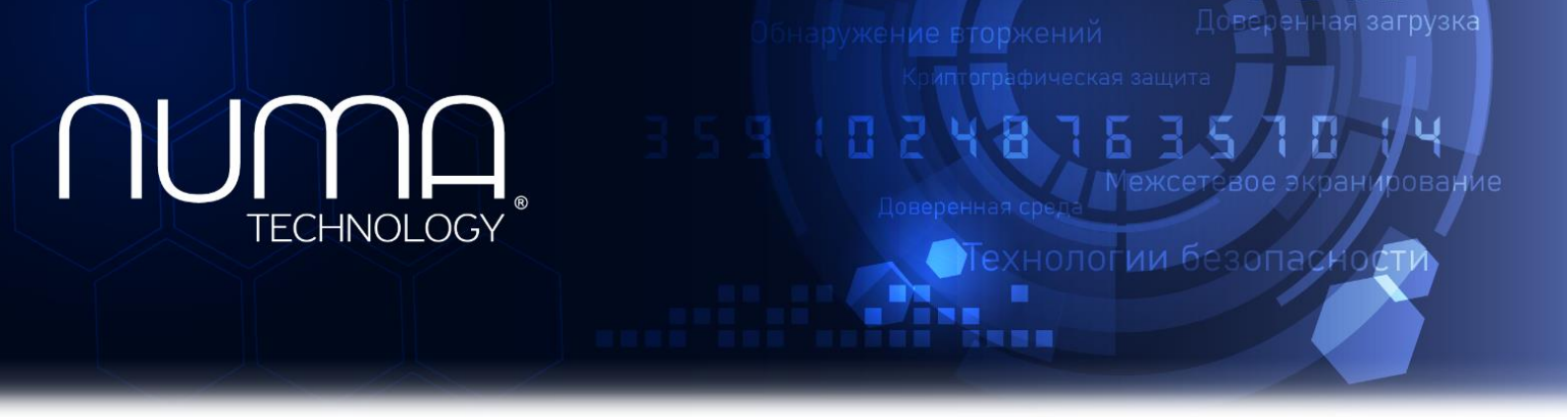

Средство доверенной загрузки уровня базовой системы ввода-вывода
Модуль доверенной загрузки Numa Arce
Руководство пользователя
643.АМБН.00032-01 34 01
Листов 14

2022

Литера

АННОТАЦИЯ

Настоящее руководство является документом, содержащим сведения, необходимые для работы пользователю с изделием Модуль доверенной загрузки Numa Arce 643.АМБН.00032-01 (далее – Изделие).

В документе содержатся сведения о назначении Изделия, условия и порядок работы с Изделием, описание процедур смены паролей пользователей, а также перечень сообщений, выдаваемые оператору в ходе работы с Изделием, описание их содержания и действий, которые следует предпринять при появлении этих сообщений.

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Руководство пользователя
Версия документа	1.0
Обозначение документа	643.АМБН.00032-01 34 01
Утвержден	643.АМБН.00032-01 34 01–ЛУ
Тип Изделия	Средство доверенной загрузки уровня базовой системы ввода-вывода
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Децимальный номер Изделия	643.АМБН.00032-01
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	СДЗ, средство доверенной загрузки уровня базовой системы ввода-вывода

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение программы

Изделие является средством доверенной загрузки уровня базовой системы ввода-вывода и предназначено для обеспечения контроля целостности базовой системы ввода-вывода, модуля доверенной загрузки, идентификации и аутентификации пользователей, разграничения доступа на основе ролей, авторизации на уровне базовой системы ввода-вывода до загрузки основных компонентов операционной среды, а также организации доверенной загрузки операционной системы после процедуры контроля целостности загружаемой среды.

Изделие интегрировано и функционирует только в базовой системе ввода-вывода Numa BIOS 643.АМБН.00001-01 производства ООО «НумаТех».

