Numa BIOS и МДЗ Numa Arce

Российский BIOS и программный модуль доверенной загрузки

июнь 2026

NUMA TECHNOLOGY®

О компании

Компания **Нума Технологии** – российский разработчик специализированного программного обеспечения и средств защиты информации. Деятельность компании сосредоточена на проведении разработок по ключевым направлениям информационных технологий, значимых для создания безопасных информационных систем.

18
лет опыта разработки СЗИ

более 1000
защищенных объектов информатизации

4
направления технологий безопасности

7
СЗИ собственной разработки

Направления деятельности

- Разработка и производство программных и программно-технических средств защиты информации;
- Создание защищенных программно-технических комплексов;
- Проектирование и реализация комплексных решений по безопасной обработке и хранению данных;
- Оказание услуг по защите информации в информационных системах;
- Профильные научно-исследовательские и опытно-конструкторские работы.

Лицензии НумаТех

Лицензия ФСТЭК России №3527
от 25.09.2018
на осуществление деятельности по технической защите конфиденциальной информации.

Лицензия ФСТЭК России №1845
от 25.09.2018
на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации.

Лицензия ФСТЭК России №3552
от 27.12.2024
на проведение работ, связанных с созданием средств защиты информации.

Лицензия ФСБ России №1189Н
от 26.11.2018
на осуществление разработки, производства, распространения шифровальных (криптографических) средств.

Лицензия ФСБ России №12643
от 23.12.2022
на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

Лицензия МО РФ №2486
от 23.12.2024
на проведение работ, связанных с созданием средств защиты информации.

Numa BIOS

Российская БСВВ для x86/x64
платформ Intel и AMD

Numa BIOS. Общие сведения

В реестре российского ПО
Реестровая запись №5467
от 24.06.2019

Numa BIOS – российская БСВВ, разработана в полном соответствии со стандартом UEFI и заменяет стандартный BIOS.

Вариант 1. Стандартный BIOS

Более 80 исполнений под различные типы средств вычислительной техники

- Стационарные ПЭВМ
- Серверы
- Моноблоки
- Ноутбуки

Вариант 2. Доверенный BIOS

Для использования в составе серверных платформ, к которым предъявляются требования по безопасности информации

Сертификат ФСТЭК России №4260 от 23.06.2020
4 уровень доверия и ТУ

- Программно-технические межсетевые экраны (п. 12.2 Требований по безопасности информации, утвержденных приказом ФСТЭК России от 2 июня 2020г. №76)
- Защищенные программно-технические комплексы (Для защиты информации в ГИС, ИСПДн, АСУ ТП, КИИ)

NUMA TECHNOLOGY | ПРОДУКТЫ ТЕХНОЛОГИЧЕСКИХ ПАРТНЕРОВ

AQUARIUS ICL ТЕХНО ДЕПО [компьютерс] ПРОТЕЙ СпецТехника Lanner

Numa BIOS. Особенности и преимущества

Для каждой аппаратной платформы разрабатывается отдельное исполнение Numa BIOS, обладающее набором основных функций стандартного BIOS. Срок разработки от двух до шести месяцев

- **Возможность реализации уникальных функций** (по управлению СВТ, поддержке устройств, безопасности) **и доработки под требования заказчика** (производителя СВТ);
- **Модульная архитектура** (возможности по встраиванию криптопровайдера, гипервизора, СДЗ, драйверов и пр.);
- **Небольшой размер** (около 2 МБ в типовой конфигурации);
- **Соответствие требованиям импортозамещения и критериям Минпромторга** (ПП РФ №719 и ПП РФ №878);
- **Гарантированное отсутствие опасных функциональных возможностей на уроне программного обеспечения аппаратной платформы** (архитектура программного обеспечения и технологии его безопасной разработки);
- **Существенный потенциал по сертификации в системах сертификации ФСТЭК России, ФСБ России и Минобороны России** (Исходные коды доступны для контроля отсутствия недекларированных возможностей (НДВ-2);
- **Возможность применения сертифицированного ФСТЭК России, ФСБ России и Минобороны России программного модуля доверенной загрузки Numa Arce** (производство НумаТех, разработанного специально для использования в среде Numa BIOS) – новый уровень безопасности!

