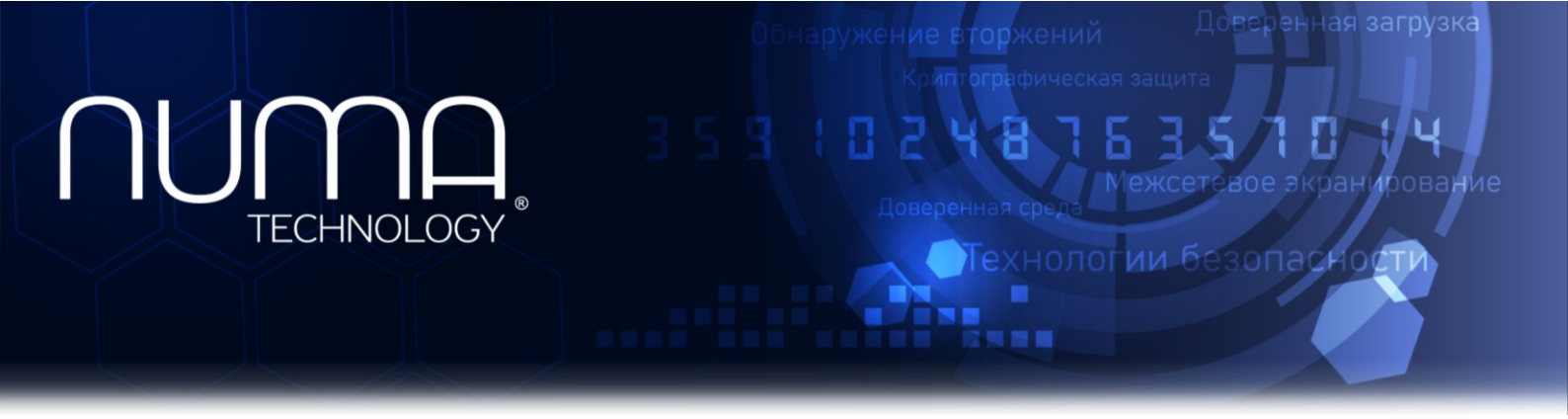

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Руководство пользователя

643.АМБН.00002-01 34 01

Листов 15

Санкт-Петербург

2022

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Идентификация документа

Название документа	Руководство пользователя
Обозначение документа	643.АМБН.00002-01 34 01
Тип Изделия	Средство доверенной загрузки уровня базовой системы ввода-вывода 4 класса
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Идентификация требований	«Требования к средствам доверенной загрузки», утвержденные приказом ФСТЭК России от 27 сентября 2013 г. № 119. «Профиль защиты средств доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ» (ФСТЭК России, 2013); «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02 июня 2020 г. № 76 по 4 уровню доверия. Задание по безопасности 643.АМБН.00002-01 47 01
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	СДЗ, средство доверенной загрузки уровня базовой системы ввода-вывода

1.2. Аннотация

Настоящее руководство является документом, содержащим сведения, необходимые для работы оператора с Изделием модуль доверенной загрузки Numa Arce 643.АМБН.00002-01 (далее – Изделие).

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

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Назначение

Изделие предназначено для выполнения доверенной загрузки: осуществлении запуска с доверенных и предопределенных заранее носителей 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.

2.2. 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 на период, установленный администратором (от 3 до 60 минут) при превышении установленного администратором количества (от 1 до 8) неуспешных попыток аутентификации пользователя;

– возможность проверки соответствия аутентификационной информации определенной метрике качества (алфавит пароля 75 символов, длин пароля от 1 до 20 символов);

– возможность установления ограничений на время действия аутентификационной информации (пароля) на срок от 30 до 365 дней, вводимой (вводимого) пользователем в диалоговом интерфейсе при идентификации/аутентификации и блокирования доступа пользователя при превышении ограничений идентификация и аутентификация пользователя до выполнения действий по загрузке полезной нагрузки 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 полезной нагрузки (данных MBR, ОС), файлов, поставленных на контроль администратором Изделия (в том числе журнала транзакций Ext3/Ext4/NTFS, реестра Windows), конфигурационных параметров, ПО региона ME, GbE микросхемы путем вычисления контрольных сумм;

– возможность контроля целостности модулей БСВВ Numa BIOS, образа Изделия, полезной нагрузки, загружаемой с помощью HTTP Boot путем проверки валидности и верифицированности цифровой подписи;

– 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;

– 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.

2.3. Роли пользователей, поддерживаемые Изделием

Изделие поддерживает три роли пользователей:

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

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

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

2.4. Режимы функционирования Изделия

Изделие поддерживает следующие режимы работы

2.4.1. Режим администрирования

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

В режиме администрирования доступна настройка основных параметров и конфигураций Изделия.

2.4.2. Штатный режим функционирования Изделия

Переход в штатный режим работы осуществляется автоматически после идентификации и аутентификации пользователя, обладающего ролью пользователя, или администратора для загрузки ОС.

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

2.4.3. Режим работы для аудитора

После авторизации аудитора на экране Изделия появляется меню, которое состоит из профилей загрузки и пункта «Панель управления». В данном режиме аудитору доступно две функции:

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

– действия с журналом аудита: просмотр, экспорт на USB-носитель.

2.4.4. Аварийный режим

При аварийном режиме работы Изделия предусматривается блокировка СВТ, на которое установлено Изделие в связи с нарушением контроля целостности Изделия или среды функционирования. Дальнейшая работа Изделия возможна только после переустановки Изделия в режиме начальной инициализации.

2.4.5. Режим начальной инициализации

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

2.5. Дополнительные требования

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

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

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

При работе с технологией HTTP Boot генерацию ключей для цифровой подписи необходимо выполнять в доверенной ОС.

