РусБИТех
WWW.RUSBITECH.RU

СПРАВКА

ОБ ОСОБЕННОСТЯХ И ОСНОВНЫХ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЯХ АПМДЗ «МАКСИМ-М1»

МАКСИМ®

АППАРАТНО-ПРОГРАММНЫЙ МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ «МАКСИМ-М1»

(Изделие М-643М1)

HARDWARE READY FOR ASTRA LINUX
ASTRA LINUX SPECIAL EDITION

МАКСИМ®

НАЗНАЧЕНИЕ АПМДЗ «МАКСИМ-М1»

АПМДЗ «МАКСИМ-М1» (изделие М-643М1) — аппаратно-программный модуль доверенной загрузки может использоваться на территории Российской Федерации в качестве средства защиты от НСД к техническим, программным и информационным ресурсам ПЭВМ, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно, а также конфиденциальную информацию с уровнем защиты до КА1 включительно. **АПМДЗ «МАКСИМ-М1» соответствует требованиям ФСБ России к АПМДЗ ЭВМ по классу 1Б.**

СЕРТИФИКАТ СООТВЕТСТВИЯ

ФСБ России
No СФ/027-1879 от 29 июня 2012 г.

АПМДЗ «МАКСИМ-М1» ОБЕСПЕЧИВАЕТ:

- ✓ Двухфакторную идентификацию и аутентификацию пользователей на этапе начальной загрузки до передачи управления ОС.
- ✓ Ведение в энергонезависимой памяти недоступных для стирания журналов регистрации событий аутентификации пользователей и контроля целостности.
- ✓ Контроль сроков действия ключей и служебной информации пользователей с использованием часов реального времени с автономным питанием.
- ✓ Контроль целостности областей оперативной памяти, загрузочных областей жестких дисков, областей журнала файловой системы и файлов для файловых систем FAT16, FAT32, NTFS 3.0, NTFS 3.1, Ext2, Ext3 и Ext4.
- ✓ Физический датчик случайных чисел для формирования пароля аутентификации, соответствующий требованиям ФСБ.
- ✓ Защиту от подбора пароля.
- ✓ Контроль целостности реестра Windows.

КЛАСС ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

АПМДЗ «МАКСИМ-М1» может использоваться в составе автоматизированных систем класса защищенности до 1Б включительно.

Группа АС	3 группа Однопользовательская				2 группа Многопользовательская с равными полномочиями				1 группа Многопользовательская с разными полномочиями			
Класс АС	3Б	3А			2Б	2А			1Д	1Г	1В	1Б
Применение модулей доверенной загрузки	–	–	–	–	–	+	+	+	–	+	+	+
Класс межсетевых экранов	5	3	2	1	5	3	2	1	5	4	3	2
Класс СВТ	5	4	3	2	5	4	3	2	5	5	4	3
Уровень контроля отсутствия НДВ	4	3	2	1	4	3	2	1	4	4	3	2

ОС СН «Astra Linux Special Edition» АПМДЗ «Максим-М1»

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

МАКСИМ®

ХАРАКТЕРИСТИКИ АПМДЗ «МАКСИМ-М1»