Numa BIOS. Базовые функциональные возможности

- Возможность отключения определенных аппаратных компонентов, смонтированных на плате;
- Контроль целостности модулей BIOS и загружаемых объектов;
- Возможность программного обновления (как с USB-flash, так и по сети);
- Контроль целостности микропрограммного обеспечения (firmware) отдельных компонентов (микроконтроллеров) аппаратной платформы;
- Расширенные функции управления доступом и регистрации событий безопасности;
- Поддержка широкого спектра операционных систем ОС Windows (XP и новее), ОС Linux (в т.ч. все отечественные), UNIX, DOS;
- Поддержка стандартов: UEFI, ACPI, SMBIOS, CSM (legacy), PXEboot;
- Корректное функционирование HBA, RAID, SAS;
- Поддержка отечественных АПМДЗ (OptionROMs);
- Поддержка аппаратных идентификаторов: Рутокен 2.0 (touch, 2100, 3000, flash), смарт-карта РутокенЭЦП 2.0 2100, Рутокен ЭЦП 3.0 (3100, NFC 3100, 3220), JaCarta-2 (ГОСТ, PKI/ГОСТ, PKI/BIO/ГОСТ, PRO/ГОСТ), Esmart Token ГОСТ;
- Возможность активации МДЗ Numa Arce путем ввода лицензии.

Numa Arce

Первый в России программный модуль доверенной загрузки, сертифицированный ФСБ России и МО РФ

Numa Arce. Общие сведения

Numa Arce – программный модуль доверенной загрузки, разработанный НумаТех специально для использования в среде Numa BIOS.

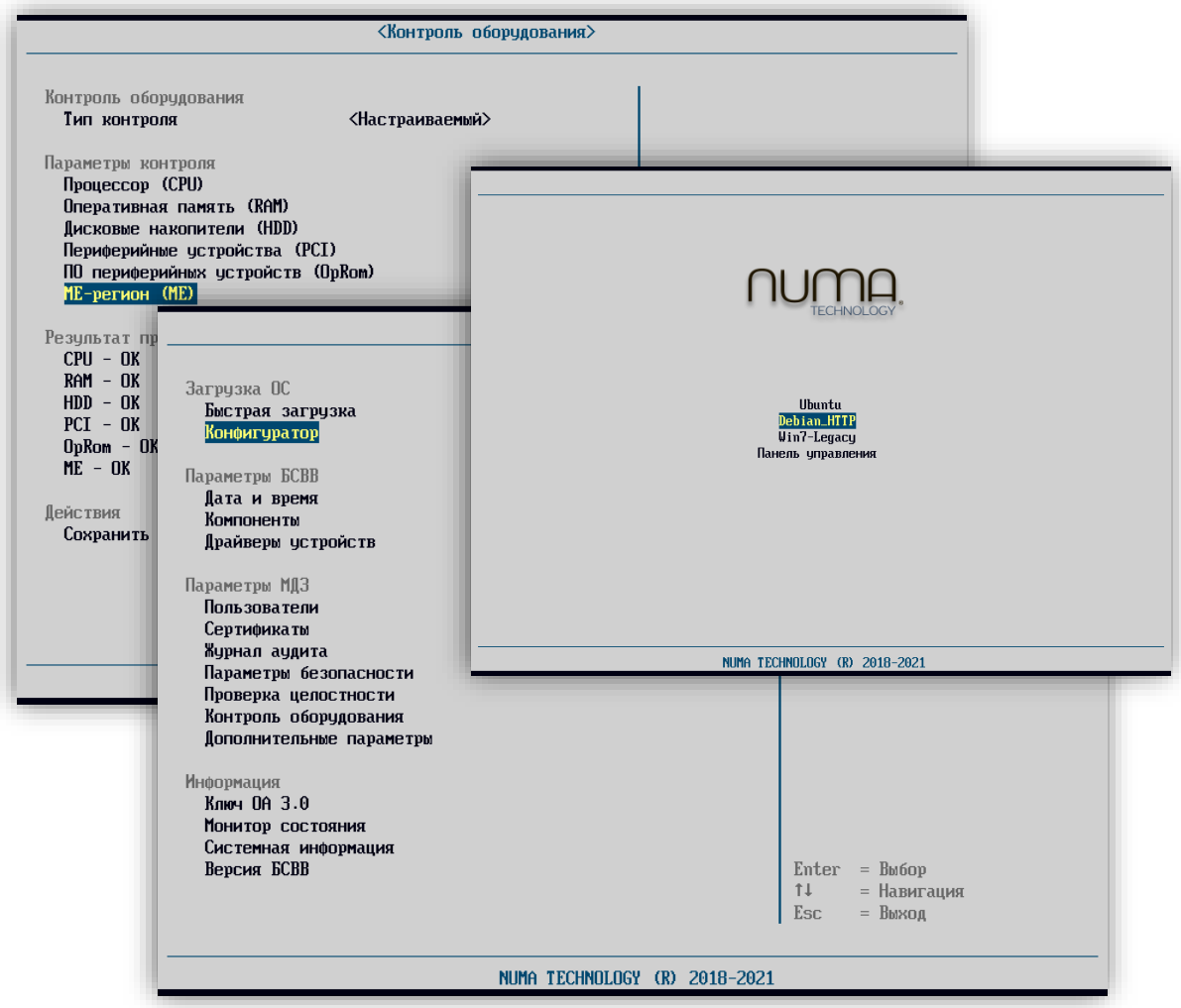
В реестре российского программного обеспечения
Реестровая запись №5343 от 06.05.2019

