(19) Евразийское патентное ведомство

(11) 041757 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.11.29

(21) Номер заявки
202100171

(22) Дата подачи заявки
2021.06.17

(51) Int. Cl. ***G06F 21/50*** (2006.01)
G06F 21/62 (2006.01)

(54) СПОСОБ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ, РЕАЛИЗУЕМЫЙ НА УРОВНЕ АППАРАТНОЙ ПЛАТФОРМЫ ПОСРЕДСТВОМ МЕХАНИЗМОВ ВИРТУАЛИЗАЦИИ, И УСТРОЙСТВО ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(31) **2021111440**
(32) **2021.04.22**
(33) **RU**
(43) **2022.10.31**

(71)(73) Заявитель и патентовладелец:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "КИРОВСКИЙ РЕГИОНАЛЬНЫЙ ЦЕНТР ДЕЛОВОЙ ИНФОРМАЦИИ" (ООО "КРЦДИ") (RU)

(72) Изобретатель:
Фетищев Евгений Анатольевич, Фетищев Алексей Евгеньевич (RU)

(56) RU-C2-2581552
RU-C2-2557476
RU-C2-2446447
RU-C1-2691187
US-A1-20190130106
US-A1-20110167473

(57) Изобретение относится к области компьютерной безопасности и используется при создании защищенных компьютерных систем, предназначенных для передачи, обработки и хранения конфиденциальной информации. Целью предлагаемого технического решения является повышение безопасности компьютера. Технический результат изобретения заключается в обеспечении доверенной загрузки аппаратной платформы; создании защищенной среды функционирования для виртуальной машины; эмуляции аппаратных устройств компьютерной системы; эмуляции микропрограммного кода, необходимого для функционирования виртуальной машины; запрете предоставления виртуальным машинам информации о реальном составе аппаратных ресурсов компьютерной системы; запрете предоставления прямого доступа виртуальной машины к аппаратным устройствам компьютерной системы; запрете соответствия эмулируемых аппаратных устройств аппаратным устройствам компьютерной системы; управлении доступом субъектов доступа к объектам доступа; управлении доступом субъектов доступа к памяти, участвующей в обработке и хранении информации; управлении аппаратной конфигурацией компьютерной системы; управлении информационными потоками между виртуальными машинами при сетевом взаимодействии посредством межсетевого экрана; применении обратимого преобразования информации для соблюдения конфиденциальности; защите хранения исполняемого кода, данных системы защиты информации и параметров микропрограммного кода аппаратной платформы.

041757 B1

041757 B1

Данное изобретение относится к области компьютерной безопасности, в частности используется при создании защищенных компьютерных систем, предназначенных для передачи, обработки и хранения конфиденциальной информации, и в том числе используемых в составе защищенных локальных сетей предприятий и организаций.

В качестве компьютерной системы могут выступать однопользовательские и многопользовательские средства вычислительной техники (далее СВТ), автоматизированные рабочие места (далее АРМ), сетевые маршрутизаторы и т.д.

Под аппаратной платформой компьютерной системы понимается совокупность встроенного микропрограммного обеспечения на базе центральных процессоров (например, Intel, AMD, ARM и т.п.) и серийно выпускаемых аппаратных компонентов, определяющая архитектуру компьютерной системы.

Способ защиты компьютерной системы от несанкционированного доступа (далее НСД) к информации, реализуемый на уровне аппаратной платформы, применим к компьютерным системам независимо от устанавливаемых в них операционных систем.

Граничные условия применения способа защиты компьютерной системы от НСД к информации, реализуемой на уровне аппаратной платформы, определяются только наличием поддержки технологии виртуализации в аппаратных устройствах, входящих в состав компьютерной системы (например, определяющих архитектуру x86/x64 и т.д.).

Устройство для осуществления способа защиты компьютерной системы от НСД к информации, реализуемое на уровне аппаратной платформы компьютерной системы, предусматривает только проводное подключение периферийных устройств. Например, периферийных устройств с использованием интерфейсов USB, VGA и т.д.

