



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как обеспечить комплексную защиту информационных систем предприятия?

Андрей ПАСТУХОВ
НумаТех



О компании



Компания Нума Технологии – российский разработчик программного обеспечения и средств защиты информации, а также оператор услуг по защите информации, системной интеграции и консалтингу в области информационной безопасности.

10
лет

опыта
разработки
СЗИ

4

направления
технологий
безопасности

более
1000

защищенных
объектов
информатизации

7

СЗИ
собственной
разработки

3

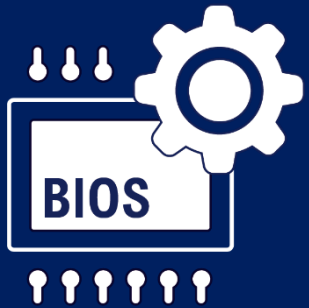
международных
технологических
партнера

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.

Области компетенций НумаТех

Микропрограммное
обеспечение БСВВ



Numa BIOS

Доверенная загрузка
операционных систем



Numa Arce

Комплексная
сетевая безопасность



Numa Edge

Технологии доверенной
виртуализации



Numa vServer

Техническая поддержка

Консультационные услуги

Профессиональные сервисы

Области применения продуктов



в государственных информационных системах до 1 класса защищенности включительно (Приказ ФСТЭК России № 17 от 11.02.2013);

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 № 31 от 14.03.2014);

в информационных системах персональных данных до 1 уровня защищенности (Приказ ФСТЭК России № 21 от 18.02.2013);

при защите значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК России № 239 от 25.12.2017);

в информационных системах общего пользования 2 класса (Приказ ФСТЭК России № 489 от 31.08.2010)

Numa BIOS. Назначение



Numa BIOS - российское программное обеспечение базовой системы ввода-вывода, разработанное с учетом требований по безопасности информации и критериев импортозамещения, являющееся полноценной альтернативой иностранным BIOS для средств вычислительной техники, построенных на базе x86 / x64 платформ Intel и AMD.



Ведется сертификация на соответствие Техническим условиям и Требованиям по безопасности информации, утвержденным приказом ФСТЭК России от 30.07.2018 № 131 - по 4 уровню доверия.

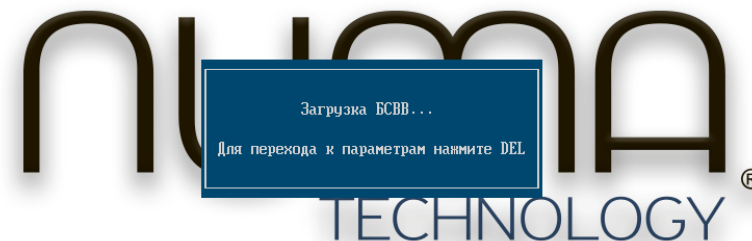
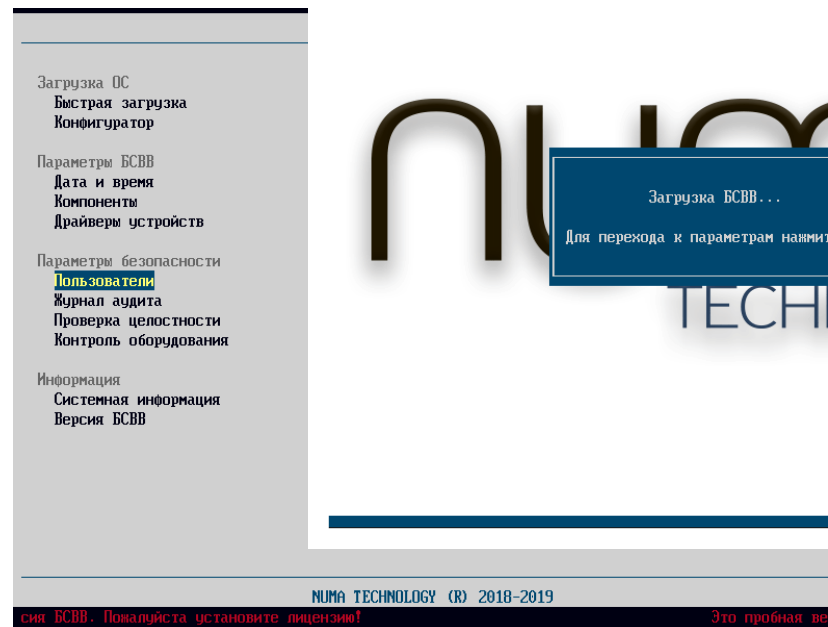
Предварительный планируемый срок окончания сертификации: II квартал 2020 года.



