Общество с ограниченной ответственностью «Нума Технологии»

УТВЕРЖДЕН

643.АМБН.00022-01 34 01–ЛУ

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Руководство пользователя

643.АМБН.00022-01 34 01

Листов 15

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

2020

Литера

АННОТАЦИЯ

Настоящее руководство является документом, содержащим сведения, необходимые для работы оператора с Изделием модуль доверенной загрузки Numa Arce 643.АМБН.00022-01 (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.

Данный документ выполнен в соответствии с ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение программы

1.1.1. 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.

1.2. Функциональные возможности программы

1.2.1. Изделие функционирует только в БСВВ Numa BIOS 643.АМБН.00001-01 производства ООО «НумаТех».

1.2.2. Изделие выполняет проверку аппаратных ресурсов, загрузку и запуск загружаемой операционной среды при включении питания или в случае перезагрузки комплекса, контроль целостности ОС перед запуском ее в памяти аппаратной платформы, а также обеспечивает защиту от НСД до этапа загрузки ОС.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования безопасности

2.1.1. Установка, конфигурирование и управление Изделия должны быть произведены администратором в соответствии с документом «Руководство администратора» 643.АМБН.00022-01 32 01.

2.1.2. 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 логин-паролю) и/или АНП и ПИН-код в случае авторизации с использованием АНП.

Для Изделий, функционирующих на аппаратных платформах с процессорами Baytrail (ma3, tca3), ApolloLake (ma5, tca5mse, onix smarc mse, onix psmc mse, cometa-m mse, mars1.2 mse, malahit2.1 mse, chrome mse, coral mse), SkyLake (tc170mse), 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.

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

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

2.1.5. После включения на СВТ автоматически запускается контроль целостности.

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

3. ПОРЯДОК РАБОТЫ С ИЗДЕЛИЕМ

3.1. Порядок действий пользователя

3.1.1. Работа пользователя заключается в выполнении следующих действий:

- запуск СВТ;
- авторизация;
- выполнение текущих задач в ОС;
- завершение работы.

3.2. Запуск СВТ

3.2.1. Запуск СВТ, на которой установлено Изделие, осуществляется путем подачи питания СВТ.

3.3. После включения на СВТ 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.

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

3.3.2. Доступ к СВТ получают только зарегистрированные пользователи.

3.4. Авторизация

3.4.1. 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).

3.4.2. Пользователь, не зарегистрированный на СВТ, не сможет пройти авторизацию.

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

3.4.4. Авторизация с использованием логина и пароля пользователя

3.3.4.1. 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»;

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

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

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».

Для Изделий, функционирующих на аппаратных платформах с процессорами Baytrail (ma3, tca3), ApolloLake (ma5, tca5mse, onix smarc mse, onix psmc mse, cometa-m mse, mars1.2 mse, malahit2.1 mse, chrome mse, coral

mse), SkyLake (tc170mse), 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.

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

3.3.4.3. При вводе имени пользователя, не зарегистрированного в Изделии, Изделие выдает сообщение:

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

3.3.4.4. 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.

3.4.5. Авторизация с использованием АНП

3.3.5.1. Для авторизации с использованием АНП необходимо:

– вставить АНП в USB–разъем СВТ;

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

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

ВНИМАНИЕ! В случае ошибочного ввода пин–кода происходит перезагрузка СВТ.

3.3.5.6. 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 также необходимо обратиться к администратору СВТ.

3.4.6. Авторизация с использованием АНП, логина и пароля

3.3.6.1. Для авторизации с использованием АНП, логина и пароля необходимо:

– вставить 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».

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

3.3.6.3. Последствия ошибочного ввода параметров авторизации описаны в п.п. 3.3.4.3. – 3.3.4.7. и 3.3.5.4. – 3.3.5.6.

3.5. Завершение работы

3.5.1. Для завершения работы пользователю необходимо выключить СВТ штатным способом.

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

Примечание. Отсоединение АНП от СВТ до его выключения 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	Ошибка ввода имени	Ввести правильно имя

Сообщение	Описание сообщения	Действия пользователя
пользователя или пароль!»	пользователя или пароля	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
«СА не загружен!»	При авторизации по токену обнаружено отсутствие сертификата удостоверяющего	Обратиться к администратору

Сообщение	Описание сообщения	Действия пользователя
	центра в БСВВ	
«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	Сообщить администратору

Сообщение	Описание сообщения	Действия пользователя
	целостности модуля операционной среды	
«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					