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

1.2. Функциональные возможности программы

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

1) аутентификацию пользователей и администраторов Изделия:

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

– возможность регистрации не менее 5 равноправных администраторов;

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

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

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

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

– Изделие обеспечивает возможность контроля целостности следующих объектов:

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

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

– журналов транзакций файловых систем Ext3, Ext4 и NTFS;

– разделов и элементов системного реестра ОС Windows;

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

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

3) самотестирование:

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

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

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

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

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

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

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

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

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

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

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

– создание (инициализация) служебных структур данных;

– формирование контрольных сумм служебных структур данных.

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

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

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

– просмотр и модификация списка зарегистрированных пользователей;

– блокирование и разблокирование зарегистрированных пользователей;

– просмотр и модификация конфигурационных параметров Изделия;

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

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

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

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

– просмотр, настройка установленных EFI-драйверов устройств;

– просмотр, настройка возможности защиты EFI-переменных;

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

– пересчет эталонных значений для объектов контроля целостности;

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

- установка системного времени и даты;
- запрос, загрузка файла лицензии;
- обновление Изделия (использование данной функции ограничено Правилами);
- просмотр версии Изделия.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования безопасности

Конфигурирование и управление Изделия должны быть произведены администратором Изделия в соответствии с документом «Руководство администратора» 643.АМБН.00032-01 32 01.

АНП должны эксплуатироваться в соответствии с их эксплуатационной документацией.

Перед началом работы пользователь должен быть зарегистрирован администратором Изделия.

Пользователь должен получить от администратора информацию о типе идентификации и аутентификации и идентификационные/аутентификационные данные:

Тип идентификации/аутентификации:

- АНП;
- АНП + логин/пароль.

Идентификационные/аутентификационные данные:

- при типе аутентификации АНП: физический АНП, пин-код АНП;
- при типе аутентификации АНП + логин/пароль: физический АНП, пин-код АНП, логин, пароль.

Пользователю необходимо запомнить свои учетные данные, необходимые для идентификации/аутентификации.

Ошибки, допущенные пользователем при аутентификации, могут привести к блокировке работы пользователя с Изделием. При блокировке работы пользователя с Изделием необходимо обратиться к администратору Изделия.

После включения питания на СВТ автоматически запускается контроль целостности Изделия, среды функционирования Изделия, всей элементов, поставленных на контроль администратором Изделия. В случае возникновения ошибок необходимо обратиться к администратору Изделия.

2.2. Технические требования

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

Таблица 1 – Характеристики СВТ, на которых функционирует Изделие

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

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

3. ПОРЯДОК РАБОТЫ С ИЗДЕЛИЕМ

Работа пользователя заключается в выполнении следующих действий:

- запуск СВТ с установленным Изделием;
- выполнение текущих задач в загруженной на СВТ ОС;
- завершение работы/выключение СВТ.

3.1. Запуск СВТ с Изделием

Запуск СВТ, на котором установлено Изделие, осуществляется путем подачи питания на СВТ и/или включением, путем нажатия на кнопку типа «Вкл/Выкл».

После включения СВТ Изделием запускается автоматический контроль целостности. В случае если контроль целостности самого Изделия, среды функционирования Изделия – БСВВ Numa BIOS был пройден с ошибками, Изделие переходит в аварийный режим работы при этом выдается сообщение об ошибке и осуществляется блокировка работы СВТ и загрузки ОС.

В случае такого поведения необходимо обратиться к администратору Изделия.

3.1.1. Запуск мобильных и десктопных платформ

Для мобильных и десктопных платформ, указанных в таблице 1, в случае успешного завершения контроля целостности Изделие попросит пользователя пройти идентификацию и аутентификацию, после чего перейдет в главное меню, где отображены профили загрузки, настроенные администратором Изделия. В случае если администратором предустановлен только один профиль загрузки, после тайм-аута Изделие перейдет к загрузке этого профиля. В случае если в Изделии настроены несколько профилей загрузки – пользователю с помощью клавиш навигации необходимо выбрать профиль загрузки и нажать клавишу «Enter» для его загрузки. Если в Изделии не предустановлены профили загрузки, то Изделие сообщит об ошибке, прозвучит звуковой сигнал (при наличии технической возможности).