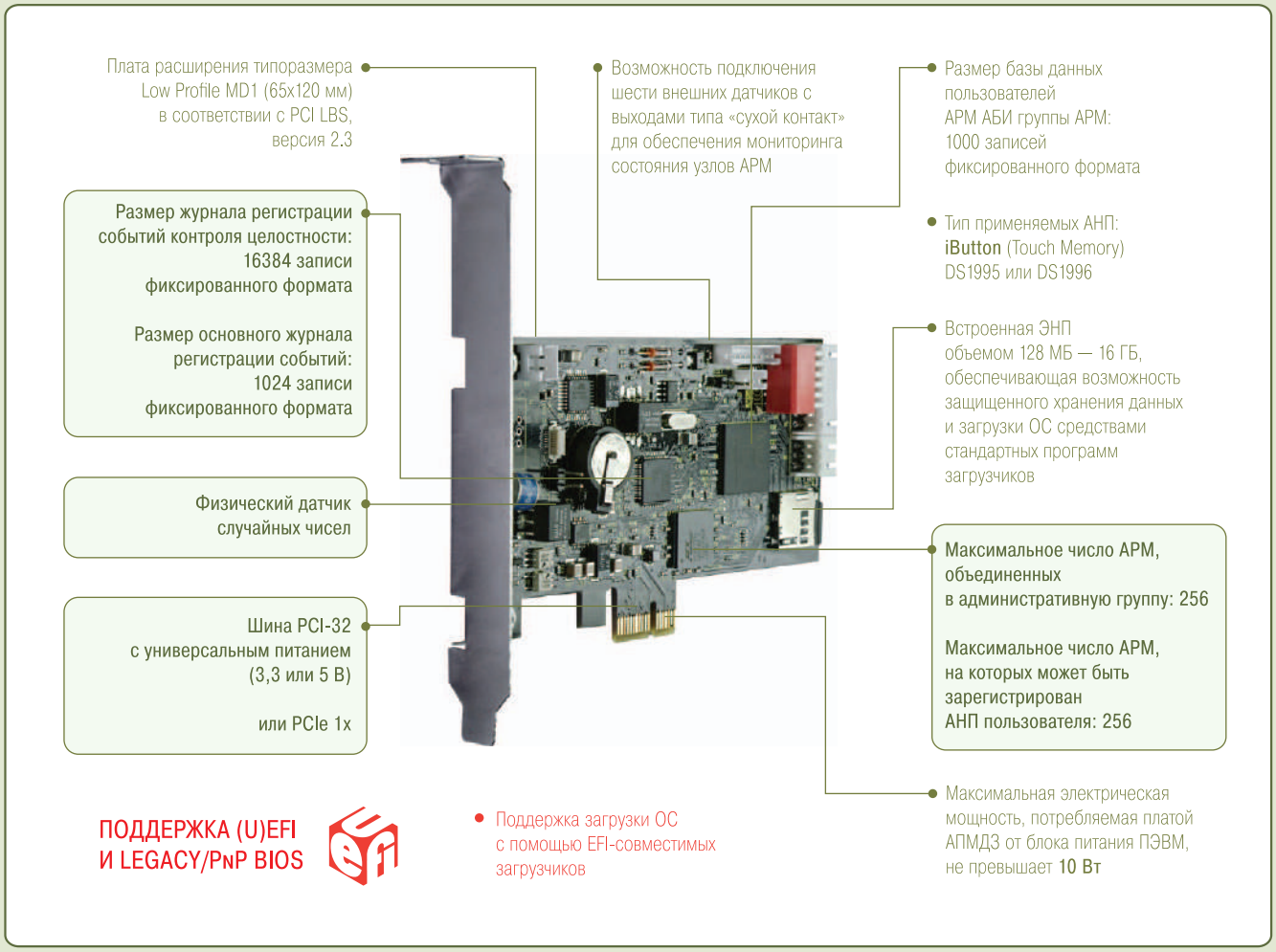
ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ АПМДЗ «МАКСИМ-М1»

Поддерживает операционные системы:

ASTRA LINUX — HARDWARE READY FOR ASTRA LINUX ASTRA LINUX SPECIAL EDITION

LINUX
Ядро 2.6.x
или 3.x.x

WINDOWS
2000/XP/Vista/7
Server 2003/2008
Microsoft Windows

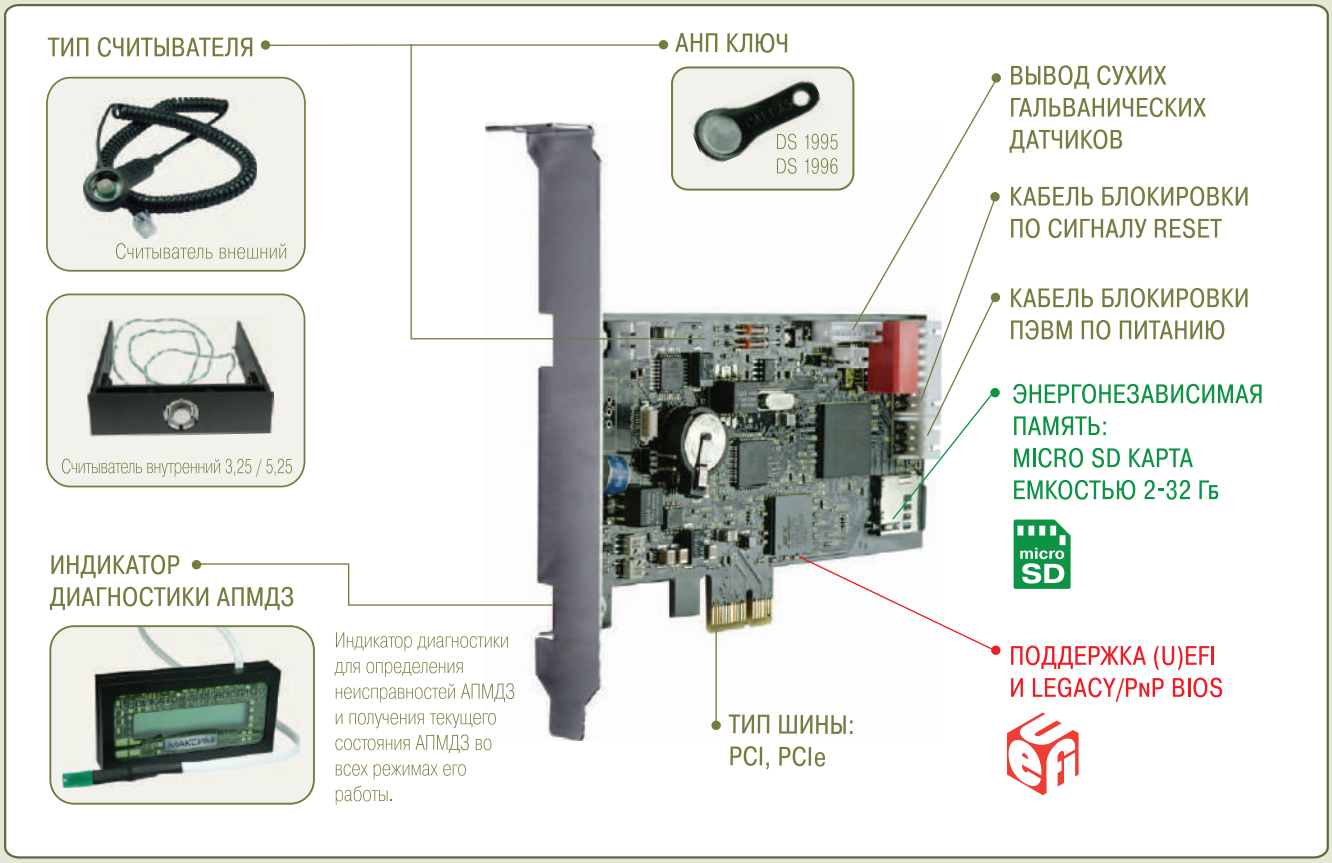


Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

МАКСИМ®

КОМПЛЕКТ ПОСТАВКИ АПМДЗ «МАКСИМ-М1»



Наименование компонента	Варианты поставки компонента	Количество
Плата АПМДЗ	PCI PCI-E	1 штука
Считыватель АНП типа iButton	Внешний (поставляется с креплением) Внутренний 3.5” Внутренний 5.25”	1 штука
Кабель блокировки	Кабель блокировки ПЭВМ Кабель блокировки по RESET Оба варианта кабеля (комплект)	1 штука
Съемный накопитель microSD	Опционально 2-32 Гб	1 штука
АНП типа iButton (может поставляться в любом необходимом количестве)		1 штука
Программное обеспечение и документация на CD		1 штука

Дополнительное оборудование (в комплект поставки АПМДЗ не входит)	
Индикатор диагностики АПМДЗ	опционально
АНП россыпью	опционально