Сертификат ФСБ России №СФ/527-5551 от 17.06.2026
«Требования к механизмам доверенной загрузки ЭВМ» (класс защиты 2, класс сервиса Б) и может использоваться для защиты от НСД к информации, не содержащей сведений, составляющих ГТ

Сертификат МО РФ №5224 от 03.03.2021
«Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), Профиль защиты СДЗ ИТ.СДЗ.УБ2.ПЗ, РД НДВ-2*, реальных и декларируемых в документации функциональных возможностей.

* Сертифицирован вместе со средой функционирования Numa BIOS

Сертификат ФСТЭК России №4228 от 04.03.2020
Требования доверия (приказ ФСТЭК России от 2 июня 2020г. №76) по 4 УД, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), Профиль защиты СДЗ ИТ.СДЗ.УБ4.ПЗ (ФСТЭК России, 2013) и 3Б
Истек. Техническая поддержка до 31.12.2035

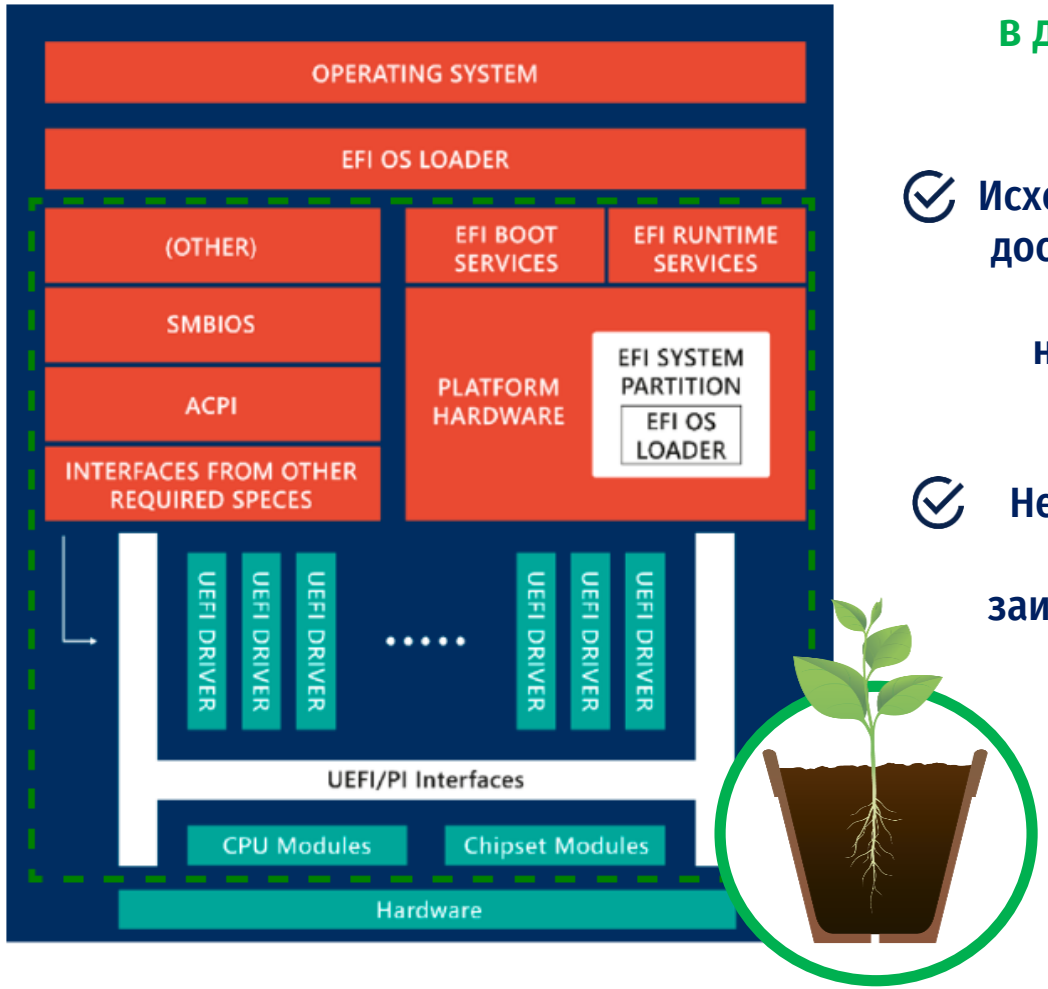


Numa Arce. Функциональные возможности

- Контроль целостности базовой системы ввода-вывода, собственных модулей, загрузочной записи, журнала аудита, данных пользователей и сертификатов;
- Возможность пошагового контроля целостности, с вычислением контрольной суммы по ГОСТ Р 34.11-2012, следующих компонентов: объекты загружаемой операционной системы (данные MBR, ОС, поставленные на контроль администратором); файлы, поставленные на контроль администратором СДЗ в том числе журнала транзакций Ext3/Ext4/NTFS, реестра Windows; конфигурационные параметры; ПО региона ME, GbE соответствующей микросхемы SPI flash-памяти на системной плате (для отдельных аппаратных платформ);