Из уровня техники известен способ доверенной загрузки в виртуализированных средах RU 2581552 C2 (МПК G06F 21/31, G06F 21/41, G06F 21/64. заявка №2014136615/08, 10.09.2014; опубликовано 20.04.2016 в Бюл. № 11), включающий в себя создание раздела на жестком диске виртуализированной среды с загрузчиком, обеспечивающим доверенную загрузку виртуальных машин, добавление модуля микропрограммы доверенной загрузки в виртуальный BIOS, осуществление запуска виртуальной машины, осуществление конфигурации загрузчика. С последующим перезапуском виртуальной машины, проведением аутентификации пользователя виртуальной машины, проведением контроля целостности файлов виртуальной машины. Минусом данного способа является то, что он предназначен для виртуальных машин, а не для физических СВТ. Любая виртуальная машина без доверенной загрузки СВТ может быть скомпроментрирована. Компоненты, запускаемые до начала работы виртуальных сред (например, гипервизор первого типа, контролирующий работу виртуальных машин, загрузчик виртуальной среды и т.д.), располагаются в не защищенной среде (незащищенный жесткий диск, реальный BIOS и т.д.), соответственно могут быть скомпрометированы.

Предлагаемое техническое решение предусматривает расположение компонентов системы защиты в аппаратном устройстве, в том числе в защищенном исполнении, обеспечивает доверенную загрузку как СВТ, так и виртуальных сред и соответственно не может быть скомпрометировано.

Целью предлагаемого технического решения является повышение безопасности компьютера, а именно

предотвращение создания в компьютерной системе скрытых каналов несанкционированной передачи защищаемой информации со стороны аппаратных устройств и микропрограммного обеспечения, встроенного в устройства аппаратной платформы компьютерной системы;

изоляция данных управления и программного обеспечения компьютерной системы от аппаратных устройств (шин и устройств) и микропрограммного обеспечения, встроенного в устройства аппаратной платформы компьютерной системы;

управление информационными потоками между виртуальными машинами и физическими аппаратными устройствами (шины и устройства) компьютерной системы.

Технический результат предлагаемого изобретения заключается в

обеспечении доверенной загрузки аппаратной платформы;

создании защищенной среды функционирования для виртуальной машины;

эмуляции аппаратных устройств компьютерной системы, включая вычислительные ресурсы компьютерной системы;

эмуляции микропрограммного кода (в частности, базовой системы ввода-вывода и т.д.), необходимого для функционирования виртуальной машины;

запрете предоставления виртуальным машинам информации о реальном составе аппаратных ресурсов компьютерной системы;

запрете предоставления прямого доступа виртуальной машины к аппаратным устройствам компьютерной системы, кроме устройств, сертифицированных по требованиям защиты информации государственными органами страны для применения в компьютерной системе;

запрете соответствия эмулируемых аппаратных устройств аппаратным устройствам компьютерной системы с целью обеспечения невозможности эксплуатации уязвимостей устройств аппаратной платформы для любого программного обеспечения, выполняющегося внутри виртуальной машины;

управлении доступом субъектов доступа к объектам доступа (виртуальных машин к аппаратным устройствам компьютерной системы и аппаратных устройств компьютерной системы к вычислительным ресурсам компьютерной системы, связанным с функционированием виртуальной машины);

управлении доступом субъектов доступа к памяти, участвующей в обработке информации (в частности, оперативной памяти);

управлении доступом субъектов доступа к памяти, участвующей в хранении информации (в частности, разграничении доступа к носителям информации, в том числе к разделам носителей информации);

управлении аппаратной конфигурацией компьютерной системы с целью контроля неизменности аппаратной конфигурации;

управлении информационными потоками между виртуальными машинами при сетевом взаимодействии посредством межсетевого экрана;

применении обратимого преобразования информации для соблюдения конфиденциальности;

защите хранения исполняемого кода и данных системы защиты информации (далее СЗИ);

защите хранения параметров микропрограммного кода аппаратной платформы (в частности, базовой системы ввода-вывода).

Заявленный технический результат достигается

предварительной подготовкой аппаратной платформы, состоящей из

нейтрализации устройств аппаратной платформы компьютерной системы, не участвующих в обработке, хранении и передаче информации или представляющих угрозу безопасности информации,

устранения избыточности исполняемого кода микропрограммного кода аппаратной платформы,

устранения избыточности исполняемого кода привилегированных режимов функционирования аппаратной платформы компьютерной системы и его защита от модификации;

обеспечением доверенной загрузки аппаратной платформы компьютерной системы;

обеспечением доверенной загрузки системы защиты информации;

обеспечением защиты микропрограммного кода аппаратной платформы от анализа;

обеспечением защиты исполняемого кода системы защиты информации от анализа;

запретом обновления микропрограммного кода аппаратной платформы, в том числе удаленного;

очисткой областей памяти, содержащих данные системы защиты информации и виртуальных машин в устройствах хранения, перед их выделением или повторном использовании;

