при каждом входе в меню контроля оборудования. Если КС аппаратной конфигурации не совпадает с сохраненной, то выдается сообщение об ошибке (см. рисунок 48).

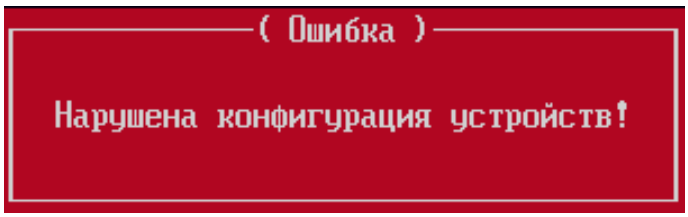

Рисунок 48 – Сообщение об ошибке контроля целостности аппаратной платформы

После входа в меню контроля оборудования можно посмотреть какой

тип устройств привел к нарушению целостности. Например, на рисунке 48 можно проследить, что к нарушению целостности привели устройства RAM (возможно, нарушение произошло из-за подключения или отключения устройства, или подключения заново устройства в другой порт).

Рисунок 49 – Меню «Контроль оборудования» с отключенным типом оборудования

Настраиваемый контроль позволяет гибко управлять контролем аппаратной платформы. Появляется возможность включения/выключения отдельных типов устройств и отдельных устройств из контроля. На рисунке 49 представлено окно контроля оборудования в режиме настраиваемого контроля.

В данном режиме доступна настройка отдельных типов устройств. На рисунке 50 представлено окно настройки параметров устройств PCI.

Рисунок 50 – Настройка параметров контроля устройств PCI

Для типов устройств доступны следующие типы контроля:

1) отключен – устройства данного типа не контролируются;

2) полный – контролируются все подключенные устройства данного типа;

3) настраиваемый – имеется возможность включения/выключения отдельных устройств из контроля целостности.

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.

4.6.5. «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 51).

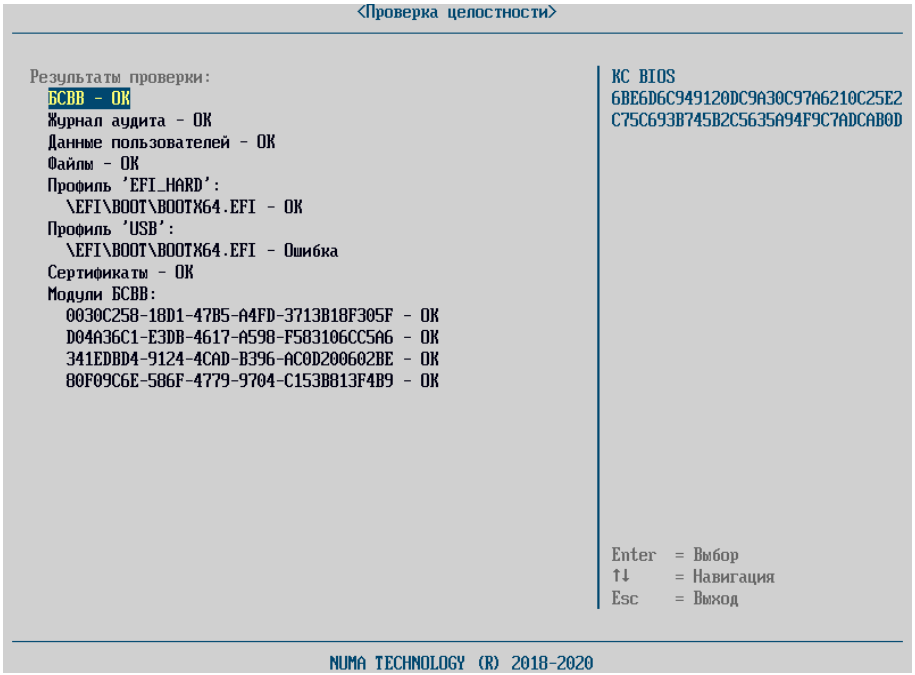

Рисунок 51 – Результат контроля целостности вручную

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

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

4.6.6. Дополнительные параметры

4.6.6.1. Проверка отзыва сертификата

Для настройки проверки отзыва сертификатов доступны следующие настраиваемые параметры:

«Использовать OCSP» – пункт меню отвечает за использование протокола OCSP (Online Certificate Status Protocol) во время процедуры верификации сертификатов. URL OCSP сервера берется из проверяемых сертификатов. OCSP запрос выполняется как при проверке пользователя (сертификата в токене), так и при создании TLS соединения, при проверке сертификата сервера;

«Сертификат OCSP» – контролирует возможность проверки отзыва сертификата подписи OCSP с помощью CLR;

«Сертификат TLS» – данное поле отвечает за проверку отзыва сертификатов с помощью CRL при установке защищенного TLS соединения к LDAP. В случае если CRL будет отсутствовать и не будет выполнен OCSP запрос, то TLS соединение не установится. Доступно три значения параметра «Не проверять», «Всю цепочку», «Только сертификат сервера».

«Проверка пользовательского сертификата» – проверка отзыва сертификата пользователя с помощью CRL;

«Использовать CDP» – отвечает за использование CDP в качестве источника CRL. При выставленном флаге в данном поле необходимо либо ввести «CDP URL», либо выставить поле «Читать CDP сертификата».

4.7. Раздел «Информация»

4.7.1. «Системная информация»

Выбрав пункт меню «Системная информация», можно получить сведения о параметрах процессоре, оперативной памяти, устройствах в SATA портах, адресах сетевых контроллеров, используемых в системе аппаратных ресурсов (см. рисунок 52).

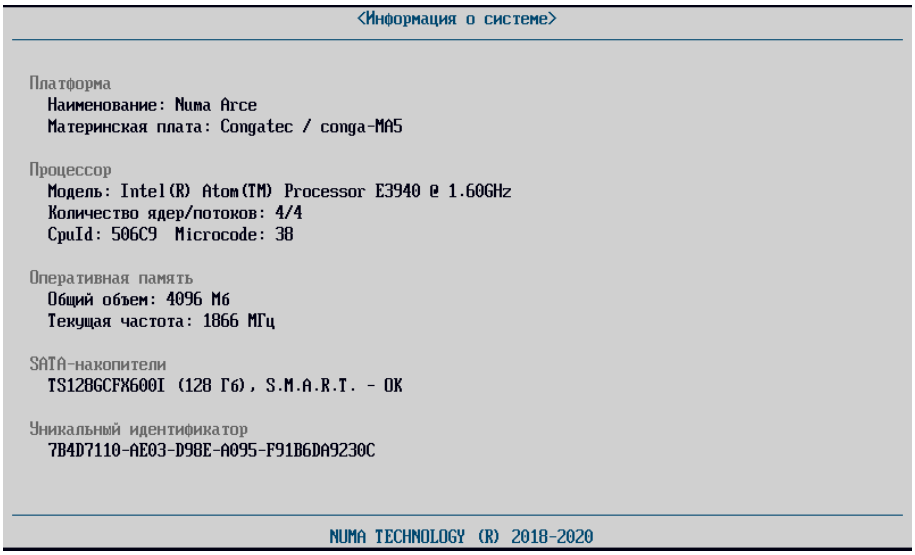

Рисунок 52 – Информация о системе

4.7.2. «Версия БСВВ»

Подменю «Версия БСВВ» показывает текущую версию прошивки БСВВ, информацию о лицензии и позволяет обновить версию Изделия с USB-флеш-накопителя (см. рисунок 53).