- Возможность контроля целостности ОС, загружаемой с помощью HTTPBoot путем проверки валидности и верифицированности цифровой подписи по ГОСТ Р 34.10-2012;
- Исключение возможности нерегламентированного доступа к внешним устройствам ввода-вывода до момента полной загрузки СВТ;
- Многоуровневая ролевая модель доступа, с поддержкой технологии SSO, PKI;
- Поддержка аппаратных идентификаторов: Рутокен 2.0 (touch, 2100, 3000, flash), смарт-карта РутокенЭЦП 2.0 2100, Рутокен ЭЦП 3.0 (3100, NFC 3100, 3220), JaCarta-2 (ГОСТ, PKI/ГОСТ, PKI/BIO/ГОСТ, PRO/ГОСТ), Esmart Token ГОСТ;
- Поддержка аутентификации AD/LDAP-серверах, в том числе с использованием сертификатов X.509;
- Настраиваемый контроль состава компонентов аппаратного обеспечения СВТ, основываясь на их идентификационной информации: процессора; оперативной памяти; дисковых накопителей; устройств на шине PCI, включая программное обеспечение таких устройств (OpROM); накопителей на шине SATA;
- Невозможность получения доступа к ресурсам МДЗ из программной среды СВТ после завершения работы МДЗ;
- Журнал регистрации событий МДЗ хранится в энергонезависимой памяти с возможностью экспорта.

