

# Numa BIOS и МДЗ Numa Arce

Российский BIOS и программный  
модуль доверенной загрузки

# ПРОФИЛЬ КОМПАНИИ НУМАТЕХ

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

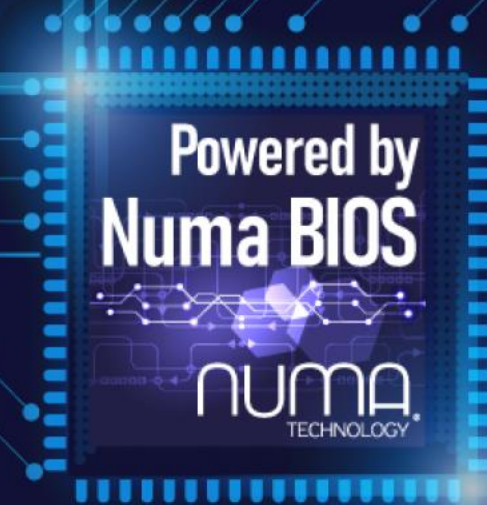


**ЛИЦЕНЗИЯ МИНОБОРОНЫ РОССИИ №2486**  
**от 23.12.2024**

на проведение работ, связанных с созданием  
средств защиты информации.

# NUMA BIOS

Первый российский BIOS для  
клиентских устройств и серверов



# БСВВ NUMA BIOS



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



В реестре российского ПО  
Реестровая запись №5467  
от 24.06.2019



Для каждой аппаратной платформы разрабатывается отдельное исполнение Numa BIOS, обладающее набором основных функций стандартного BIOS.

## Базовые возможности:

- ✓ Возможность отключения аппаратных компонентов, смонтированных на плате
- ✓ Контроль целостности модулей BIOS и загружаемых объектов
- ✓ Возможность программного обновления с USB-flash или по сети
- ✓ Поддержка аппаратных идентификаторов: Рутокен, JaCarta, Esmart;
- ✓ Контроль целостности микропрограммного обеспечения и отдельных компонентов
- ✓ Расширенные функции управления доступом и регистрации событий безопасности
- ✓ Поддержка широкого спектра операционных систем ОС Windows, ОС Linux, UNIX, DOS
- ✓ Поддержка стандартов: UEFI, ACPI, SMBIOS, CSM (legacy), PXEboot
- ✓ Корректное функционирование HBA, RAID, SAS
- ✓ Поддержка отечественных АПМДЗ
- ✓ Возможность активации ПМДЗ Numa Arce

## Технологические партнеры

**AQUARIUS**

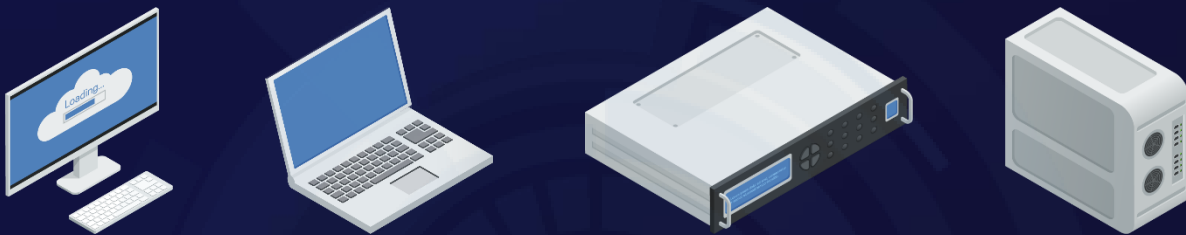


# ИСПОЛНЕНИЯ NUMA BIOS

## СТАНДАРТНЫЙ BIOS

Более восьмидесяти исполнений под различные типы средств вычислительной техники различных производителей

- ✓ Стационарные ПЭВМ
- ✓ Моноблоки
- ✓ Ноутбуки
- ✓ Серверы



## 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.

Истек. Техническая поддержка до 31.12.2035

- Программно-технические межсетевые экраны (п. 12.2 Требований по безопасности информации, приказ ФСТЭК России от 02.06.2022 г. №76)
- Защищенные программно-технические комплексы (Для защиты информации в ГИС, ИСПДн, АСУ ТП, КИИ)

# ПРЕИМУЩЕСТВА NUMA BIOS



## ГАРАНТИРОВАННАЯ БЕЗОПАСНОСТЬ

Обеспечивается на уровне программного обеспечения аппаратной платформы



## УПРОЩЕННАЯ СЕРТИФИКАЦИИ

Для аппаратной платформы в системах ФСТЭК, ФСБ и Минобороны России. Исходные коды доступны для контроля отсутствия недеklarированных возможностей (НДВ-2)