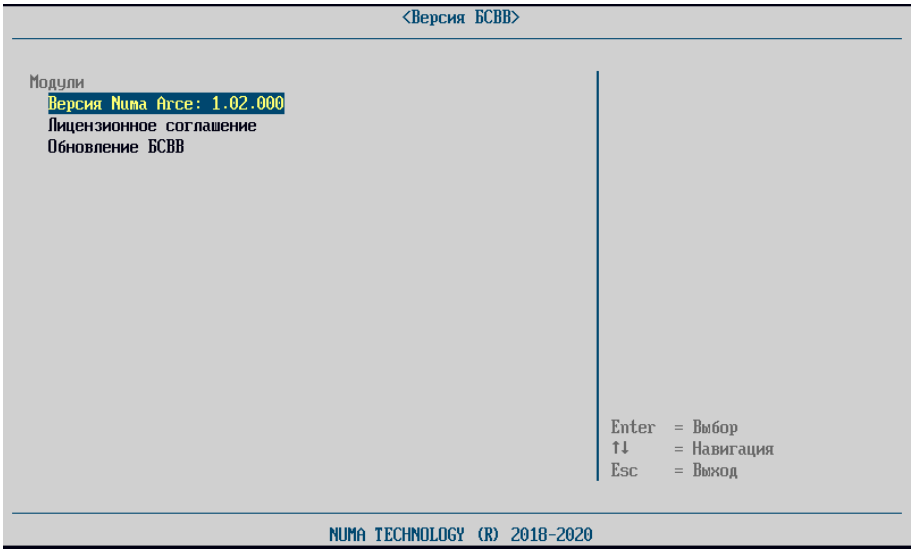

Рисунок 53 – Раздел версия Изделия

При просмотре версии Изделия указывается информация, представленная на рисунке 54.

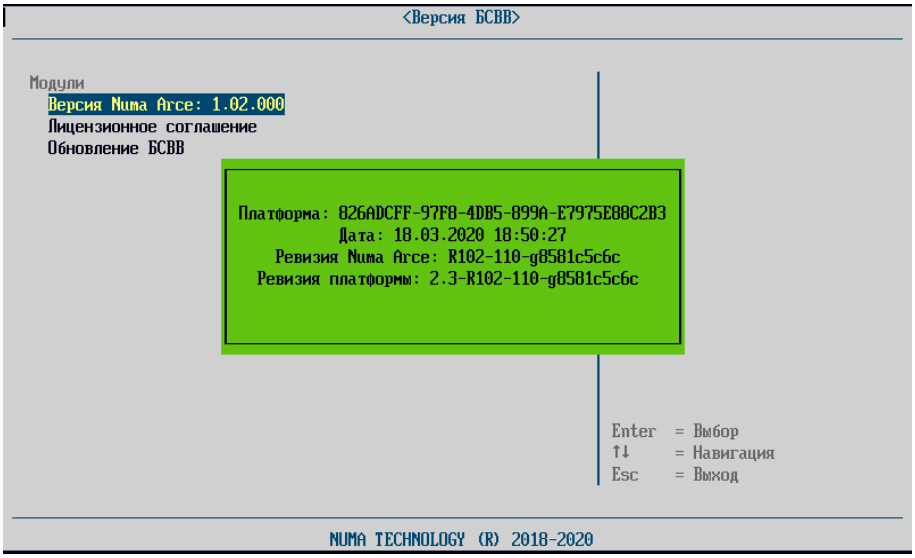

Рисунок 54 – Версия Изделия

4.7.2.1. «Обновление»

Внимание! Не допускается выключение питания во время обновления.

Примечание. Для установки/обновления Изделия требуется USB-флеш-накопитель с файловой системой FAT32.

Внимание! Процедура безопасной установки/обновления Изделия должна начинаться с проверки контрольной суммы полученного Изделия на соответствие сертифицированной версии! Процедура выполняется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00022-01 94 01.

Для обновления необходимо выполнить следующие действия:

1) выгрузить журнал аудита согласно разделу 4.6.3. Изделие не позволит начать обновление до выгрузки всего журнала аудита на USB-флеш-накопитель;

2) записать файл-прошивку, полученный от производителя ПО (или Изготовителя устройства) на USB-флеш-накопитель и подключить к аппаратной платформе;

3) включить СВТ;

4) в меню «Панель управления» выбрать подменю «Версия БСВВ» –

«Обновление БСВВ»;

5) в открывшемся списке файлов выбрать файл прошивки и нажать «Enter»;

6) в появившемся окне подтвердить проведение обновления;

Рисунок 55 – Диалоговое окно обновления

7) в появившемся окне «Обновить EFI-переменные?», нажать «Y»;

8) подтвердить действия нажатием «Enter» в следующем окне;

9) начнется запись образа прошивки в флеш-память.

По окончании обновления будет показано сообщение (см. рисунок 56) и СВТ будет выключен.

Рисунок 56 – Сообщение об успешном обновлении Изделия

При выборе несоответствующего данной аппаратной платформе бинарного файла обновления Изделие выдаст сообщение об ошибке (см. рисунок 57).