Numa Arce. Основные отличия от конкурирующих продуктов

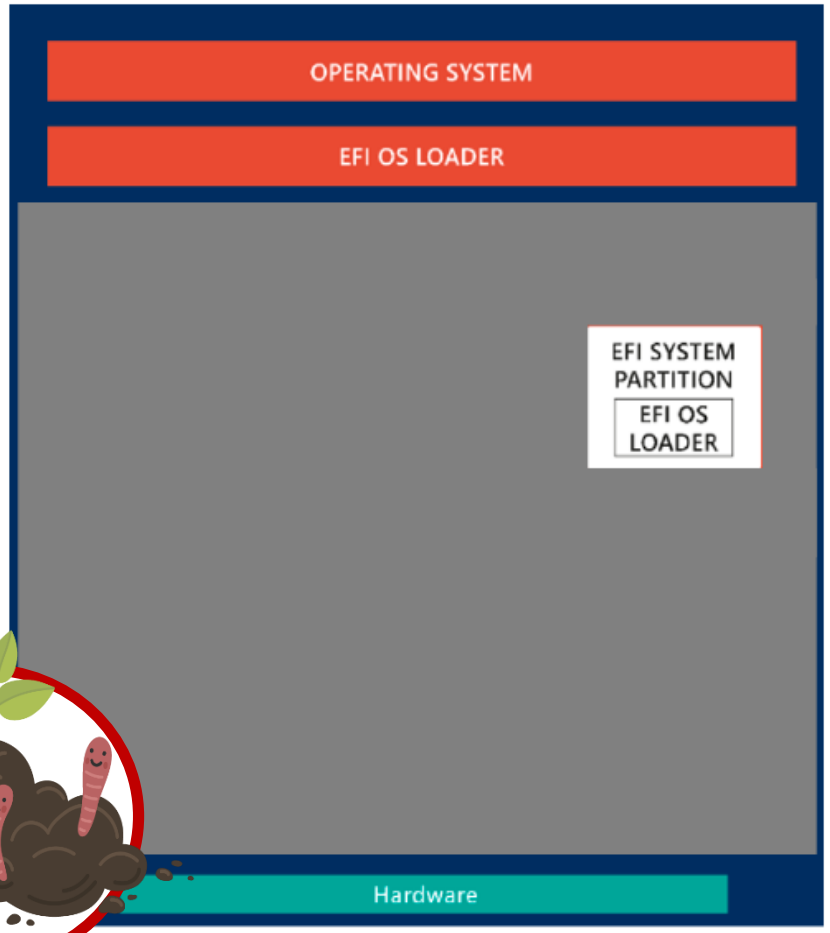
Так видят BIOS в НумаТех:



Numa Arce функционирует в доверенной среде – Numa BIOS

- Исходные коды Numa BIOS доступны для анализа на предмет наличия недекларированных возможностей.
- Не содержит бинарных компонентов заимствованных у других разработчиков

Так видят BIOS разработчики других МДЗ:



Numa Arce. Основные отличия от других программных МДЗ

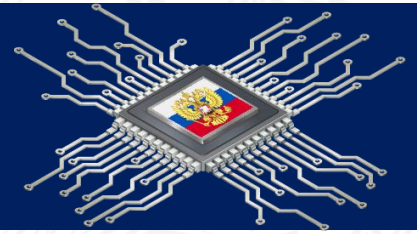
МДЗ Numa Arce
в среде Numa BIOS

Другие ПМДЗ
в недоверенной среде зарубежных
и отечественных* BIOS

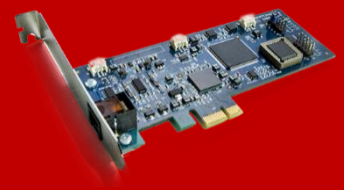
Гарантия корректного функционирования СВТ с внедренным в BIOS программным МДЗ, подтвержденная производителем BIOS	✗
Обновления BIOS НЕ могут влиять на работоспособность МДЗ	✗
Специальная разработка для работы в среде доверенного BIOS на конкретной аппаратной платформе	✗
Доверенная среда функционирования, обеспечивающая реальную безопасность на своем уровне архитектуры СВТ	✗

*** BIOS, в составе которых используются бинарные модули, недоступные для анализа на НДВ.**

Numa Arce и аппаратные МДЗ: защита на бумаге или на практике?