## МОДУЛЬНАЯ АРХИТЕКТУРА

Возможно встраивание криптопровайдера, гипервизора, СДЗ, драйверов и других компонентов



## СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ

Соответствие требованиям импортозамещения и критериям Минпромторга (ПП РФ №719 и ПП РФ №878)



## ЗАКАЗНАЯ РАЗРАБОТКА

Возможность реализации уникальных функций и доработки под требования заказчика



## ВСТРОЕННЫЙ ПМДЗ

Возможность применения программного модуля доверенной загрузки Numa Arce, сертифицированного ФСТЭК России, ФСБ России и Минобороны России



## НЕБОЛЬШОЙ РАЗМЕР

Около 2 МБ в типовой конфигурации

# NUMA ARCE

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

не извлекается из CBT

контроль аппаратного обеспечения

функционирует в среде Numa BIOS

контроль при загрузке по сети

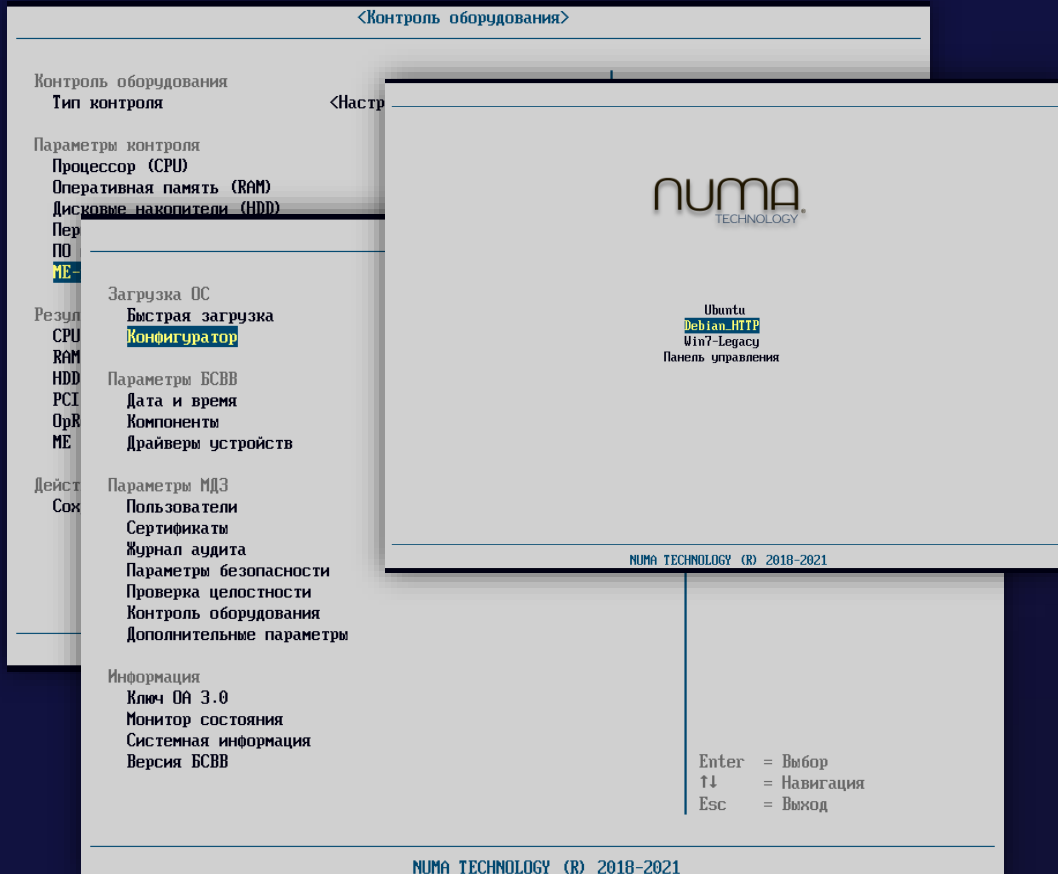
модуль доверенной загрузки



# ПМДЗ NUMA ARCE



**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 гостайну



Сертификат МО РФ №7127 от 10.10.2024  
«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  
Истек. Техническая поддержка до 31.12.2035  
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 ЗБ

