Общество с ограниченной ответственностью «Нума Технологии»

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Технические условия

643.АМБН.00002-01 90 01

Краткая выписка

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

2021

Литера

О ДОКУМЕНТЕ

Идентификация документа

Название документа	Технические условия. Краткая выписка
Версия документа	Версия 1.0.0
Обозначение документа	643.АМБН.00002-01 90 01
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Идентификация разработчика	ООО «НумаТех»

Настоящий документ является выпиской из документа «Технические условия» 643.АМБН.00002-01 90 01 для изделия «Модуль доверенной загрузки Numa Arce» 643.АМБН.00002-01.

Настоящий документ содержит в себе следующие разделы оригинального документа:

- 1. Технические требования;
- Перечень применяемых сокращений.

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящие технические условия (далее – ТУ) распространяются на средство доверенной загрузки «Модуль доверенной загрузки Numa Arce» 643.АМБН.00002-01 (далее – Изделие), производимое ООО «НумаТех».

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 реализовано в виде EFI-модуля, интегрированного в программное обеспечение базовой системы ввода-вывода (далее – БСВВ) Numa BIOS производства компании ООО «НумаТех», предназначенного для установки в СВТ, построенных на базе x86/x64 платформ Intel, взамен оригинального BIOS.

Изделие взаимодействует с БСВВ в соответствии со спецификацией UEFI 2.4.

Изделие поставляется в составе файлов-прошивок, подготовленных к установке в СВТ, на компакт-диске или USB-флеш-накопителе.

Изделие может применяться:

- в государственных информационных системах до 1 класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.);
- в информационных системах для обеспечения до 1 уровня защищенности персональных данных в соответствии с требованиями документа «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введен в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г.);
- в системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);
- при защите значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК от 25декабря 2017 г № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

Совместно с рабочей и программной документацией на Изделие настоящие ТУ представляют собой полный комплекс требований на Изделие и его изготовление, правила приемки, методы испытаний, транспортирование и хранение.

Пример записи Изделия при заказе и ссылках в другой технической документации: Изделие Модуль доверенной загрузки Numa Arce 643.АМБН.00002-01.

Настоящий документ разработан в соответствии с ГОСТ 2.114-2016.

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1.1. Основные параметры и характеристики

1.1.1. Изделие должно соответствовать требованиям настоящих ТУ.

1.1.2. Изделие должно соответствовать требованиям руководящего документа «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013 г.), а также методического документа «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты» ИТ.СДЗ.УБ4.ПЗ (ФСТЭК России, 2013 г.), а также документу «Задание по безопасности» АМБН.00002-01 47 01, «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.

1.1.3. Изделие должно реализовывать следующие функции безопасности в соответствии с требованиями документов: «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ» (ФСТЭК России, 2013), а также «Задания по безопасности» 643.АМБН.00002-01 47 01 с расширенными компонентами функциональных требований безопасности:

- разграничение доступа к управлению ОО;
- управление работой ОО;
- управление параметрами ОО;
- идентификация и аутентификация;
- аудит безопасности ОО;
- тестирование ОО, контроль целостности программного обеспечения и параметров ОО;
- контроль компонентов СВТ;
- блокирование загрузки операционной системы средством доверенной загрузки;
- сигнализация средства доверенной загрузки;
- обеспечение безопасности после завершения работы ОО.

1.1.4. Изделие реализует функции безопасности, описанные в п.1.1.3, обеспечивающие 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 установленного администратором количества неуспешных попыток аутентификации пользователя;
- 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 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;
- 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.

Изделие реализует функции безопасности, обеспечивающие выполнение следующих расширенных функциональных возможностей:

- реализация сценариев блокировки (по длительности блокировки, включая звуковую идентификацию) Изделия при превышении порога неуспешных попыток аутентификации пользователя;
- возможность проверки соответствия аутентификационной информации определенной метрике качества;
- идентификацию и аутентификацию 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 путем отображения условных знаков типа «*»;
- ограничение времени действия аутентификационной информации (пароля) пользователя с последующей блокировкой доступа к Изделию при превышении срока действия пароля;
- 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.