МДЗ Numa Arce



Классический АПМДЗ*

МДЗ Numa Arce		Классический АПМДЗ*
✓	**Не извлекается из СВТ, является его частью****	✗
✓	**Исполняет свой код в доверенной среде, не зависит от настроек и конфигурации BIOS**	✗
✓	**Для полнофункциональной работы не требуется дополнительного физического подключения к разъемам системной платы**	✗

* Наличие аппаратного датчика случайных чисел в составе АПМДЗ является аргументом только для случаев, когда такой датчик требуется для работы со средствами криптографической защиты информации в соответствии с их (СКЗИ) правилами пользования.

** При наличии прямого физического доступа к СВТ нарушитель с любым потенциалом может легко отключить аппаратный МДЗ. Для отключения МДЗ Numa Arce помимо физического доступа к СВТ нужны специфические навыки и умения, специальный инструментарий и большой объем времени.

Numa Arce. Обычные аргументы против

Утверждение	Реальная ситуация
Баг в программном МДЗ превращает весь компьютер в «кирпич». Аппаратный МДЗ можно вытащить переинициализировать.	Разработка Numa Arce ведется в соответствии со стандартами SDLC, реализованными в НумаТех. За все время от пользователей МДЗ Numa Arce не было зафиксировано подобных обращений. В отдельных версиях МДЗ Numa Arce реализована возможность перевода аппаратной платформы в режим начальной инициализации и восстановления работоспособности МДЗ Numa Arce на месте.
Программный МДЗ хранит данные в микросхеме БСВВ, откуда их можно прочесть.	В случае с Numa Arce такие усилия лишены всякого смысла. Если предположить, что нарушитель смог сделать дамп программного обеспечения БСВВ (высокий потенциал, навыки и специальный инструментарий, прямой физический доступ к СВТ), то критичные данные все равно будут ему не доступны (например, аутентификационная информация пользователей). Кроме того, записать обратно модифицированную прошивку нельзя.
Если в БСВВ найдена ошибка, то разработчик материнской платы оперативно готовит и предоставляет обновление. В случае с программным МДЗ нужно ждать подготовки и тестирования соответствующего образа, включающего код МДЗ. В некоторых случаях обновление БСВВ может пройти автоматически, что сделает невозможным использование программного МДЗ.	МДЗ Numa Arce функционирует в среде Numa BIOS. Любые обновления Numa BIOS не влияют на работоспособность МДЗ Numa Arce и подготавливаются с учетом возможности использования последнего.

Numa Arce. Обычные аргументы против

Утверждение	Реальная ситуация
Аппаратный замок более универсален по встраиванию. Его можно использовать на любом ПК, где есть соответствующий разъём (PCI-E, miniPCI-E или M.2)	В некоторых случаях, справедливых для ряда СВТ (серверов, ноутбуков, планшетов, моноблоков) такая «универсальность» как раз оказывается существенным минусом, делающим, в том числе, невозможным применение аппаратных МДЗ.
	МДЗ уровня базовой системы ввода-вывода исходя из особенностей архитектуры продуктов данного класса более требовательны к среде функционирования, однако они более эффективны, когда речь заходит о приобретении новых СВТ с предустановленным СДЗ, либо когда BIOS, находящийся в эксплуатации СВТ, позволяет выполнить инсталляцию такого МДЗ. МДЗ Numa Arce: **- не занимает слота на материнской плате;** **- более тесная интеграция с СВТ;** **- низкая стоимость владения (дешевле в три – пять раз);** **- установка не влияет на гарантию поставщика СВТ;** **- эксплуатация не требует реализации специальных организационно-административных мероприятий (опечатывание системных блоков и пр.).**

По вопросам связанными с продуктами Numa BIOS и Numa Arce обращайтесь к менеджерам Партнерского отдела НумаТех:

e-mail: sales@numatech.ru

тел: (812) 309-06-01 доб. 666, 777

web: numatech.ru