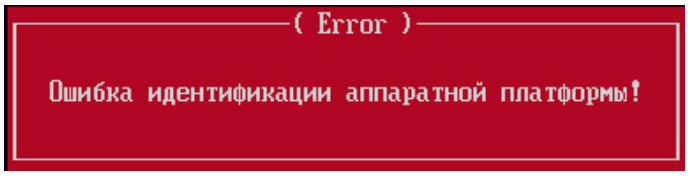

Рисунок 57 – Сообщение о некорректном файле обновления Изделия

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

Сообщение	Описание	Действие
«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 Flash-диска	Вставить USB Flash-диск в USB-порт
«Ошибка восстановления: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск 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 Flash–диска	Вставить USB Flash–диск в USB–порт
«Ошибка восстановления: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск с поддерживаемой файловой 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
«Количество попыток авторизации на АНП истекло»	Было осуществлено количество неудачных попыток авторизации, которые привели к блокировке АНП	Обратиться к администратору безопасности или ответственному человеку для разблокирования АНП
«Пользователь <USER_NAME> удален»	Успешное удаление пользователя	

Сообщение	Описание	Действие
«Ошибка выгрузки: нет носителя»	Нет USB Flash–диска	Вставить USB Flash–диск USB–порт
«Ошибка выгрузки: неподдерживаемый носитель»	USB Flash–диск имеет неподдерживаемую файловую систему	Предъявить диск с поддерживаемой файловой системой
«Нет CD/DVD–ROM носителя»	Отсутствует носитель	Вставить инсталляционный носитель
«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

Сообщение	Описание	Действие
«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
«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=11223344556677889900112233445566778899001122334455667788990011223344556677889900112
```

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 CSV-файле.

Порядок следования полей в общем случае указан в таблице 2.1, для пользователей «логин/пароль» – в таблице 2.2, для пользователей «АНП» – в таблице 2.3.

Таблица 2.1 – Порядок следования полей в общем случае

Поле	Описание поля
Тип аутентификации	Возможные значения: – 0 – логин пароль; – 1 – АНП; – 3 – АНП + логин пароль.
Тип пользователя	Возможные значения: – 0 – пользователь; – 1 – администратор
Имя пользователя	login
ФИО пользователя	в юникоде не более 25 символов
Контактная информация	в юникоде не более 50 символов

Таблица 2.2 – Порядок следования полей для пользователей «логин/пароль»

Поле	Описание поля
Тип хэш-суммы	Возможные значения: 4 – ГОСТ Р 34.11-2012
Дата задания пароля пользователя	YYYY-MM-DD_HH:MM:SS
Хэш-значение пароля	строка

Таблица 2.3 – Порядок следования полей для пользователей «АНП»

Поле	Описание поля
Тип данных сопоставления	Возможные значения: – CN; – MAIL; – DIGEST
Значение данных сопоставления	Строка

Пример для пользователя типа «логин пароль»:

```
0;1;adm555;Stepanov I.V.;NUMA;04;2011-02-
15_14:08:32;25DEDBD14BB3A6A5DC0174D7D233740A10A159F3B25AC
BCB96DA829303701F2F
```

Пример для пользователя типа «АНП»:

```
1;1;token_111;Stepanov I.V.;NUMA;CN;NUMA Client1
Certificate
1;1;token_222;Stepanov I.V.;NUMA;CN;NUMA Client2
Certificate;DIGEST;11223344556677889900112233445566778899
00112233445566778899001122
```

ПРИЛОЖЕНИЕ 3

Справочное

СПИСОК СОБЫТИЙ, РЕГИСТРИРУЕМЫХ В ЖУРНАЛЕ

Код события	Мнемоника	Уровень критичности		Описание
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) Ошибка (error)	Создание (добавление) нового пользователя, заносится в журнал при каждой записи во флеш новой карточки пользователя
0x0004	HEVENT_DELETE_USER	6/3	Информация (info) Ошибка (error)	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
0x0008	HEVENT_EXPORT_HISTORY_TO_USB	7	Отладочная (debug)	Выгрузка журнала аудита на USB, заносится при выборе пункта меню, осуществляющего сохранение информации журнала на USB
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_L	6/3	Информация (info)	Старт запуска ОС, событие заносится в журнал перед

Код события	Мнемоника	Уровень критичности		Описание
	OAD_OS		Ошибка (error)	каждой загрузкой ОС с результатом «успех» и в случае если загрузка ОС не прошла, т. е. вернулись из загрузчика в БСВВ с результатом «Ошибка»
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 накопитель
0x0010	HEVENT_ADMIN_MODE_EXIT	7	Отладочная (debug)	Выход из меню "Панель управления", заносится в журнал при выборе профиля загрузки
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_M	7	Отладочная	Выход из меню управления пользователями

Код события	Мнемоника	Уровень критичности		Описание
	ODE_EXIT		(debug)	
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, заносится в журнал при нажатии ESC в меню "Панель управления" с дальнейшей перезагрузкой
0x001A	HEVENT_TOKEN_EJECTED	5	Уведомление (notice)	Уведомление об извлечении токена
0x001B	HEVENT_BIOS_UPDATE_MODE_ENTER	7	Отладочная (debug)	Вход в пункт меню «ВерсияБСВВ\обновления БСВВ»
0x001C	HEVENT_BIOS_UPDATE_MODE_EXIT	7	Отладочная (debug)	Выход в пункт меню «ВерсияБСВВ\обновления 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

Код события	Мнемоника	Уровень критичности		Описание
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
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»
0x003E	HEVENT_MAX_WRONG_PIN_REACHED	2	Критическая ошибка (critical)	Достигнуто максимальное количество подряд неверно введённых ПИН-кодов для токена
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_R	3	Ошибка (error)	Сертификат отозван

Код события	Мнемоника	Уровень критичности		Описание
	EVOKED			
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
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
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

Код события	Мнемоника	Уровень критичности		Описание
0x0050	HEVENT_BOOT_CFG_CHANGE	6/3	Информация (info) Ошибка (error)	Изменение профиля 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
0x005B	HEVENT_HISTORY_SEVERITY_LVL_CHANGE	1	Тревога (alert)	Изменение уровня записи в журнал
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 меню «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 (info)	Загрузка профиля загрузки
0x0060	HEVENT_ADMIN_BOOT	6	Информация (info)	Выбор пункта меню "Панель управления"
0x0063	HEVENT_BOOT_MNGR_IMPORT_OPT	6	Информация (info)	Импорт профилей загрузки с USB накопителя
0x0064	HEVENT_BOOT_MNGR_EXPORT_OPT	6	Информация (info)	Импорт профилей загрузки на USB накопитель

Код события	Мнемоника	Уровень критичности		Описание
0x0065	HEVENT_REVOKE_CERTS_CFG_CHANGED	6	Информация (info)	Изменение конфигурации настройки отзыва сертификатов
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 OpenSSL
0x006F	HEVENT_NUMA_ARCE_START	5	Уведомление (notice)	Запуск модуля доверенной загрузки
0x0070	HEVENT_RESET_BIOS_TO_MII	0	Ошибка системы (emergency)	Сброс настроек БСВВ
0x0071	HEVENT_HW_MONITOR_FAIL	3	Ошибка (error)	Нарушена целостность оборудования
0x0076	HEVENT_PASSWD_GUESSING	1	Тревога (alert)	Подбор пароля

Код события	Мнемоника	Уровень критичности		Описание
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_HW_MONITORING_ON	6	информация (info)	Включен контроль оборудования
0x008B	HEVENT_HW_MONITORING_OFF	6	информация (info)	Контроль оборудования отключена
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
0x00A6	HEVENT_LOAD_TLS_CLIENT_CERT	6	информация (info)	Добавлен клиентский сертификат TLS
0x00AA	HEVENT_PASSWORD_POLICY_CHANGED	5	уведомление	Изменение параметра парольной политики
0x00AB	HEVENT_LOAD_HTTP_BOOT_CERT	6	Информация (info)	Загрузка доверенного сертификата для проверки целостности образа загружаемого по HTTP Boot

Код события	Мнемоника	Уровень критичности		Описание
0x00AC	HEVENT_HTTP_BOOT_ ALLOW_INSECURE	6	Информация (info)	Изменение настроек HTTP Boot: изменение настройки протокола HTTP

ПРИЛОЖЕНИЕ 4

Инструкция по генерации ключей и сертификатов в ОС Astra Linux версии 1.6 и выше для работы с технологией HTTP Boot в Numa Arce

Данный раздел описывает основные настройки для построения инфраструктуры открытых ключей (PKI) с помощью библиотеки OpenSSL в ОС Astra Linux версии 1.6 и выше для работы с технологией HTTP Boot в модуле доверенной загрузки Numa Arce 643.АМБН.00022-01.

1. Предварительная подготовка АРМ с ОС Astra Linux версии 1.6 и выше

Для работ по генерации ключей и сертификатов в ОС Astra Linux необходимо:

– установить пакет библиотек libgost-astra;

– настроить конфигурационный файл;

– создать инфраструктуру УЦ для генерации ключей и сертификатов.

1.1. Установка и настройка пакета библиотек libgost-astra

В состав дистрибутива ОС Astar Linux версии 1.6 и выше (далее - ОС Astra Linux) входит пакет библиотек libgost-astra для выполнения защитного преобразования по алгоритмам ГОСТ.

Для установки данного пакета необходимо:

– вставить установочный диск для ОС Astra Linux версии 1.6 и выше в дисковод;

– авторизоваться под административным пользователем;

– выполнить команду для установки пакета библиотек;