Numa BIOS включен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Регистрационный номер ПО: 5467

Дата регистрации: 24.06.2019



Numa BIOS. Возможности и преимущества



Наличие
исходных кодов



Российское
микропрограммное
обеспечение



Полноценная замена
оригинального
BIOS



Универсальная
модульная
архитектура



Управление
аппаратными
компонентами



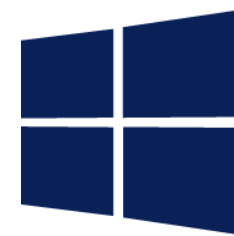
Установка МДЗ
Numa Arce



Встроенные
функции контроля



Поддержка
стандартов



Поддержка
требований
Microsoft



Заказная разработка
и адаптация

Numa Arce. Назначение



Numa Arce – программный модуль доверенной загрузки, разработанный НумаТех специально для использования в среде Numa BIOS. Предназначен для защиты средств вычислительной техники от несанкционированного доступа и обеспечения контроля целостности программной и аппаратной конфигурации СВТ, на которых он установлен, до начала работы операционной системы или гипервизора.



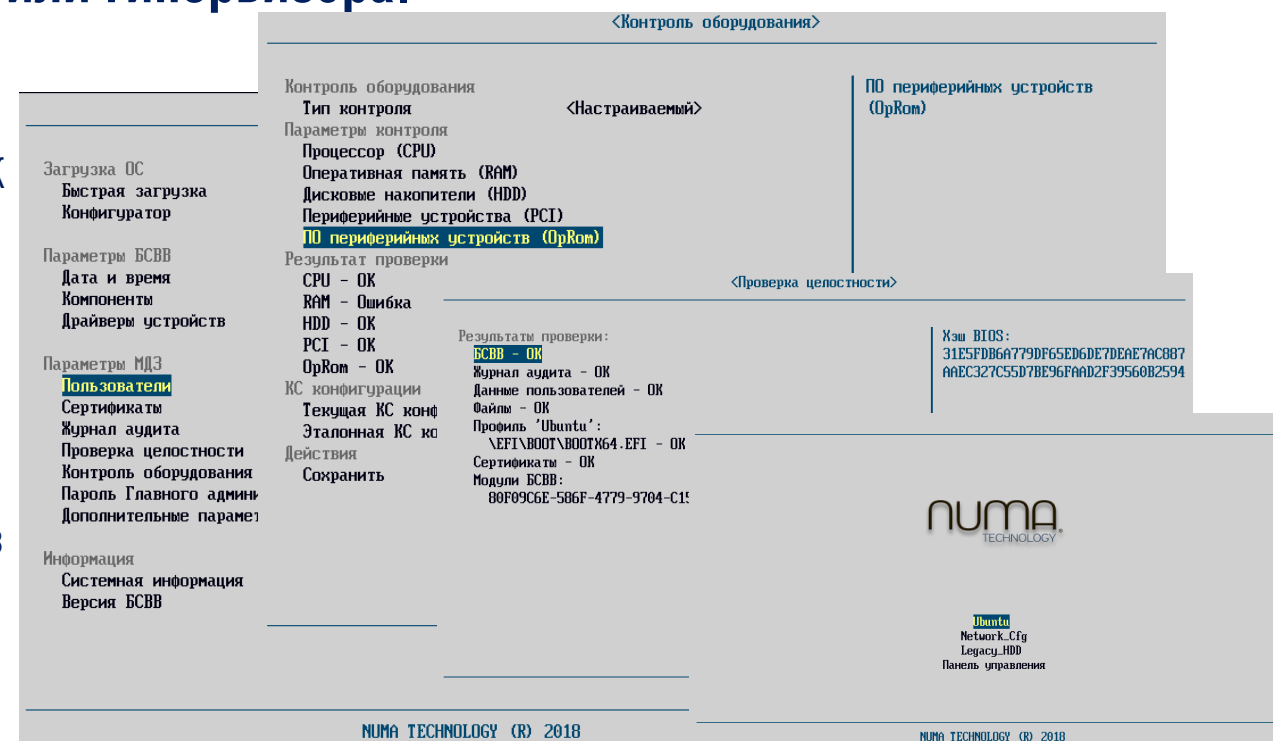
Ведется сертификация на соответствие «Требованиям к средствам доверенной загрузки» (ФСТЭК России, 2013) и Профилю защиты ИТ.СДЗ.УБ4.ПЗ. Предварительный планируемый срок окончания сертификации: IV квартал 2019 года.