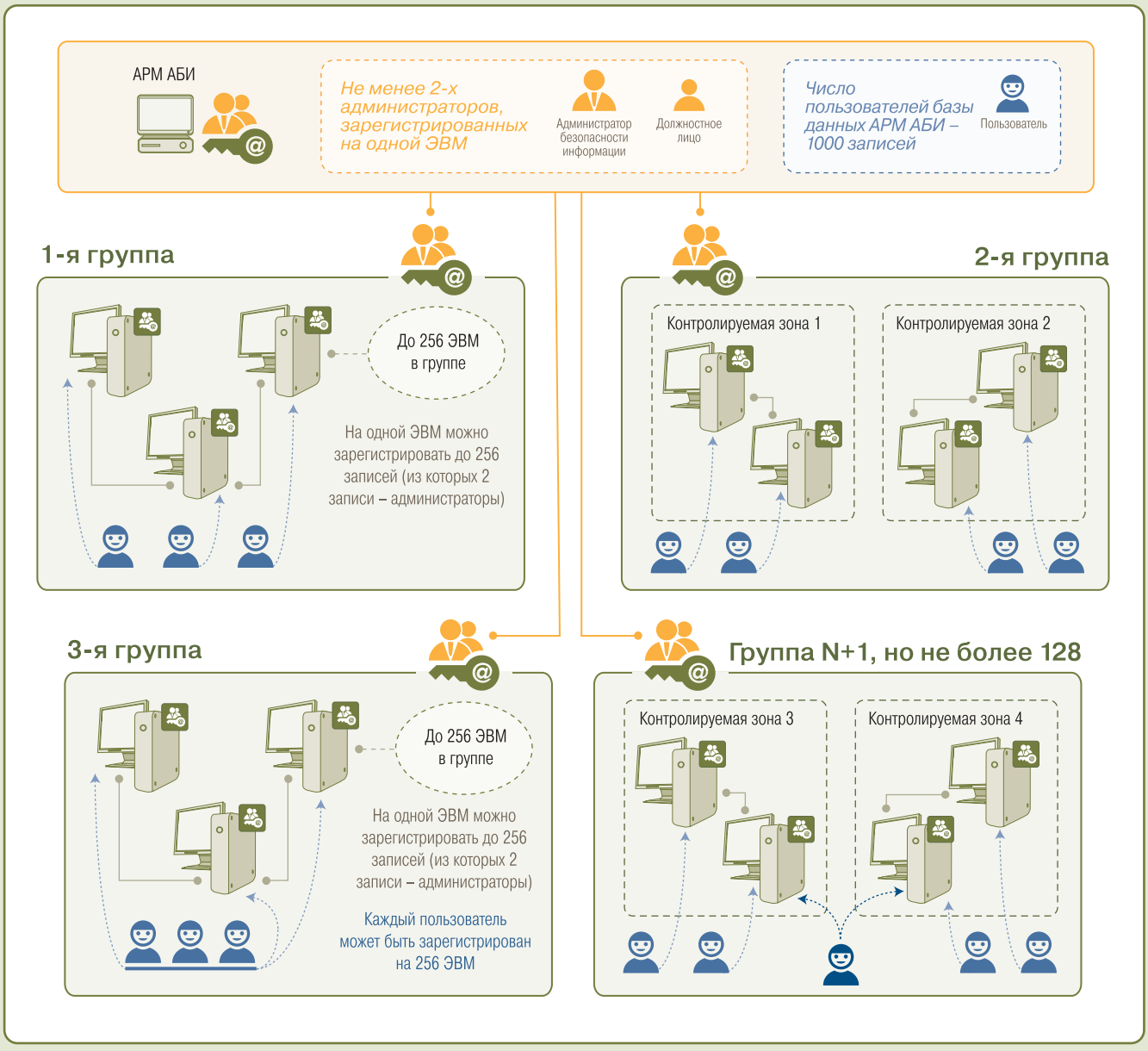
Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