3.1.2. Запуск сетевых и серверных платформ

Для сетевых и серверных платформ, указанных в таблице 1, в случае успешного завершения контроля целостности Изделие переходит в главное меню, где отображены профили загрузки, настроенные администратором Изделия. В случае если администратором предустановлен только один профиль загрузки, после тайм-аута Изделие перейдет к загрузке этого профиля. В случае если в Изделии настроены несколько профилей загрузки – пользователю с помощью клавиш навигации необходимо выбрать профиль загрузки и нажать клавишу «Enter» для его загрузки. Если в Изделии не предустановлены профили загрузки, то Изделие сообщит об ошибке, прозвучит звуковой сигнал (при наличии технической возможности). В главном меню для сетевых и серверных платформ, указанных в таблице 1, могут отображаться неактивные профили загрузки – такие профили загрузки высвечиваются серым цветом и являются неактивными. Для возможности загрузки таких профилей пользователю необходимо пройти процедуру идентификации/аутентификации, после чего пользователь сможет выбрать данный профиль для загрузки.

3.2. Идентификация и аутентификация

Изделие поддерживает идентификацию и аутентификацию следующего типа:

- по АНП (необходим АНП и ввод ПИН-кода);
- по АНП, логину/паролю (необходим АНП, ввод ПИН-кода, логина и пароля).

Регистрация пользователей осуществляется только администратором Изделия. Перед авторизацией необходимо обратиться к администратору Изделия для получения идентификационных (логин, АНП) и аутентификационных (пароль, ПИН-код) данных.

Навигация по меню осуществляется навигационными клавишами «↓», «↑», подтверждение выбора осуществляется клавишей «Enter».

При вводе имени пользователя, не зарегистрированного администратором в Изделии, и/или неправильного пароля отобразится сообщение:

```
Неверное имя пользователя или пароль!
```

Внимание. Количество неуспешных попыток ввода и общее количество процедур аутентификации, после которых произойдет блокировка пользователя, определяется администратором Изделия. Пользователь заблокирован до тех пор, пока администратор вручную не разблокирует пользователя.

3.2.1. Авторизация с использованием АНП

Для авторизации с использованием АНП необходимо:

– подключить АНП в USB-разъем СВТ;

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

В случае успешной авторизации будет выдано сообщение «Текущий пользователь <Имя пользователя>» и произойдет загрузка ОС.

В случае достижения предельного числа попыток ввода ПИН-кода, настроенных для данного АНП, будет заблокирован сам АНП, и на каждую последующую попытку будет выдано сообщение о вводе неверного ПИН-кода.

Для разблокировки АНП необходимо обратиться к администратору Изделия.

В случае попытки входа и последующего отображения сообщения об ошибке «Пользователь <Имя пользователя> заблокирован» необходимо обратиться к администратору Изделия.

3.2.2. Авторизация с использованием АНП, логина и пароля

Для авторизации с использованием АНП, логина и пароля необходимо:

– подключить АНП в USB-разъем СВТ;

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

– в появившемся окне ввода ввести <Имя пользователя> и нажать «Enter»;

– ввести <Пароль пользователя> и нажать «Enter».

При успешной авторизации осуществлена загрузка пользовательской ОС СВТ и пользователь может приступать к работе.

В случае достижения предельного числа попыток ввода ПИН-кода, настроенных для данного АНП, будет заблокирован сам АНП, и на каждую последующую попытку будет выдано сообщение о вводе неверного ПИН-кода.

Для разблокировки АНП необходимо обратиться к администратору Изделия.

В случае попытки входа и последующего отображения сообщения об ошибке «Пользователь <Имя пользователя> заблокирован» необходимо обратиться к администратору Изделия.

3.3. Завершение работы

Для завершения работы пользователю необходимо выключить СВТ штатным способом.

Если при входе в систему пользователь производил аутентификацию с использованием АНП, то после загрузки ОС можно извлечь АНП из USB-разъема.