```
apt install libgost-astra
```

– или выполнить установку с помощью графического менеджера пакетов Synaptic (менеджер пакетов устанавливается автоматически при установке ОС и доступен через меню «Пуск» → «Панель управления» → «Программы» → «Менеджер пакетов Synaptic»):

– найти пакет libgost-astra;

– поставить метку "установить";

– нажать кнопку "Применить";

– следовать подсказкам установщика.

Установленный пакет libgost-astra обеспечивает включение в состав методов защитного преобразования, поддерживаемых пакетами OpenSSL, следующих алгоритмов:

– ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 - алгоритмы цифровой подписи;

– поддерживается обмен ключами, основанный на открытых ключах (см. RFC 4357).

Алгоритмы используют

– Закрытые ключи 256 бит для ГОСТ Р 34.11-2001, и 256/512 бит для ГОСТ Р 34.11-2012;

– Открытые ключи 512 бит для ГОСТ Р 34.11-2001 и 512/1024 для ГОСТ Р 34.11-2012;

– ГОСТ Р 34.11-94 алгоритм хеширования. Хэш 256 бит;

– ГОСТ Р 34.11-2012 алгоритм хеширования. Хэш 256 и 512 бит;

– ГОСТ 28147-89 - Симметричное защитное преобразование с ключем 256 бит; Реализованы режимы CBC, CFB и CNT, поддерживается алгоритмы "key meshing" (см. RFC 4357);

– ГОСТ 28147-89 в режиме выработки имитовставки. Базируется на алгоритме симметричного защитного преобразования. Симметричный ключ 256 бит и разрядность вставки от 8 до 64 бит (по умолчанию 32 бит).

– ГОСТ Р 34.13–2015 - Симметричное защитное преобразование «Кузнечик».

1.2. Настройка файла конфигурации с поддержкой ГОСТ алгоритмов

1.2.1. Автоматическая настройка конфигурационного файла

При установке пакета библиотек OpenSSL образец стандартного конфигурационного файла копируется в архив с образцом конфигурации, расположенным /usr/share/doc/libgost-astra/openssl.cnf.gz.

Для распаковки архива в файл конфигурации /etc/ssl/openssl.cnf необходимо выполнить команду:

```
gunzip -c /usr/share/doc/libgost-astra/openssl.cnf.gz |
sudo tee /etc/ssl/openssl.cnf > /dev/null
```

Примечание. Конфигурационный файл заменит существующий (в случае если он был), все внесенные изменения будут уничтожены.

1.2.2. Ручная настройка конфигурационного файла

Для ручного изменения конфигурации после установки пакета libgost-astra в конфигурационном файле OpenSSL (/etc/ssl/openssl.cnf) необходимо выполнить следующие действия:

– добавить в начало конфигурационного файла /etc/ssl/openssl.cnf строку

```
openssl_conf = openssl_def
```

– в конец конфигурационного файла добавить строки:

```
[openssl_def]
engines = engine_section

[engine_section]
gost-astra = gost_section

[gost_section]
engine_id = gost-astra
dynamic_path = /usr/lib/x86_64-linux-gnu/engines-
1.1/gost-astra.so
default_algorithms = ALL
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

1.3. Дополнительные изменения в конфигурационный файл

В конфигурационном файле /etc/ssl/openssl.cnf в секции [CA_default]

необходимо изменить значение директивы "dir = ./demoCA" на "dir = ./".

```
[ CA_default ]
dir = ./
```

В дальнейших настройках данный каталог будет использоваться по умолчанию.