2.6. Требования безопасности

Должен быть обеспечен контроль целостности СВТ, на которое 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 документом «Руководство администратора» 643.АМБН.00002-01 32 01.

3. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Установка, конфигурирование и управление Изделия должны быть произведены администратором в соответствии с документом «Руководство администратора» 643.АМБН.00002-01 32 01.

Перед началом работы пользователь должен быть зарегистрирован администратором Изделия, пользователь должен получить от администратора информацию о типе авторизации, а также логин и пароль (в случае авторизации по типу «логин/пароль») и/или АНП и ПИН-код в случае авторизации с использованием АНП.

Пользователю необходимо запомнить свои учетные данные, необходимые для авторизации, запомнить или сохранить пароль или ПИН-код в недоступном для других месте.

Ошибки, допущенные пользователем при авторизации, могут привести к блокировке системы.

После включения на АРМ автоматически запускается контроль целостности.

В случае появления каких-либо ошибок пользователю необходимо сообщить об этом администратору.

4. ПОРЯДОК РАБОТЫ С ИЗДЕЛИЕМ

4.1. Порядок действий пользователя

Работа пользователя заключается в выполнении следующих действий:

– запуск АРМ;

– авторизация;

– выполнение текущих задач в ОС;

– завершение работы.

4.2. Запуск АРМ

Запуск АРМ, на которой установлено Изделие, осуществляется путем нажатия кнопки подачи питания АРМ.

После включения на АРМ запускается автоматический контроль целостности. В случае если контроль целостности самого Изделия 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.

В случае успешного завершения контроля целостности Изделие переходит к запросу авторизации.

Доступ к АРМ получают только зарегистрированные пользователи.

4.3. Авторизация

Процедура авторизации может осуществляться по одной из следующих схем:

– по имени пользователя и его паролю (требуется ввод логина и пароля пользователя);

– по АНП (необходим АНП и ввод ПИН–кода);

– по АНП, логину и паролю (необходим АНП, ввод ПИН–кода, логина и пароля).

Пользователь, не зарегистрированный на АРМ, не сможет пройти авторизацию.

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

4.3.1. Авторизация с использованием логина и пароля пользователя

Для выполнения авторизации с использованием логина и пароля оператору необходимо выполнить следующие действия:

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

– в окне авторизации ввести <Имя пользователя>, закрепленное за пользователем, и нажать «Enter»;

> ***Примечание.*** *Изделие не чувствительно к регистру вводимых символов имени пользователя (логина). Например, Admin, admin и AdMiN являются равнозначными.*

– ввести пароль, присвоенный пользователю, и нажать «Enter».

При успешной авторизации на АРМ будет осуществлена загрузка пользовательской ОС, и пользователь может приступать к работе на АРМ.

Примечание. *Автоматическая загрузка после успешной процедуры авторизации будет осуществлена только при наличии одного настроенного и загруженного профиля загрузки. В случае если таких профиле загрузки несколько нужно выбрать необходимый и нажать клавишу «Enter».*

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

При вводе имени пользователя, не зарегистрированного в Изделии, или при вводе неправильных данных Изделие выдает сообщение:

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

Пользователь имеет несколько попыток для ввода авторизационных данных (логин/пароль).

Примечание. *Количество неуспешных попыток ввода, после которых произойдет блокировка пользователя, определяется администратором Изделия. Действии пользователя блокируются на определённое количество времени, установленное администратором Изделия.*

4.3.2. Авторизация с использованием АНП

Для авторизации с использованием АНП необходимо:

– вставить АНП в USB–разъем АРМ;

– 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, 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 АРМ.

4.3.3. Авторизация с использованием АНП, логина и пароля

Для авторизации с использованием АНП, логина и пароля необходимо:

– вставить АНП в USB–разъем АРМ;

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

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

Примечание. *Изделие не чувствительно к регистру вводимых символов имени пользователя (логина). Например, Admin, admin и AdMiN являются равнозначными.*

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

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

Последствия ошибочного ввода авторизационных данных описаны в п.п. 4.3.1 и 4.3.2.

4.4. Завершение работы

Для завершения работы пользователю необходимо выключить АРМ штатным

способом.

Если при входе в систему пользователь производил авторизацию с использованием АНП, то после отключения питания АРМ необходимо вынуть АНП из USB–разъема.

Примечание. *Отсоединение АНП от АРМ до его выключения приведет к перезагрузке АРМ.*

5. 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 АРМ 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 АРМ; в случае блокировки токена обратиться к администратору
«Пользователь <имя> заблокирован»	Пользователь с данным именем заблокирован	Обратиться к администратору

Сообщение	**Описание сообщения**	**Действия пользователя**
«USB-токен был извлечен! Перезагрузка!»	Токен был извлечен в процессе работы Изделия	Дождаться перезагрузки АРМ
«СА не загружен!»	При авторизации по токену обнаружено отсутствие сертификата удостоверяющего центра в Изделии	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 Изделии 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 АРМ
«Ошибка при загрузке модуля ОС»	При загрузке модуля ОС произошла ошибка	Сообщить администратору

Сообщение	**Описание сообщения**	**Действия пользователя**
«Истек срок действия пароля пользователя! Смените пароль!»	Срок действия пароля пользователя истек, необходимо сменить пароль	Сообщить администратору

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АНП	аутентифицирующий носитель персональный (токен)
АРМ	автоматизированное рабочее место
БСВВ	базовая система ввода-вывода
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.	№ докумен-та	Входящий № сопровод-ительного докум. и дата	Подп.	Дата
	измен-енных	замен-енных	новых	аннулиро-ванных					