1.1.5. Изделие реализовано в виде EFI-модуля Numa_Arce.efi и функционирует исключительно в составе БСВВ, разработанной ООО «НумаТех» для использования взамен оригинального BIOS в составе различных СВТ, построенных на базе x86/x64 платформ Intel.

1.1.6. Исполнения Numa BIOS 643.АМБН.00001-01, в среде которых может функционировать Изделие, приведены в таблице 1 документа «Формуляр» 643.АМБН.00002-01 30 01.

1.1.7. Изделие поставляется в составе файлов-прошивок, подготовленных к установке в СВТ. Интеграция Изделия в ПО БСВВ осуществляется в процессе производства файлов-прошивок.

1.1.8. В зависимости от аппаратного обеспечения СВТ (чипсет, серия материнских плат), различают исполнения файлов-прошивок с интегрированным Изделием.

1.1.9. Контрольные суммы EFI-модуля Numa_Arce.efi (Изделие) с учетом особенностей технологического процесса производства файлов-прошивок, требующих применения различных компиляторов для разных аппаратных платформ (в зависимости от чипсета), должны иметь значение, указанное в документе «Формуляр» 643.АМБН.00002-01 30 01 в таблице 2.

1.1.10. Изделие должно соответствовать требованиям раздела 3 «Требование к программе» документа «Программа и методика испытаний» 643.АМБН.00002-01 51 01.

1.2. Комплектность

1.2.1. Изделие должно поставляться в составе файла-прошивки БСВВ Numa BIOS 643.АМБН.00001-01, подготовленного к установке в СВТ и комплектоваться необходимой для эксплуатации Изделия документацией (далее – Комплект Изделия).

1.2.2. Должны быть доступны следующие типы Комплектов Изделия:

- Комплект Изделия на материальных носителях – Изделие должно поставляться на электронном носителе с комплектом документации в соответствии с таблицей 1.
- Комплект Изделия в электронном виде – Изделие и документация должны поставляться в виде файлов в соответствии с таблицей 2, которые загружаются по каналам передачи данных с сетевых ресурсов ООО «НумаТех», при условии предоставления ООО «НумаТех» соответствующего доступа.

1.2.3. Количество Комплектов Изделия, передаваемых Конечному пользователю Изделия в рамках конкретной поставки Изделия, должно определяться условиями лицензионного договора (договора поставки).

1.2.4. Количество лицензий на использование Изделия (число доступных установок (инсталляций) Изделия или количество СВТ, в составе которых может использоваться Изделие) доступных Конечному Пользователю должно быть указано в лицензионном сертификате, сопровождающем каждую поставку Изделия.

Примечания.

1. Лицензионный сертификат – документ, оформляемый ООО «НумаТех» на фирменном бланке, подтверждающий легитимность использования Изделия Конечным Пользователем, содержащий информацию о конкретной поставке Изделия, в том числе сведения об исполнении Изделия и типе СВТ, для использования на котором предназначено исполнение Изделия в рамках конкретной поставки.

2. Ограничения прав по использованию Изделия, связанные с наличием Лицензий на использование ПО, реализуемые ООО «НумаТех» в рамках мер по защите авторских прав в отношении программных продуктов собственной разработки, приведены в разделе 10 настоящих Технических условий.

3. Лицензионный сертификат должен передаваться Конечному пользователю при передаче прав на использование Изделия или совместно с СВТ, на которые Изделие было предустановлено производителем (поставщиком) СВТ.