очисткой областей оперативной памяти аппаратной платформы компьютерной системы перед их выделением или повторным использованием;

реализацией особенностей архитектуры СЗИ;

изоляцией виртуальных машин;

реализацией особенностей передачи информации между виртуальными машинами в компьютерной системе;

эмуляцией аппаратных устройств компьютерной системы;

самотестированием механизмов защиты системы защиты информации;

восстановлением безопасного состояния компьютерной системы;

определением субъектов и объектов доступа на уровне аппаратной платформы;

обработкой системой защиты информации запросов виртуальной машины на доступ к физическим аппаратным устройствам компьютерной системы в следующем порядке:

виртуальная машина осуществляет запрос на доступ к физическим аппаратным устройствам на основе предоставляемых виртуальных ресурсов,

система защиты информации осуществляет сбор данных или параметров, содержащихся в запросе виртуальной машины,

система защиты информации на основании собранных данных или параметров и в соответствии с правилами разграничения доступа субъектов доступа к объектам доступа осуществляет проверку правомочности запроса,

при положительном результате проверки система защиты информации преобразует данные или параметры виртуальных вычислительных ресурсов в данные или параметры физических вычислительных ресурсов и передает преобразованный запрос соответствующему физическому аппаратному устройству, а при отрицательном результате проверки запрос отклоняется;

обработкой системой защиты информации запросов от физических аппаратных устройств компьютерной системы на доступ к виртуальной машине в следующем порядке:

физические аппаратные устройства компьютерной системы осуществляют запрос на доступ к виртуальным вычислительным ресурсам на основе параметров физических вычислительных ресурсов,

система защиты информации осуществляет сбор данных или параметров, в запросах от физических аппаратных устройств, система защиты информации на основании собранных данных и в соответствии с правилами распределения доступа субъектов доступа к объектам доступа осуществляет проверку правомочности запроса,

при положительном результате проверки система защиты информации преобразует данные или параметры физических вычислительных ресурсов компьютерной системы в данных или параметров вирту-

альных вычислительных ресурсов и передает преобразованный запрос от физического аппаратного устройства компьютерной системы виртуальной машине, а при отрицательном результате проверки запрос отклоняется;

управлением конфигурацией аппаратных средств компьютерной системы при запуске компьютерной системы, реализующим

определение системой защиты информации фактического состава всех аппаратных устройств, а также параметров их функционирования,

первичную проверку соответствия фактического состава всех аппаратных устройств компьютерной системы, включая периферийные устройства, списку аппаратных устройств, разрешенных системой защиты информации для использования в составе компьютерной системы, а также соответствия параметров выявленных в компьютерной системе физических аппаратных устройств, разрешенным параметрам, установленным системой защиты информации для данного состава аппаратных устройств,

установление для каждой роли, предусматриваемой системой защиты информации, списка разрешенных для использования в рамках данной роли физических аппаратных устройств,

блокирование компьютерной системы при выявлении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных системой защиты информации к использованию в составе компьютерной системы для ролей пользователей и администраторов,

блокирование компьютерной системы при несоответствии параметров выявленных физических аппаратных устройств разрешенным параметрам, установленным системой защиты информации для данного состава аппаратных устройств компьютерной системы для ролей пользователей и администраторов;

управлением конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы, обеспечивающим эшелонированную защиту от несанкционированного изменения конфигурации аппаратных средств компьютерной системы, от создания скрытых каналов несанкционированного доступа, как к вычислительным ресурсам компьютерной системы, так и к программной среде виртуальной машины и к пользовательским обрабатываемым данным, подлежащим защите от НСД к информации, и основанным на

периодической проверке состава аппаратных средств компьютерной системы и параметров их функционирования,

непрерывном анализе запросов от физических аппаратных устройств компьютерной системы на доступ к вычислительным ресурсам компьютерной системы (в том числе связанным с функционированием виртуальной машины);

управлением конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в режиме обслуживания, реализующим

осуществление непрерывного контроля системой защиты информации параметров функционирования всех аппаратных устройств компьютерной системы, а также проверку соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защиты информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

возможность изменения списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы и списка аппаратных устройств, разрешенных для каждой роли, предусматриваемой системой защиты информации;

управлением конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в режиме аудита, реализующим

осуществление системой защиты информации непрерывного контроля параметров функционирования всех аппаратных устройств компьютерной системы, а также проверку соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защиты информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

отключение аппаратных устройств и блокирование работы компьютерной системы при подключении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