Numa Arce включен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Регистрационный номер ПО: 5343

Дата регистрации: 06.05.2019



Numa Arce. Возможности и преимущества



Обеспечение
доверенной
загрузки ОС



Комплексный
контроль
целостности



Неизвлекаемый
модуль
доверенной загрузки



Ролевая модель
разграничения
доступа



Поддержка
технологий
SSO, PKI



Удаленная авторизация
пользователей
на LDAP/AD



Возможность
интеграции с
SIEM системами



Поддержка
аппаратных
идентификаторов



Единственное
ПО
тонкого клиента



Централизованный
сбор событий
безопасности

Numa vServer. Назначение



Numa vServer – доверенная система серверной виртуализации, разработанная с учетом требований по безопасности информации, предназначенная для создания защищенной виртуальной инфраструктуры корпоративного уровня.

Области применения:



Виртуализация
отдельных
серверов



Частные
облачные
инфраструктуры

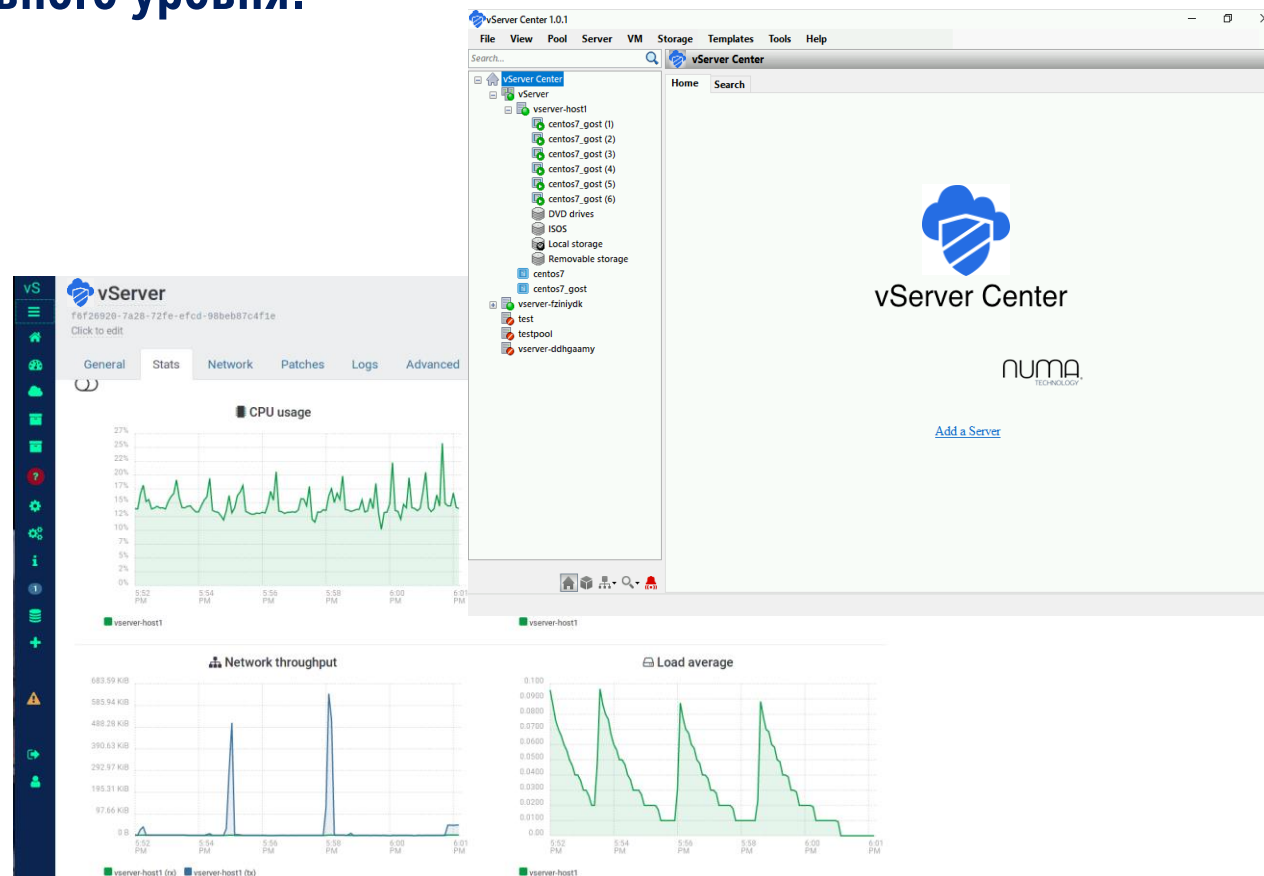


Защищенная
среда
Numa Sphere



Ведется подготовка к сертификации на соответствие Техническим условиям и Требованиям по безопасности информации, утвержденным приказом ФСТЭК России от 30.07.2018 № 131 - по 4 уровню доверия.

Предварительный планируемый срок окончания сертификации: IV квартал 2020 года.



Numa vServer. Возможности и преимущества



Наличие
исходных
кодов



Гарантированная
непрерывность
бизнеса



Расширенные
возможности работы
с графикой



Виртуализация
сети



Работа с системами
хранения
данных



Active directory
и ролевая модель
управления



Запуск любых
типов VM



Мониторинг
и статистика



Создание
резервных
копий

Numa vServer. Особенности



Numa vServer. Защищенное частное облако. Требования

Основной задачей проекта являлось создание защищённого географически распределённого частного облака, обладающего следующими характеристиками:

- Бесшовное масштабирование вычислительных ресурсов и системы хранения;
- Отказоустойчивость и катастрофоустойчивость;
- Настраиваемый уровень резервирования;
- Возможность сервисного управления (IaaS/PaaS/SaaS);
- Зонирование облака.

Задача выполнялась в два этапа:

- Построение базового узла облака;
- Интеграция нескольких узлов и системы управления.