Таблица 1 – Состав Комплекта Изделия на материальных носителях

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
1	Компакт-диск в составе: 1. Файл-прошивка Изделия, исполнение ___ 2. Документацией, в составе: – 643.АМБН.00002-01 32 01 Руководство администратора; – 643.АМБН.00002-01 34 01 Руководство пользователя; – 643.АМБН.00002-01 94 01 Инструкция по проверке контрольных сумм		На электронном носителе Идентификатор СЗИ РОСС RU.0001.4228._____
2	Конверт для хранения компакт-диска		
3	643.АМБН.00002-01 30 01 Формуляр		В печатном виде
4	Заверенная копия сертификата соответствия требованиям по безопасности информации Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)		В печатном виде
5	Транспортная тара		Представляет собой пластиковый пакет с застежкой типа zip-lock

Таблица 2 – Состав Комплекта Изделия в электронном виде

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
1	Файл-прошивка Изделия, исполнение __		В электронном виде Идентификатор СЗИ РОСС RU.0001.4228._____
2	Документацией, в составе: – 643.АМБН.00002-01 32 01 Руководство администратора; – 643.АМБН.00002-01 34 01 Руководство пользователя; – 643.АМБН.00002-01 94 01 Инструкция по проверке контрольных сумм – 643.АМБН.00002-01 30 01 Формуляр		В электронном виде
3	Копия сертификата соответствия требованиям по безопасности информации Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)		В электронном виде

Примечание.

1. Порядок получения Изделия при электронной поставке описан в разделе 8 Формуляра 643.АМБН.00002-01 30 01.

1.3. Маркировка

1.3.1. Маркировка и упаковка Комплекта Изделия должна производиться в соответствии с документом «Инструкция по маркировке и упаковке» 643.АМБН.00002-01 91 01.

1.3.2. Маркировка Изделия должна соответствовать требованиям технической документации ООО «НумаТех» и должна включать в себя:

- идентификатор СЗИ;
- номер экземпляра Комплекта Изделия.

Примечание.

1. Идентификатор СЗИ – идентификатор средства защиты информации, является уникальным параметром для каждой поставки Изделия, который:

- *содержится в Лицензионном сертификате;*
- *наносится на электронные носители, содержащие Изделие;*
- *указывается в формуляре Изделия;*
- *отображается в меню администрирования Изделия.*

Идентификатор СЗИ имеет следующий формат РОСС RU.0001.YYYY.XXXXXX, где:

- *первая группа знаков содержит прописные буквы и цифры РОСС RU.0001, указывающие на систему сертификации ФСТЭК России;*
- *вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;*
- *третья группа знаков указывает на порядковый номер СЗИ в системе учета средств защиты информации, произведенных ООО «НумаТех».*

1.3.3. Сертифицированные Комплекты Изделия должны маркироваться идентификатором СЗИ. Идентификатор СЗИ должен быть указан:

- в подразделах 2.1, 4.4, разделе 7 Формуляра 643.АМБН.00002-01 30 01;
- на компакт-диске при поставке на материальных носителях.

Идентификатор СЗИ должен отображаться в оснастке меню администрирования, установленного на СВТ Изделия.

1.3.4. Идентификатор СЗИ соответствующий конкретной поставке Изделия, должен регистрироваться ООО «НумаТех» в «Журнале учета выпущенных Изделий и учета идентификаторов СЗИ» совместно со следующей информацией о поставке Изделия:

- число лицензий и номер лицензии;
- количество экземпляров и тип Комплектов Изделия;
- сведения о конечном пользователе и цепочке поставки Изделия.

Примечание.

Номер лицензии – уникальный номер, приводимый в Лицензионном сертификате, который идентифицирует конкретную поставку Изделия.

1.3.5. Номер экземпляра Комплекта Изделия должен наноситься на электронный носитель, и приводиться в разделе 18 Формуляра 643.АМБН.00002-01 30 01.

ПЕРЕЧЕНЬ ПРИМЕНЯЕМЫХ СОКРАЩЕНИЙ

АРМ	–	автоматизированное рабочее место
БСВВ	–	базовая система ввода-вывода
ПЗ	–	профиль защиты
ПО	–	программное обеспечение
СЗИ	–	средство защиты информации
ТУ	–	технические условия
ЭП	–	электронная подпись

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					