блокирование работы компьютерной системы со стороны системы защиты информации при изменении параметров функционирования аппаратных устройств;

управлением конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в эксплуатационном режиме, реализующим

осуществление системой защиты информации непрерывного контроля параметров функционирова-

ния всех аппаратных устройств компьютерной системы, а также проверку соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защипы информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

отключение аппаратных устройств и блокирование работы компьютерной системы при подключении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

блокирование работы компьютерной системы со стороны системы защиты информации при изменении параметров функционирования аппаратных устройств;

предоставлением доступа пользователям к ресурсам компьютерной системы или к виртуальным машинам только через роли с уникальными идентификаторами, присваиваемыми по результатам идентификации и аутентификации пользователя;

однозначным запретом на запрос доступа любого не идентифицированного субъекта доступа к любым объектам доступа,

запретом на любые запросы на прямой доступ между физическими аппаратными устройствами или шинами компьютерной системы, кроме устройств, сертифицированных по требованиям защиты информации государственными органами страны применения компьютерной системы, и виртуальными машинами;

конфигурированием защиты оперативной памяти с помощью системы защиты информации от прямого доступа со стороны аппаратных устройств компьютерной системы, а именно

получением из аппаратного устройства системой защиты информации списка и параметров разрешенных устройств компьютерной системы,

формированием системой защиты информации списка разрешенных к использованию в составе компьютерной системы устройств с возможностью прямого доступа к памяти,

получением системой защиты информации параметров прямого доступа к памяти от устройств, разрешенных к использованию в составе компьютерной системы,

конфигурированием системой защиты информации защиты с помощью полученных параметров прямого доступа к оперативной памяти от устройств, разрешенных к использованию в составе компьютерной системы;

защитой оперативной памяти компьютерной системы от прямого доступа со стороны аппаратных устройств компьютерной системы, обеспечиваемая системой защиты информации и включающей:

генерацию запросов прямого доступа к оперативной памяти от физических аппаратных устройств компьютерной системы;

сбор системой защиты информации данных или параметров, содержащихся в запросах прямого доступа к оперативной памяти от аппаратных устройств;

осуществление проверки системой защиты информации собранных параметров запроса в соответствие с матрицей доступа при соответствии параметров, содержащихся в запросе, параметрам прямого доступа к памяти от устройств, разрешенных к использованию в составе компьютерной системы,

выполнение разрешения запроса, в противном случае осуществление блокировки запроса,

регистрацию системой защиты информации события блокировки запроса в журнале регистрации событий;

разграничением доступа к внешним носителям информации или от внешних носителей информации, включающее

разрешение взаимодействия с внешним накопителем информации только одной виртуальной машине, при этом внешний накопитель информации становится недоступен для взаимодействия с другими виртуальными машинами,

последовательное использование внешнего накопителя информации виртуальными машинами при обмене информацией между виртуальными машинами,

обеспечение доступа нескольких виртуальных машин к совместно используемому накопителю информации в режиме только чтение;

осуществлением системой защиты информации фильтрации сетевого трафика по каждому протоколу сетевого взаимодействия в соответствии с матрицами доступа как при запросах, исходящих от виртуальной машины, так и при запросах, исходящих от физической сетевой карты, с учетом проверки типа запроса, поступившего от виртуальной машины, на его соответствие правилам разграничения доступа, установленным для уровней модели OSI или для соответствующих им протоколов, а также с учетом проверки данных, содержащихся в запросе виртуальной машины, на их соответствие атрибутам доступа, установленным системой защиты информации, осуществлением системой защиты информации регистрации событий во всех режимах работы, для каждого регистрируемого события в журнале регистрации событий сохраняется следующая информация о дате и времени события, субъекте доступа, вызывавшем регистрируемое событие, типе события (при регистрации события, связанного с доступом, также сохра-

няется информация об объекте и типе доступа), успешности осуществления события.

Устройство, реализующее предлагаемый способ, включает систему защиты информации, содержащую контроллер, память, в том числе в защищенном исполнении, подключенные к компьютерной шине, гипервизор первого типа с подсистемой запуска, подсистемой разграничения доступа, подсистемой администрирования и подсистемой регистрации событий, реализуемые на базе одного или нескольких центральных процессоров, а также чипсет, память, компьютерные шины, накопитель на жестком магнитном диске, твердотельный накопитель, USB-флэш накопитель, клавиатуру, мышь, CD/DVD/Blu-ray оптический диск, сетевую карту, видеокарту, монитор, принтер, сканер, многофункциональное устройство.