Решение реализовано на базе доверенной системы серверной виртуализации Numa vServer.



Numa vServer. Защищенное частное облако. Результаты

Один узел облака:

- Реализовано частное облако на базе локального ЦОД:
 - 1 ПБ – хранилище (4-х кратный резерв);
 - 3000 вычислительных ядер;
 - 40 Гбит/сек – скорость передачи данных;
 - Скорость чтения/записи – 10 ГБ/сек;Эксплуатация у заказчика в течении 2,5 лет.

Распределённое облако:

- Макет облака, состоящий из 2-х узлов ЦОД.
Работает в настоящее время.



Numa Edge. Назначение



Numa Edge – программно-технический межсетевой экран, соответствующий концепции универсального шлюза безопасности (UTM), обеспечивающий реализацию функций межсетевого экранирования, контентной фильтрации, обнаружения вторжений, криптографической защиты каналов передачи данных, защиты от вирусов и спама.



Самый широкий модельный ряд среди программно-технических межсетевых экранов, представленных на российском рынке и сертифицированных ФСТЭК России, все исполнения которого имеют в своем составе доверенное программное обеспечение Numa BIOS.



Развитый функционал, обеспечивающий возможность применения Numa Edge в качестве замены иностранных изделий корпоративного уровня, не соответствующих требованиям по безопасности информации и критериям импортозамещения.



Ведется сертификация на соответствие «Требованиям к межсетевым экранам» (ФСТЭК России, 2016) и Профилям защиты ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Б4.ПЗ

Предварительный планируемый срок окончания сертификации: IV квартал 2019 года.



Ведутся работы по встраиванию сертифицированного ФСБ России СКЗИ

Предварительный планируемый срок окончания работ: I квартал 2020 года.



Ведется подготовка к сертификации на соответствие «Требованиям к системам обнаружения вторжений» (ФСТЭК России, 2011) и Профилю защиты ИТ.СОВ.С4.ПЗ

Предварительный планируемый срок окончания сертификации: IV квартал 2020 года.



Numa Edge. Программные модули

В Numa Edge реализована архитектура программных модулей, которая позволяет создавать индивидуальную функциональную конфигурацию.

Возможности устройства зависят от выбранной комбинации программных модулей, каждый из которых обладает собственным набором функций.