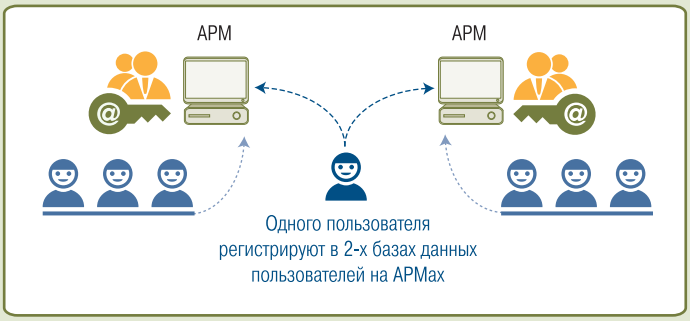
МАКСИМ®

СХЕМА АДМИНИСТРИРОВАНИЯ АПМДЗ «МАКСИМ-М1»

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ



ДЕЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ



Виды защищаемой информации

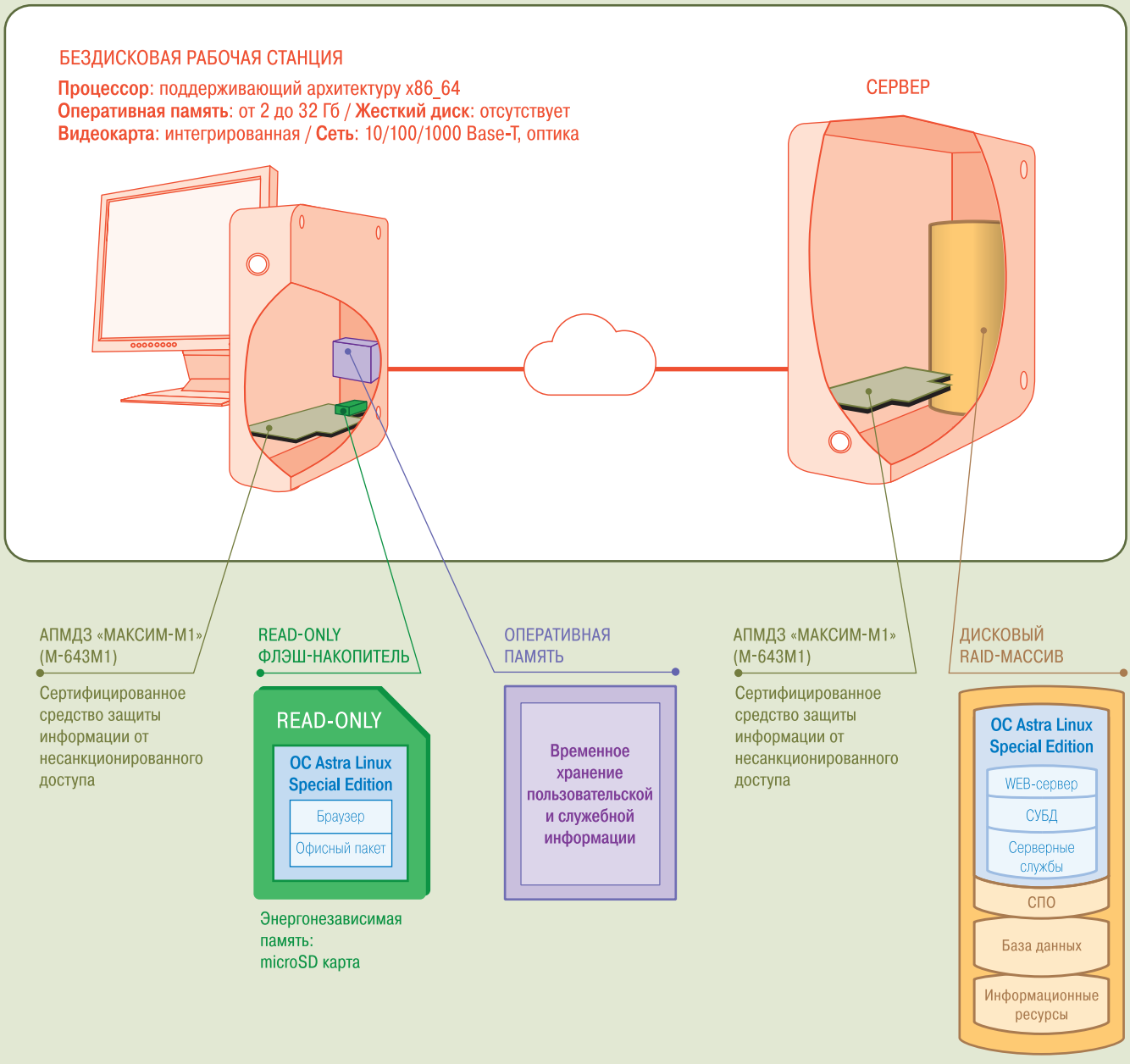
Коммерческая тайна	Персональные данные	Государственная тайна

