Общество с ограниченной ответственностью «Нума Технологии»

УТВЕРЖДЕН
643.АМБН.00022-01 90 01–ЛУ

Средство доверенной загрузки уровня базовой системы ввода-вывода

Модуль доверенной загрузки Numa Arce

Технические условия

643.АМБН.00022-01 90 01

Листов 32

2020

Литера

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

Настоящие технические условия (далее – ТУ) распространяются на средство доверенной загрузки модуль доверенной загрузки Numa Arce 643.АМБН.00022-01 (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 и состава аппаратных компонентов СВТ, на которое установлено Изделие.

Изделие реализовано в виде EFI-модуля, интегрированного в программное обеспечение базовой системы ввода-вывода (далее – БСВВ) Numa BIOS 643.АМБН.00001-01 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 информационных системах, в которых обрабатывается информация, содержащая сведения не выше уровня «совершенно секретно».

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:

Модуль доверенной загрузки Numa Arce

643.АМБН.00022-01 (исполнение XX)

Настоящий документ разработан в соответствии с ГОСТ 2.114-2016.

Перечень нормативно-методических и эксплуатационных документов, используемых в настоящих ТУ, приведен в Приложении 1.

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 второго класса защиты» ИТ.СДЗ.УБ2.ПЗ (ФСТЭК России, 2013 г.), требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», (Гостехкомиссия России, 1999 г.) – по второму уровню контроля в части программного обеспечения, реальным и декларируемым в документах функциональных возможностей.

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 второго класса защиты ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013):

- 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 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 HTTPBoot 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.

1.2. Комплектность поставки

1.2.1. 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.

1.2.2. Изделие поставляется в составе файлов-прошивок, подготовленных к установке в СВТ. Интеграция Изделия в базовую систему ввода-вывода Numa BIOS 643.АМБН.00001-01 осуществляется в процессе производства файлов-прошивок.

1.2.3. Установка Изделия на СВТ должны осуществляться согласно документу «Руководство администратора» 643.АМБН.00022-01 32 01.

1.2.4. Комплектность Изделия и способ поставки в каждом конкретном случае должны определяться договором поставки Изделия Заказчику.

1.2.5. При приемке и поставке Изделия должна проверяться его комплектность, в которую входят Изделия и документы, приведенные в таблице 1.

Таблица 1 – Комплектность поставки сертифицированного Изделия

№ 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.00022-01 32 01 Руководство администратора; − 643.АМБН.00022-01 34 01 Руководство пользователя; − 643.АМБН.00022-01 94 01 Инструкция по проверке контрольных сумм.	1 1 1 1 1	643.АМБН.00022-DVD 01 В электронном виде

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
2	Конверт для хранения компакт-диска	1	
3	643.АМБН.00022-01 30 01 Формуляр	1	В печатном виде
4	Лицензионный сертификат	1	В печатном виде.
5	Сертификат технической поддержки	1	В печатном виде

Примечание.

1. Итоговый комплект документации к Изделию зависит от договора поставки.

2. Изделие поставляется в составе файла-прошивки БСВВ, подготовленного к установке в СВТ.

3. Файл-прошивка и документация на Изделие может поставляться на компакт-диске или USB-флеш-накопителе в зависимости от договора поставки.

1.2.6. 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.00022-01 30 01 (графа «КС Изделия»).