Исполнение Numa Edge	Программные модули			
	МЭ	СКЗИ	СОВ	АВ/АС
Исполнение 1	+	-	-	-
Исполнение 2	+	-	+	-
Исполнение 3	+	+	+	-
Исполнение 4	+	+	+	+
Исполнение 5	+	+	-	-
Исполнение 6	+	+	-	+
Исполнение 7	-	-	+	-



Межсетевой экран (МЭ)

Осуществляет коммутацию и агрегирование, статическую и динамическую маршрутизацию, фильтрацию трафика с учетом обширного набора критериев, в том числе, по мандатным меткам и по базе GEO IP, проксирование веб-трафика. Встроенные функции безопасности и создание кластеров Active-passive, Active-standby гарантируют бесперебойную работу решения.

Базовый модуль



Система обнаружения вторжений (СОВ)

Модуль позволяет использовать систему обнаружения Numa IDS для защиты от комплексных сетевых атак. Имеется возможность интеграции со сторонними системами SIEM или ГосСОПКА.

Может использоваться либо в качестве единственного программного модуля, развернутого на аппаратной платформе, либо расширять функции уже развернутых на устройстве модулей.

Дополнительный модуль



Криптография ГОСТ (СКЗИ)

Модуль позволяет решить задачу построения защищенных каналов передачи данных. Поддержка российских криптографических алгоритмов и различных способов построения VPN позволяет создавать надежные межфилиальные соединения и осуществлять клиент-серверные подключения мобильных пользователей, соблюдая требования российского законодательства.

Дополнительный модуль



Антивирус/Антиспам (АВ/АС)

Модуль позволяет использовать различные встроенные антивирусные и анти-спам решения, расширяет возможности веб-прокси и контентной фильтрации.