МАКСИМ®

ПРИМЕР СОЗДАНИЯ БЕЗДИСКОВЫХ РАБОЧИХ СТАНЦИЙ

Унифицированное решение предназначено для создания защищенных автоматизированных систем, обрабатывающих информацию до грифа «совершенно секретно» включительно.

Ключевой особенностью комплекса является отсутствие на носителях информации ограниченного доступа (вся информация хранится на сервере).



- ✓ Модульная аппаратная и программная платформа
- ✓ Средства защиты информации, сертифицированные ФСБ России, ФСТЭК России и Минобороны России
- ✓ Мобильность и компактность
- ✓ Высокая производительность
- ✓ Бездисковая рабочая станция
- ✓ Легкость организации рабочего места
- ✓ Быстрая замена АРМ в случае поломки

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

МАКСИМ®

ТРЕБОВАНИЯ

ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

К оборудованию и ПО выдвигаются следующие требования:

- плата АПМДЗ устанавливается в ПЭВМ, оснащенные процессорами с архитектурой x86/x86-64 класса Pentium или выше;
- для подключения АПМДЗ системная плата ПЭВМ должна быть оснащена системной шиной PCI версии 2.3 с напряжением питания 3,3 или 5 В или PCIe версии 1.0, на которой должен быть в наличии хотя бы один свободный разъем;
- BIOS ПЭВМ должен соответствовать одной из перечисленных спецификаций: PnP BIOS версии 1.0A / EFI версии 1.10 / UEFI версии не ниже 2.1;
- PnP BIOS ПЭВМ должен поддерживать функции, определяемые спецификацией BIOS EDD версии 3.0;
- в ОС Windows 2000 должно быть установлено обновление KB835732;
- (U)EFI BIOS ПЭВМ должен обеспечивать выполнение программных модулей для аппаратной платформы x86-64 (x64/AMD64/Intel64/EM64T);
- разъем питания системной платы ПЭВМ должен отвечать требованиям спецификации ATX и иметь 20 или 24 контакта, блок питания ПЭВМ должен удовлетворять требованиям спецификации ATX.

ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ

АПМДЗ предназначен для применения в ПЭВМ, удовлетворяющих приведенны ниже эксплуатационным ограничениям:

1) системная плата ПЭВМ должна иметь хотя бы один из разъемов:
- для подключения кабеля блока питания;
- для подачи сигнала системного сброса (RESET);
- для подачи сигнала включения/выключения питания ПЭВМ (POWER_OFF);

и обеспечивать возможность подключения кабеля блокировки ПЭВМ или кабеля блокировки ПЭВМ по сигналу Reset, входящего в состав АПМДЗ.

2) при эксплуатации АПМДЗ на ПЭВМ администратором должны быть запрещены режимы энергосбережения, такие как «Standby» и «Hibernate»;

3) при использовании АПМДЗ не поддерживается:
- КЦ файлов, преобразованных криптографическими программами (BestCrypt или аналогичными), программами сжатия дисков (Drivespace и аналогичными) и т. п.;
- КЦ для логических дисков, являющихся наборами томов (например, LVM, StripeSet, Software RAID);
- КЦ секторов, размещающихся за пределами первых 8 ГБ, при условии, что хотя бы один из нескольких жестких дисков ПЭВМ не поддерживает работу с расширенным набором функций системной BIOS;
- контроль альтернативных потоков данных для директорий (контролируются только альтернативные потоки данных для файлов);
- КЦ файлов, расположенных на разделах (томах) с ФС NTFS, для которых установленная и настроенная ОС поддерживает возможность различения регистра символов имен файлов;