В примере будут использоваться расширения для генерации сертификатов. Необходимо убедиться, что расширения включены в стандартном конфигурационном файле, для этого необходимо убедиться, что в конфигурационном файле /etc/ssl/openssl.cnf имеются записи вида (строки должны быть раскомменированы, т.е. должны отсутствовать любые знаки типа «#» до начала строки):

```
[ usr_cert ]
# Эти расширения будут добавлены при подписывании запроса
нашим УЦ.
basicConstraints=critical,CA:false
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
nsComment = "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

[ v3_ca ]
# Расширения для типового УЦ
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = critical,CA:true
keyUsage = cRLSign, keyCertSign
```

Для работы с шаблоном для списка аннулированных сертификатов формата CRL V2 необходимо убедиться, что в конфигурационном файле /etc/ssl/openssl.cnf имеется строка (строка должна быть раскомменирована, т.е. должны отсутствовать любые знаки типа «#» до начала строки) вида:

```
crl_extensions = crl_ext
```

2. Создание удостоверяющих центров для генерации и работы с

сертификатами

2.1. Создание однорангового удостоверяющего центра

Для создания однорангового удостоверяющего центра (далее - УЦ) необходимо осуществить следующие действия:

– создать ключ УЦ;

– создать сертификат УЦ;

– создать ключ клиента;

– создать запрос на сертификат администратора;

– выпустить сертификат для администратора на основе запроса;

– создать списка отзыва сертификатов.

1) Создаем каталог (CA) для удостоверяющего центра, устанавливаем безопасные права доступа. Задаем значение параметра «umask» таким образом, чтобы вновь создаваемые файлы имели права доступа чтения и записи только для создавшего их пользователя:

```
mkdir CA
chmod u=rwx,g=,o= CA
cd CA
umask 066
```

2) Создаем структуру каталогов и файлов для УЦ:

```
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
touch index.txt.attr
echo 1000 > serial
```

Примечание. Файлы index.txt и serial необходимы, чтобы отслеживать статус выпущенных закрытых ключей и сертификатов.

3) Создаем закрытый ключ (private/rootca.key) для УЦ. В качестве алгоритма для закрытого ключа используется алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt
paramset:A –out private/rootca.key
```

ВНИМАНИЕ! Закрытый ключ корневого сертификата удостоверяющего центра является наиболее секретным элементом инфраструктуры открытых ключей и должен быть надежно защищен.

4) Изменяем права доступа к файлу «только на чтение» для пользователя, который сгенерировал данный ключ:

```
chmod 400 private/rootca.key
```

5) Выпускаем корневой сертификат УЦ (certs/rootca.crt) (далее CA сертификат), который подписывается закрытым ключом private/rootca.key. Для закрытого ключа в сертификате используется алгоритм ГОСТ Р 34.10-2012 с длинной ключа 256 бит.

```
openssl req -new -x509 -md_gost12_256 -days 365 -
extensions v3_ca -key private/rootca.key -out
certs/rootca.crt \
-subj /C=RU/ST=SPb/L=SPb/O=ExampleInc/OU=ITdept/CN=ca-
server
```

Примечание. Параметр ***–days*** *установлен на* ***365****, что означает, что сертификат действителен в течение следующих 365 дней. Для изменения срока действия сертификата необходимо заменить числовое значение 365 на необходимое.*

Корневой сертификат является сертификатом самого удостоверяющего центра и используется для подписи и удостоверения подлинности других сертификатов. Является самоподписанным.

6) Изменяем права на данный CA сертификат:

```
chmod 444 certs/rootca.crt
```

7) Просмотреть содержимое CA сертификата можно командой:

```
openssl x509 -in certs/rootca.crt -noout -text
```

8) Генерируем закрытый ключ для сертификата администратора безопасности (private/admin.key):

```
openssl genpkey -algorithm gost2012_256 -pkeyopt
paramset:A –out private/admin.key
```

9) Просмотреть содержимое закрытого ключа можно командой:

```
openssl pkey –in private/admin.key -text
```

10) Для закрытого ключа изменяем права:

```
chmod 400 private/admin.key
```

11) Генерируем запрос на выдачу сертификата в УЦ с использованием закрытого ключа администратора безопасности (private/admin.key):

```
openssl req -md_gost12_256 –new –key private/admin.key -
out certs/admin.csr -subj
/C=RU/ST=SPb/L=SPb/O=ExampleInc/OU=ITdept/CN=admin_crt
```

12) Данный запрос на выдачу сертификата подписывается на УЦ:

```
openssl ca -extensions usr_cert -notext -md md_gost12_256
–keyfile private/rootca.key -cert certs/rootca.crt -in
certs/admin.csr -out certs/admin.crt
```

13) После выполнения команды из п.12 выводится информация о сертификате, производится уточнение о выпуске и подписи данного сертификата. Для завершения процедуры нажмите клавишу «y»:

```
Certificate is to be certified until Jul 29 08:18:30 2021
GMT (365 days)
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

14) Изменяем права на сертификат:

```
chmod 444 certs/admin.crt
```

15) Создаем файл crlnumber

```
echo 1000 > crlnumber
```

16) Создаем список отозванных сертификатов (далее - CRL) с помощью команды

```
openssl ca –keyfile private/rootca.key -cert
certs/rootca.crt  -gencrl -out crl/rootca.crl
```

17) Посмотреть результат можно следующим образом:

```
openssl crl -in crl/rootca.crl -text
```

3. Электронная подпись файла

С помощью OpenSSL возможно создание открепленной (отсоединенной) электронной подписи (далее – ЭП). С помощью открепленной ЭП возможна подпись файла любого формата, при этом сама ЭП записывается в отдельный файл (*.sign). Для создания ЭП используется закрытый ключ сертификата администратора безопасности (private/admin.key), генерируемого в предыдущем разделе.

3.1. Подпись файла и создание ЭП

1) Выбрать файл образ загружаемой ОС, который необходимо подписать для констатации его целостности и подлинности - например, test.iso. Подписываем файл образ с помощью закрытого ключа сертификата

администратора безопасности private/admin.key. Для создания файла ЭП test.iso.sign используется алгоритм ГОСТ Р 34.10-2012 с длинной ключа 256 бит.

```
openssl dgst -md_gost12_256  -sign private/admin.key -out
test.iso.sign test.iso
```

Примечание. Имя файла подписи должно быть идентично имени файла загружаемого образа ОС. Если файл образа загружаемой ОС имеет наименование Filname.iso то файла подписи должен иметь имя Filename.iso.sign.

3.2. Настройка загрузки в МДЗ Numa Arce

Для настройки загрузки с использованием технологии HTTP Boot необходимо:

– создать профиль загрузки, в качестве типа загрузки выбрать «HTTP Boot» (см. п.4.4.2.2);

– в поле "URL" указать адрес загружаемой подписанной ОС (*test.iso*). Если порт отличается от стандартных (http – 80, https – 443), необходимо указать порт через двоеточие (см. п.4.4.2.2);

– в раздел «Сертификаты» загрузить корневой сертификат УЦ == *certs/rootca.crt*, выработанного в п.2 настоящего приложения (см. п. 4.6.2.2.1);

– в появившемся разделе «Сертификат для HTTP Boot» загрузить сертификат администратора ==certs/admin.crt (см. п. 4.6.2.2.2).

Данный сертификат также возможно загрузить на сервер, где располагается подписанный образ загружаемой ОС, для этого необходимо переименовать данный сертификат *admin.crt* на *Filename.iso*.crt, где «Filename.iso» имя образа файла загружаемой ОС. Для текущего примера необходимо переименовать файл на *test.iso.sign*;

– загрузить файл ЭП *test.iso.sign* (созданный во время подписи файла *test.iso* в п.3 настоящего приложения) на HTTP(S) сервер, где располагается

соответствующий файл образ *test.iso*;

– сохранить профиль загрузки.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АНП	аутентифицирующий носитель персональный
АРМ	автоматизированное рабочее место
БСВВ	базовая система ввода-вывода
ГОСТ	государственный стандарт
КС	контрольная сумма
МДЗ	модуль доверенной загрузки
НСД	несанкционированный доступ
ОС	операционная система
ПО	программное обеспечение
УЦ	удостоверяющий центр
AHCI	advanced host controller interface
BIOS	basic input/output system
CA	certification authority
CRL	certificate revocation list
DNS	domain name system
FV	firmware volume
GUID	globally unique identifier
IDE	integrated development environment
LDAP	lightweight directory access protocol
PCI	peripheral components interconnect
PIN	personal identification number
TLS	transport layer security
UID	user identificator
URL	uniform resource locator – адрес ресурса
USB	universal serial bus

Лист регистрации изменений

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