Дополнительный модуль

Numa Edge. Возможности и преимущества



Балансировка нагрузки
между несколькими
внешними каналами



Фильтрация по
мандатным меткам,
базе GEO IP



Поддержка российских
криптографических
алгоритмов



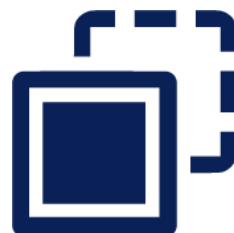
Обнаружение и
предотвращение
вторжений



Ролевая
модель
доступа



Кластер: Active-passive,
Active-standby
с сохранением состояния



Поддержка
ICAP

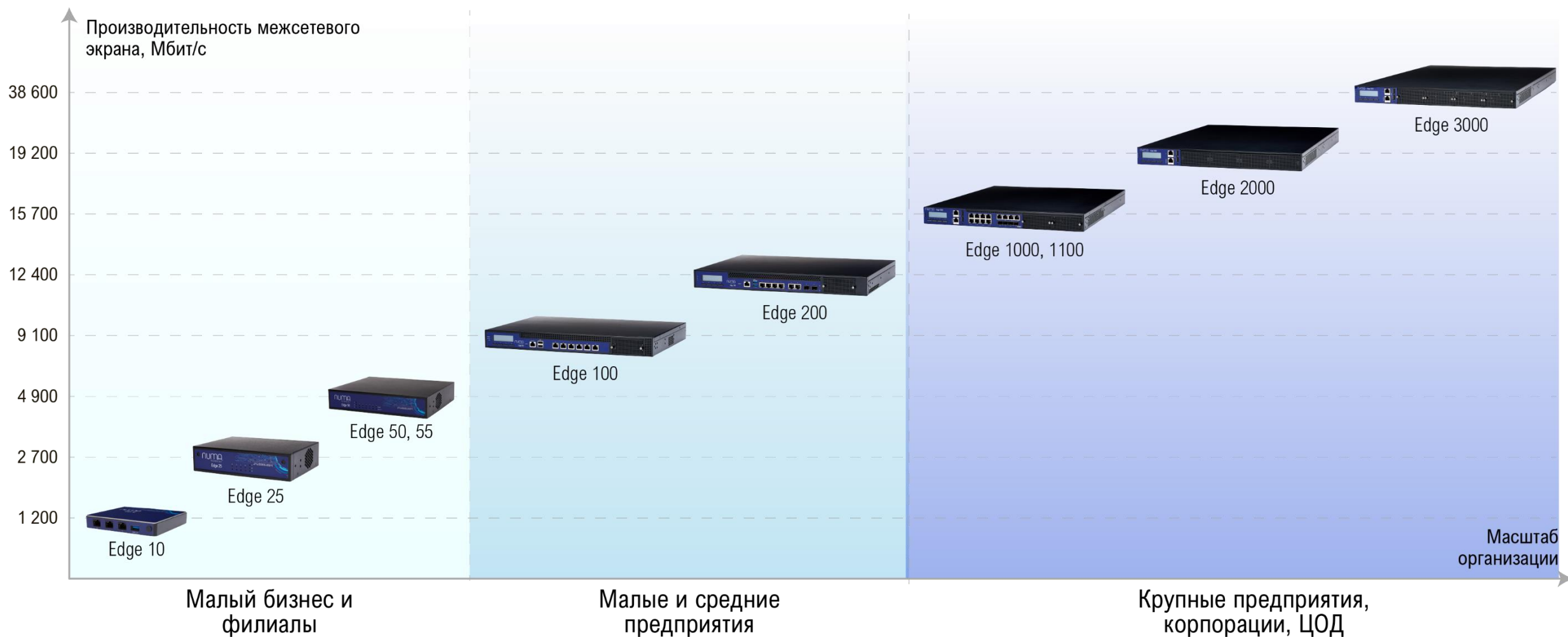


Разнообразие
сетевых
интерфейсов



Доверенная
аппаратная
платформа

Numa Edge. Продуктовая линейка



Numa Edge. Аппаратные модули расширения



Устройства серий Numa Edge 100 и выше могут комплектоваться дополнительными сетевыми модулями расширения.

	Numa Edge 100	Numa Edge 200	Numa Edge 1000	Numa Edge 1100	Numa Edge 2000	Numa Edge 3000
Доступное количество	1 модуль расширения	1 модуль расширения	2 модуля расширения	4 модуля расширения		
4xRJ45 GE	✓	✓	✓	✓	✓	✓
8xRJ45 GE	✓	✓	✓	✓	✓	✓
4xSFP GE	✓	✓	✓	✓	✓	✓
8xSFP GE	✓	✓	✓	✓	✓	✓
2xSFP+ 10GE	—	—	✓	✓	✓	✓
4xSFP+ 10GE	—	—	—	—	✓	✓
2xQSFP+ 40GE	—	—	—	—	—	✓

Numa Edge. Беспроводные технологии

Устройства Numa Edge 10, 25, 50, 55, предназначенные для защиты филиалов и малого бизнеса, поддерживают беспроводные технологии 3G, Wi-Fi и LTE, в том числе, их одновременную работу. Возможность работы через сотового оператора стандарта 3G или LTE может быть полезна в случае неполадок на линии у основного провайдера, позволяя обеспечить резервный канал передачи данных. Поддержка беспроводного стандарта Wi-Fi увеличивает удобство работы пользователей, при этом информационная система остается под надежной защитой.



	Numa Edge 10	Numa Edge 25	Numa Edge 50	Numa Edge 55
3G	✓	—	—	—
Wi-Fi	✓	✓	✓	✓
LTE	—	✓	✓	✓
LTE + Wi-Fi	—	✓	✓	✓