4) при использовании подсистемы КЦ АПМДЗ должно быть обеспечено выполнение следующих ограничений:
- длина пути любого контролируемого файла в ОС Windows (для ФС FAT16, FAT32, NTFS) не должна превышать 256 символов;
- длина пути любого контролируемого файла в ОС Linux (для ФС Ext2, Ext3, Ext4) не должна превышать 1024 символов;

МАКСИМ®

ТРЕБОВАНИЯ

- количество контролируемых файлов не должно превышать 4095;
- число контролируемых записей реестра не должно превышать 1023;
- количество контролируемых файлов реестра не должно превышать 255;
- размер блока данных для ФС Ext2, Ext3, Ext4, NTFS не должен превышать 4 КБ;
- не допускается использование символьных ссылок в ФС NTFS (NTFS Symbolic Link), точек соединения ОС Windows (Windows Junction Point), жестких ссылок ФС NTFS (NTFS Hardlink);

5) при использовании АПМДЗ обеспечивается работа (подсистемы КЦ и утилиты чтения служебной информации) только совместно с ОС Windows 7 (32 и 64 бит), 2008 Server (32 и 64 бит), Vista (32 и 64 бит), 2003 Server (32 и 64 бит), XP, 2000 Server/Workstation, а также Linux (с ядром 2.6.x или 3.x.x).

СПЕЦИАЛЬНЫЕ УСЛОВИЯ

АПМДЗ может использоваться на территории Российской Федерации в качестве средства защиты от НСД к техническим, программным и информационным ресурсам ПЭВМ, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно, а также информацию, не содержащую сведений, составляющих государственную тайну (конфиденциальную информацию с уровнем защиты до КА1 включительно), при выполнении следующих условий:

- сохранение в тайне персональных аутентификаторов, записанных в АНП, паролей администраторов и пользователей, идентификатора и главного ключа АПМДЗ (во внутренней ЭНП платы АПМДЗ);
- соблюдение условий и правил эксплуатации, установленных в эксплуатационной документации.

А также при выполнении следующих требований:

1) для эксплуатации АПМДЗ в составе ПЭВМ должны быть проведены исследования технических средств ПЭВМ (в том числе исследования системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования ПЭВМ и АПМДЗ или к утечке защищаемой информации. Исследования должны проводиться специализированной организацией с последующей экспертизой в установленном порядке;

2) при транспортировке и хранении АПМДЗ должны быть приняты организационно-технические меры, исключающие НСД к его программным и аппаратным средствам;

3) при эксплуатации АПМДЗ должны быть приняты организационно-технические меры по сохранению целостности корпуса ПЭВМ, исключающие НСД к аппаратным средствам АПМДЗ и техническим средствам ПЭВМ, расположенным внутри системного блока ПЭВМ, после установки и настройки АПМДЗ;

4) при эксплуатации АПМДЗ должны быть предусмотрены меры, препятствующие модификации (перепрограммированию) как системной программы BIOS, так и расширений BIOS в ПЭВМ с установленным АПМДЗ;

5) при установке аппаратных компонентов АПМДЗ обязательно подключение кабеля блокировки ПЭВМ по сигналу RESET или кабеля блокировки ПЭВМ, входящих в состав АПМДЗ. При подаче сигналов сброса (RESET) и/или выключения питания (POWER_OFF) на соответствующие разъемы системной платы ПЭВМ должна обеспечиваться перезагрузка или выключение питания ПЭВМ. Возможность влияния на эти механизмы со стороны программных и аппаратных средств ПЭВМ (например, путем отключения из BIOS Setup) должна быть исключена;

6) необходимо обеспечить невозможность перевода ПЭВМ в режимы энергосбережения, при выходе из которых управление не передается АПМДЗ (например, режимы S3, S4);