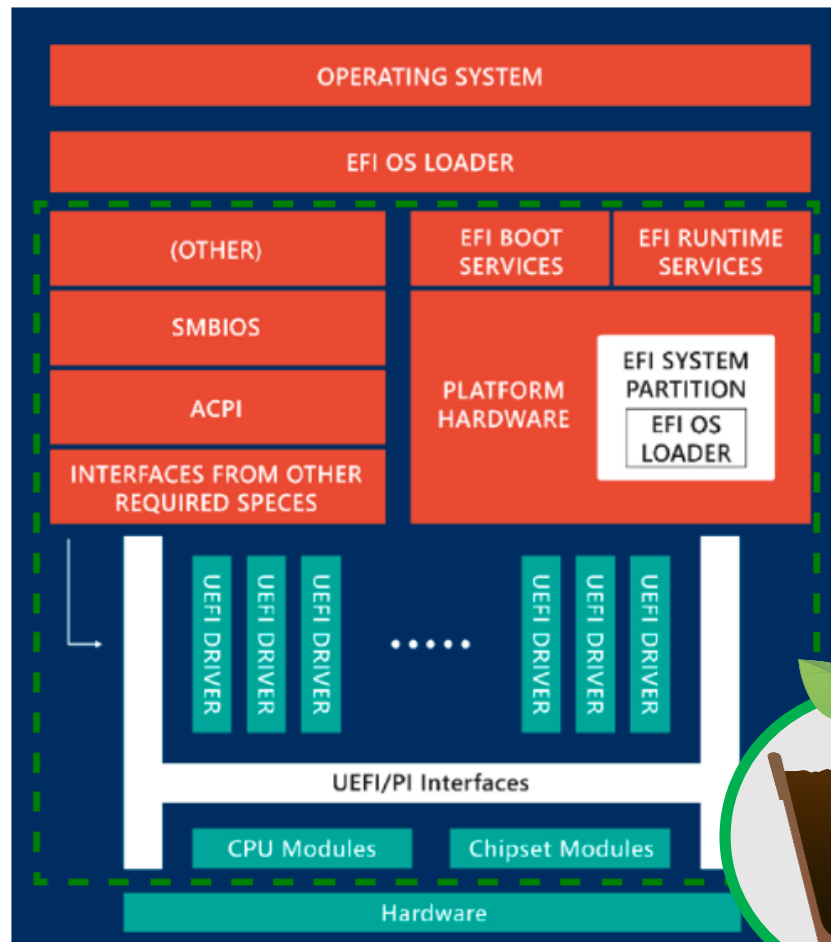
# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ



- ✓ 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/ВЮ/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.

# ОСНОВНЫЕ ОТЛИЧИЯ ОТ КОНКУРИРУЮЩИХ ПРОДУКТОВ

Так видят BIOS в НумаТех:



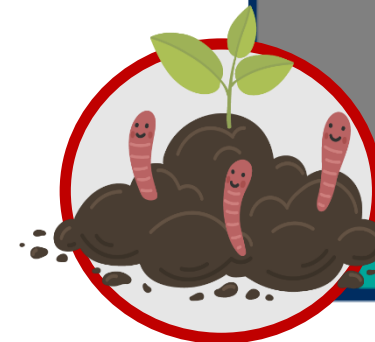
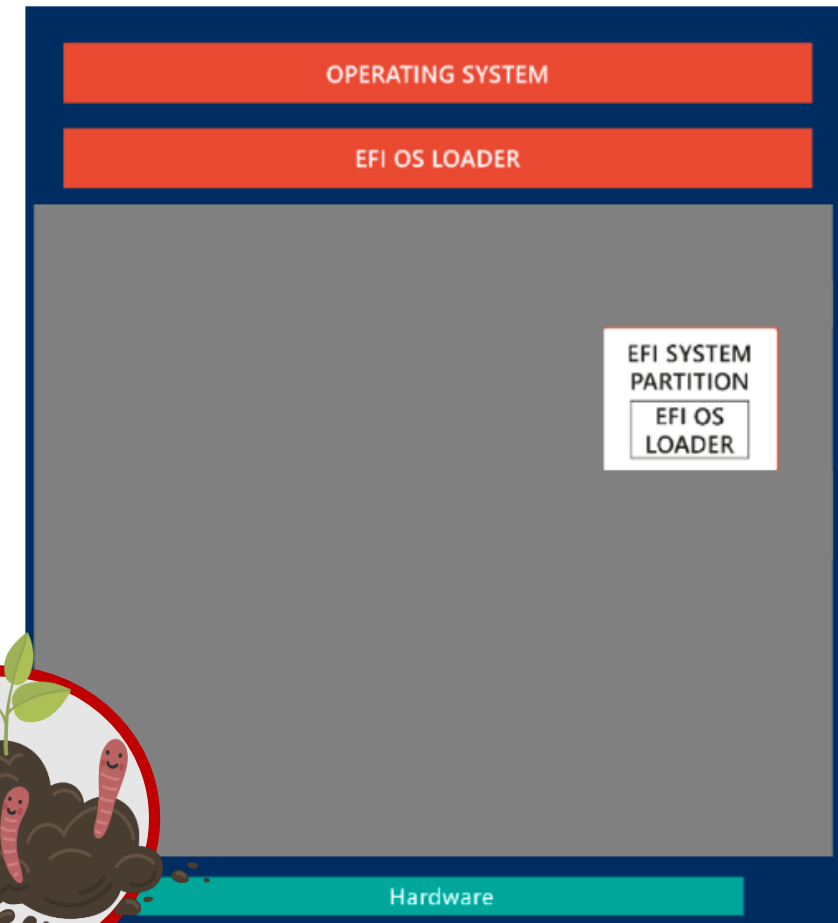
Numa Arce функционирует  
в доверенной среде –  
Numa BIOS