Примечание. Отсоединение АНП от СВТ до загрузки ОС приведет к перезагрузке СВТ.

4. СООБЩЕНИЯ ОПЕРАТОРУ

Сообщения БСВВ в штатном режиме работы приведены в таблице 2.

Таблица 2 – Сообщения БСВВ в штатном режиме работы

Сообщение	Описание сообщения	Действия пользователя
«Нарушена целостность БСВВ»	Нарушена целостность БСВВ	Сообщить администратору
«ПИН-код не может быть нулевой длины!»	Вместо ввода ПИН-кода пользователь нажал клавишу«Enter»	Ввести правильный ПИН-код
«Вход. Нажмите ENTER или вставьте USB-токен»	Приглашение к авторизации	Нажать на клавиатуре клавишу «ENTER» для перехода к авторизации по логин/паролю; установить в соответствующий USB порт СВТ токен для авторизации по токену
«Вход. Имя пользователя»	Приглашение к вводу имени пользователя	Ввести имя пользователя для авторизации с использованием логин/пароля
«Вход. Пароль пользователя»	Приглашение к вводу пароля пользователя	Ввести пароль пользователя для авторизации с использованием логин/пароля
«Неверное имя пользователя или пароль!»	Ошибка ввода имени пользователя или пароля	Ввести правильно имя пользователя и пароль после окончания временной блокировки
«Проверка целостности»	Сообщение о начале проверки целостности	Дождаться окончания проверки
«Введите ПИН-код»	Приглашение к вводу ПИН-кода	Ввести ПИН-код
«Неверный ПИН-код!»	Введен неверный ПИН-код или заблокирован токен	В случае ввода неверного ПИН–кода нажать «ENTER»; ввести правильный ПИН-код после перезагрузки СВТ; в случае блокировки токена обратиться к администратору
«Пользователь <имя> заблокирован»	Пользователь с данным именем заблокирован	Обратиться к администратору
«USB-токен был извлечен! Перезагрузки!»	Токен был извлечен в процессе работы БСВВ	Дождаться перезагрузки СВТ

Сообщение	Описание сообщения	Действия пользователя
«СА не загружен!»	При авторизации по токену обнаружено отсутствие сертификата удостоверяющего центра в БСВВ	Обратиться к администратору
«Ошибка. Доступ запрещен!»	Общее сообщение об ошибке при авторизации по токену	Обратиться к администратору
«Сертификат СА еще не вступил в действие!»	Сертификат удостоверяющего центра еще не вступил в действие	Обратиться к администратору
«Истек срок действия сертификата СА!»	Истек срок действия сертификата удостоверяющего центра	Обратиться к администратору
«Нет карточек для токен-пользователей!»	При авторизации по токену в БСВВ не найдено ни одного токен-пользователя	Обратиться к администратору
«Сбой даты/времени! Смените пароль!»	Обнаружен сбой системного времени	Сообщить администратору
«Проверка модулей, пожалуйста, подождите»	Выполняется контроль целостности модулей операционной среды	Дождаться окончания проверки
«Нарушена целостность модуля ОС»	Обнаружено нарушение целостности модуля операционной среды	Сообщить администратору
«Проверка модулей завершена успешно!»	Успешное завершение процедуры контроля целостности модулей операционной среды	Не требуется
«Загрузка ОС, пожалуйста, подождите»	Выполняется загрузка ОС	Дождаться окончания загрузки ОС на СВТ
«Ошибка при загрузке модуля ОС»	При загрузке модуля ОС произошла ошибка	Сообщить администратору
«Истек срок действия пароля пользователя! Смените пароль!»	Срок действия пароля пользователя истек, необходимо сменить пароль	Сообщить администратору

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АНП	аутентифицирующий носитель персональный (токен)
СВТ	автоматизированное рабочее место
мдз	модуль доверенной загрузки
НСД	несанкционированный доступ
ОС	операционная система
ПИН	персональный идентификационный номер
ПО	программное обеспечение
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					