ТРЕБОВАНИЯ

7) один сеанс работы АПМДЗ, т. е. время между включением (перезагрузкой) ПЭВМ и началом загрузки ОС, не должен превышать 24 часов;

8) должна быть обеспечена невозможность загрузки ОС с внешних устройств (устройств, подключаемых к внешним интерфейсным разъемам ПЭВМ, например, SCSI, SATA и т. д., за исключением устройств, подключаемых по интерфейсам USB и IEEE 1394);

9) должна быть обеспечена невозможность загрузки ОС со всех загрузочных устройств, за исключением загрузочного системного НЖМД (или устройства хранения), после передачи управления от ПО АПМДЗ программе-загрузчику ОС;

10) АПМДЗ разрешается устанавливать в ПЭВМ, аттестованную и допущенную для обработки конфиденциальной информации без предъявления каких либо дополнительных специальных требований. АПМДЗ разрешается устанавливать в ПЭВМ, аттестованную для обработки информации с грифом не выше «совершенно секретно», и имеющую соответствующее предписание. При этом должны выполняться требования предписания и перечисленные ниже требования;

11) вокруг ПЭВМ с установленным АПМДЗ и считывателя АНП необходимо обеспечить контролируемую зону радиусом, указанным в предписании на ПЭВМ, но не менее 3 м;

12) радиопередатчики, связную и измерительную аппаратуру, телефонные аппараты и другое оборудование, имеющие цепи, выходящие за пределы контролируемой зоны, необходимо располагать от ПЭВМ с установленным АПМДЗ и от считывателя АНП на расстоянии, указанном в предписании на ПЭВМ, но не менее 1,2 м;

13) провода, кабели и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны, необходимо располагать от ПЭВМ с установленным АПМДЗ и от считывателя АНП на расстоянии, указанном в предписании на ПЭВМ, но не менее 0,5 м;

14) электропитание ПЭВМ с установленным АПМДЗ необходимо осуществлять либо от трансформаторной подстанции, расположенной в пределах контролируемой зоны и не имеющей выхода низковольтных цепей за ее пределы, либо через сертифицированный сетевой помехоподавляющий фильтр, обеспечивающий затухание по паспортным данным не менее 10 дБ в диапазоне частот 0,15–1000 МГц. При этом сетевой фильтр и отходящий от него сетевой кабель должны размещаться в контролируемой зоне на расстояниях от ПЭВМ и от считывателя АНП не ближе значений, приведенных в перечислениях 12) и 13) соответственно. Заземление фильтра должно проводиться на контур заземления, расположенный в пределах контролируемой зоны;

15) заземление ПЭВМ с установленным АПМДЗ необходимо осуществлять на контур заземления, размещенный в пределах контролируемой зоны и не имеющий гальванических контактов с другими токопроводящими коммуникациями, выходящими за пределы контролируемой зоны;

16) АПМДЗ может эксплуатироваться в помещениях, где ведутся разговоры, содержащие сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно»;

17) подключение ПЭВМ с установленным АПМДЗ к линиям связи, выходящим запределы контролируемой зоны, необходимо осуществлять через сертифицированные средства криптографической защиты информации (СКЗИ), установленные в пределах контролируемой зоны на расстоянии от ПЭВМ с АПМДЗ и от считывателя АНП не менее указанного в 13). При использовании СКЗИ, встраиваемых в ПЭВМ с АПМДЗ, необходимо обеспечить в пределах контролируемой зоны гальваническую развязку между канальными цепями СКЗИ и линией связи, выходящей за пределы контролируемой зоны;

18) при эксплуатации АПМДЗ запрещается вносить изменения в его конструкцию и работать с открытой крышкой системного блока ПЭВМ.

Научно-производственное объединение
РусБИТех
Открытое акционерное общество

ВАШ НАДЁЖНЫЙ И КОМПЕТЕНТНЫЙ ПАРТНЁР

117105, Россия, г. Москва, Варшавское шоссе, д. 26
Тел.: +7 (495) 648-06-40 / Факс.: +7 (495) 648-06-39
E-mail: mail@rusbitech.ru / Сайт: www.rusbitech.ru