✓ 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 И ДРУГИЕ ПМДЗ

## NUMA ARCE В СРЕДЕ NUMA BIOS



- ✓ Гарантия корректного функционирования ПМДЗ Numa Arce в среде Numa BIOS, подтвержденная разработчиком BIOS
- ✓ Обновления BIOS не могут влиять на работоспособность МДЗ
- ✓ Numa Arce специально доработан для функционирования на каждой конкретной аппаратной платформе
- ✓ Доверенная среда функционирования ПМДЗ – Numa BIOS, обеспечивает реальную безопасность на своем уровне архитектуры СВТ

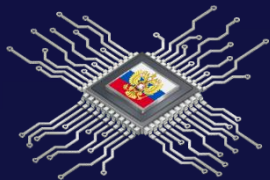


## ПМДЗ В НЕДОВЕРЕННОЙ СРЕДЕ BIOS

- ✗ BIOS, в составе которых используются бинарные модули, недоступные для анализа на НДВ.
- ✗ ПО ПМДЗ зависит от обновлений BIOS и часто разработчики не могут взаимодействовать с вендорами BIOS напрямую
- ✗ Требуется дополнительное исследование и доработка для применения ПМДЗ на разных аппаратных платформах.
- ✗ ПМДЗ обеспечивает безопасность только на уровне выше BIOS, что создает большую площадь для атаки на нижнем уровне архитектуры СВТ

# ПМДЗ И АПМДЗ

## ПМДЗ NUMA ARCE



- ✓ Не извлекается из СВТ, является его частью. Для несанкционированного отключения помимо физического доступа к СВТ нужны навыки, инструментарий и большой объем времени
- ✓ Исполняет свой код в доверенной среде, не зависит от настроек и конфигурации BIOS
- ✓ Для работы не требуется дополнительного физического подключения к плате



## КЛАССИЧЕСКИЙ АПМДЗ

- ✗ При наличии прямого физического доступа к СВТ нарушитель с любым потенциалом может легко отключить аппаратный МДЗ
- ✗ Для полноценной работы необходима дополнительная настройка и подготовка платы
- ✗ Физически подключается к плате, что ограничивает возможность подключения дополнительных устройств
- ✗ Наличие аппаратного датчика случайных чисел. *Необходим только, когда такой датчик требуется для работы в соответствии с правилами пользования СКЗИ*

# ОБЫЧНЫЕ АРГУМЕНТЫ ПРОТИВ

| Утверждение                                                                                                                                                                                                                                                                                                                                       | Реальная ситуация                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Баг в программном МДЗ превращает весь компьютер в «кирпич». Аппаратный МДЗ можно вытащить и 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.<br>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.<br>Если предположить, что нарушитель смог сделать дампы программного обеспечения БСВВ (высокий потенциал, навыки и специальный инструментарий, прямой физический доступ к СБТ), то критичные данные все равно будут ему недоступны (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 делает 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.                                                                                                                                                                                                                            |

# ОБЫЧНЫЕ АРГУМЕНТЫ ПРОТИВ

## Утверждение

Аппаратный замок более универсален по встраиванию. Его можно использовать на любом ПК, где есть соответствующий разъём (PCI-E, miniPCI-E или M.2)

## Реальная ситуация

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 установку 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 ВСЕМ ВОПРОСАМ

НУМА ТЕХНОЛОГИИ



Отдел по работе с Партнерами

+7 812 309 06 01

[sales@numatech.ru](mailto:sales@numatech.ru)

numa<sup>®</sup>  
TECHNOLOGY

СПАСИБО ЗА ВНИМАНИЕ