Комплексная защита инфраструктуры

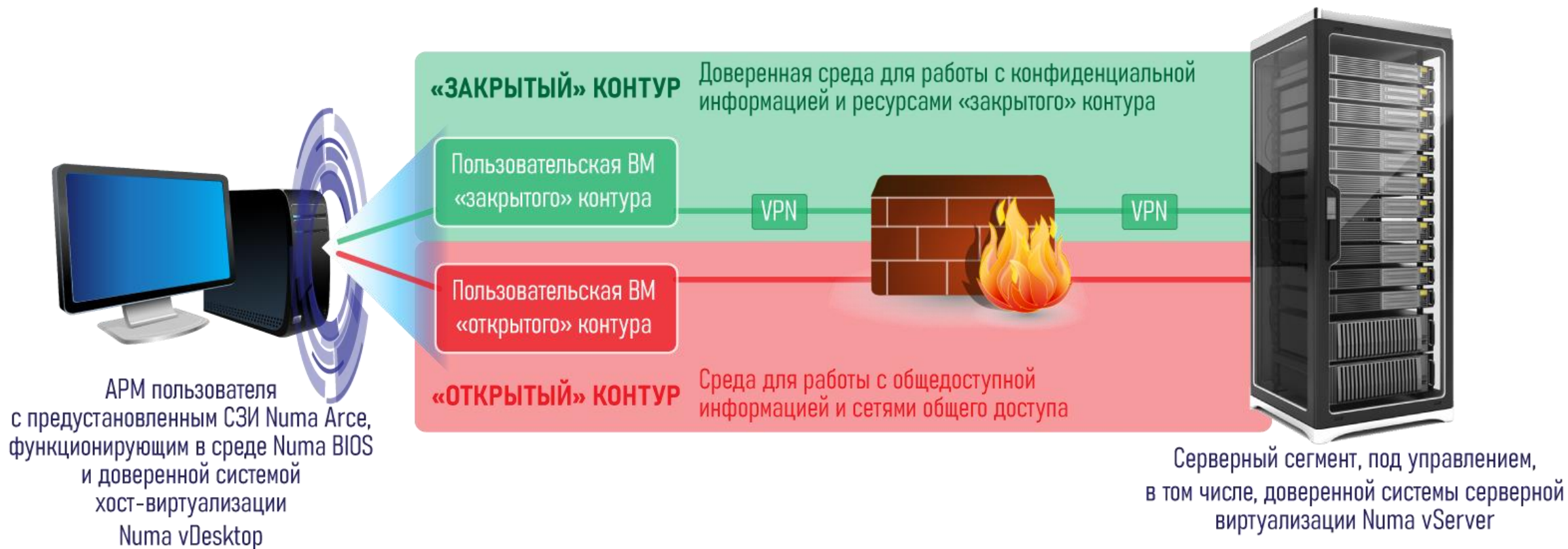
Тип средства защиты	Направление защиты	Продукты «НумаТех»
Средства защиты информации от НСД	Защита рабочих станций и серверов	Доверенная БСВВ Numa BIOS (Нет аналогов) ; Модуль доверенной загрузки Numa Arce ;
	Защита среды виртуализации	Доверенная система хост-виртуализации Numa vDesktop (Нет аналогов) ; Доверенная система серверной виртуализации Numa vServer .
	Защита мобильных устройств	Доверенная БСВВ Numa BIOS (Нет аналогов) ; Модуль доверенной загрузки Numa Arce ; Доверенная система хост-виртуализации Numa vDesktop (Нет аналогов) .
Межсетевой экран	Защита сетевой инфраструктуры	Программно-технический межсетевой экран Numa Edge
Средство обнаружения вторжений	Защита сетевой инфраструктуры	Система обнаружения вторжений Numa IDS ; Программно-технический межсетевой экран Numa Edge (с установленным программным модулем Numa IDS).
Средства защиты каналов передачи данных	Защита сетевой инфраструктуры	Программно-технический межсетевой экран Numa Edge (с установленным СКЗИ).

Комплексное использование продуктов НумаТех

Специализированное комплексное решение **Numa Sphere** - защищенная среда функционирования информационных систем

Numa Sphere. Концепция решения

Numa Sphere – защищенная среда функционирования информационных систем любого масштаба и распределённости, обеспечивающая реализацию необходимых функций безопасности информации на всех уровнях архитектуры информационной системы, без ущерба для качества ее сервисов.



Numa Sphere. Основные компоненты. Защищенный АРМ пользователя

Аппаратная платформа, с предустановленным программным обеспечением и средствами защиты информации:

- Программное обеспечение Numa BIOS;
- Модуль доверенной загрузки Numa Arce;
 - Защита от НСД, доверенная загрузка АРМ, неизвлекаемость из АРМ.
- Доверенная система host-виртуализации Numa vDesktop;
 - Создание и изоляция «открытой» и «защищенной» среды (в виде виртуальных машин: доверенная VM, Интернет VM)
 - Использование единого физического канала для передачи информации разного уровня обработки (конфиденциальная и открытая)
 - Однонаправленная передача данных из «открытой» в «защищенную» среду обработки данных посредством однонаправленного шлюза.
 - **Изолированное СКЗИ.** Изолированная виртуальная машина для защиты канала связи. СКЗИ недоступно пользователю (он не может оказать влияния на его работу).



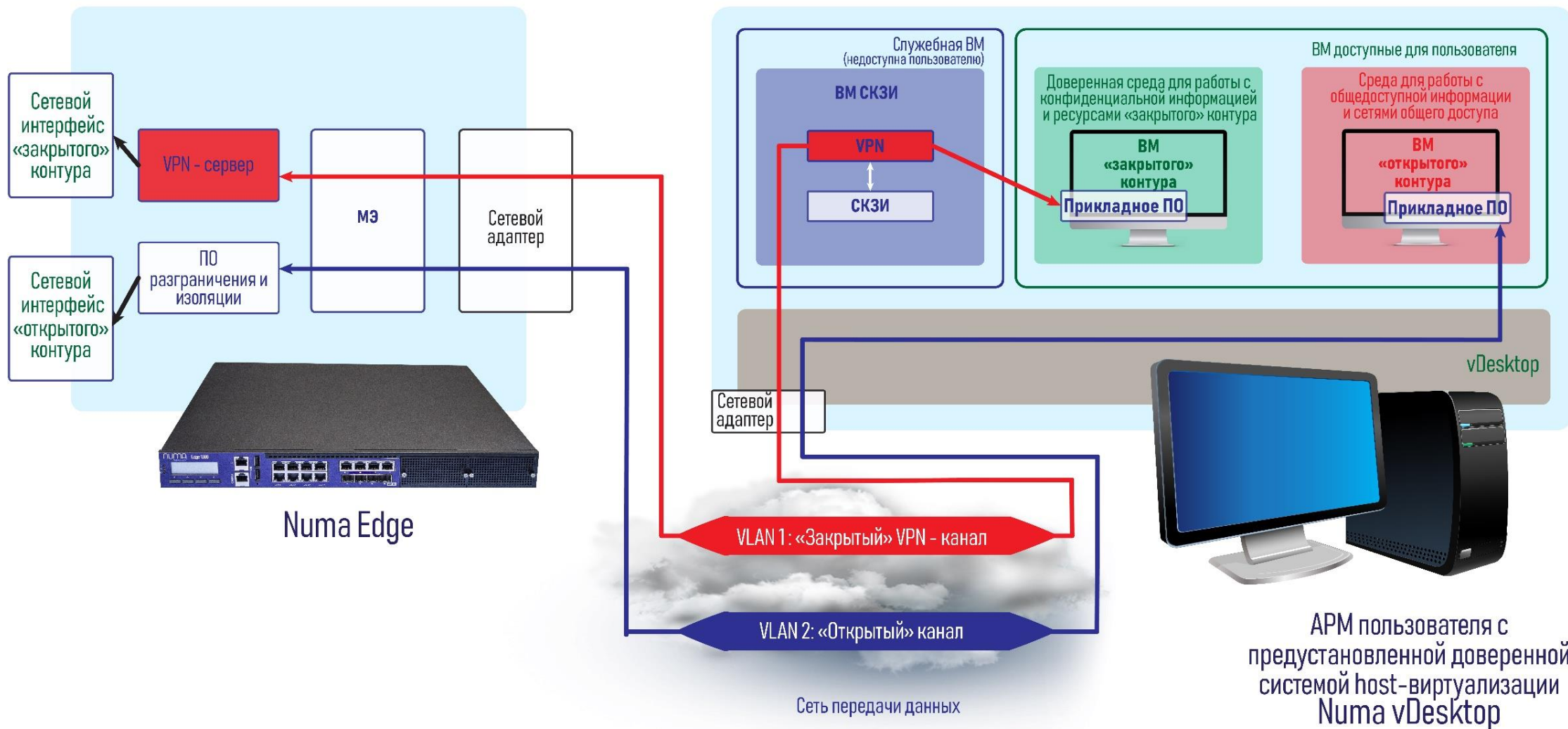
Numa Sphere. Основные компоненты. Защита сети и каналов связи

Программно-аппаратный комплекс Numa Edge, обеспечивающий:

- защиту периметра ЛВС от внешних угроз;
- сегментирование ЛВС объекта информатизации и управление информационными потоками;
- фильтрацию сетевого трафика и защиту от вредоносного контента;
- защиту каналов связи, выходящих за пределы контролируемой зоны;
- защиту каналов связи внутри контролируемой зоны между территориальными подразделениями - криптошлюз для ВМ «защищенного» контура.



Numa Sphere. Принцип функционирования. Организация информационных потоков



АРМ пользователя с
предустановленной доверенной
системой host-виртуализации
Numa vDesktop

Как обеспечить комплексную защиту информационных систем предприятия?

Использовать продукты и технологии НумаТех!

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ



**+7 (921) 858 9661,
pastukhov@numatech.ru
<https://numatech.ru>**