В качестве компьютерных шин могут быть использованы PCI, PCIExpress, SMBus, USB, ATA, SATA, PS/2, SCSI, SAS, Fibre Channel, InfiniBand, I2C, SPI, FireWire, DMI, HyperTransport, Thunderbolt.

Пример реализации предлагаемого способа и устройства

Рассмотрим поэтапно предварительную подготовку аппаратной платформы.

а) Отключение (нейтрализация) устройств аппаратной платформы компьютерной системы, не участвующих в обработке, хранении и передаче информации или представляющих угрозу безопасности информации.

Отключение (нейтрализация) устройств аппаратной платформы компьютерной системы, не участвующих в обработке, хранении и передаче информации или представляющих угрозу безопасности информации включает реализацию следующих мер.

Физическое отключение в аппаратной платформе компьютерной системы, по возможности, электропитания хост-контроллеров шин, не участвующих в обработке и передаче информации или представляющих угрозу безопасности информации. При отсутствии возможности физического отключения электропитания хост-контроллеров шин, должна быть произведена нейтрализация их работы путем блокировки неиспользуемых аппаратных интерфейсов (портов, разъемов, слотов).

Физическое отключение в аппаратной платформе компьютерной системы по возможности электропитания устройств, не участвующих в обработке, хранении и передаче информации или представляющих угрозу безопасности информации:

устройств, использующих беспроводные каналы связи (например, WiFi, 3G, Bluetooth, NFC и т.д.);

устройств, позволяющих отслеживать действия пользователя (например, веб-камера, микрофон, модули позиционирования, сенсоры и т.д.);

устройств удаленного управления аппаратной платформой компьютерной системы;

устройств управления электропитанием аппаратной платформы компьютерной системы.

При отсутствии возможности отключения электропитания указанных устройств произведена их нейтрализация путем удаления встроенного в них микропрограммного кода, создающего угрозы безопасности информации.

Если часть встроенного микропрограммного кода не создает угрозы безопасности информации в аппаратной платформе компьютерной системы и не может быть удалена без прекращения функционирования соответствующего устройства, представлено убедительное доказательство невозможности возникновения угроз безопасности информации в аппаратной платформе компьютерной системы при использовании указанного кода.

В аппаратной платформе компьютерной системы блокированы неиспользуемые аппаратные интерфейсы (порты) следующих устройств: видеоадаптера, проводного сетевого адаптера, аудио-контроллера, устройств (плат) расширения и т.д.

б) Устранение избыточности микропрограммного кода, размещенного в коммерческих аппаратных платформах.

Из состава микропрограммного кода аппаратной платформы компьютерной системы удален избыточный исполняемый код для различных стадий инициализации/работы микропрограммного кода.

Например, в базовой системе ввода-вывода удалены

компоненты, реализующие драйверы сетевых карт и стек сетевых протоколов;

компоненты, реализующие стандартные файловые системы (FAT, NTFS, exFAT и т.д.);

компоненты, реализующие программное обеспечение Computrace;

компоненты поддержки Intel Management Engine;

компоненты, реализующие EFI-оболочки (Shell), из-под которых можно запускать различные EFI-приложения;

компоненты, реализующие EFI-приложения;

и т.д.

в) Устранение избыточности исполняемого кода привилегированных режимов функционирования аппаратной платформы компьютерной системы и его защита от модификации.

Из состава исполняемого кода привилегированных режимов функционирования аппаратной платформы компьютерной системы удален исполняемый код компонентов обновления микропрограммного кода аппаратной платформы компьютерной системы (например, UEFI BIOS в режиме SMM).

Рассмотрим обеспечение доверенной загрузки аппаратной платформы компьютерной системы.

СЗИ обеспечивает доверенную загрузку аппаратной платформы компьютерной системы с последо-

вательным подтверждением целостности микропрограммных компонентов аппаратной платформы компьютерной системы, участвующих в цепочке доверенной загрузки.

При этом передача функций управления следующему микропрограммному компоненту аппаратной платформы компьютерной системы, участвующему в цепочке доверенной загрузки, производится от предыдущего микропрограммного компонента аппаратной платформы компьютерной системы только при подтверждении целостности этого компонента.

При отсутствии подтверждения целостности любого из микропрограммных компонентов аппаратной платформы компьютерной системы, участвующих в цепочке доверенной загрузки, дальнейшая загрузка компьютерной системы запрещается.

Перед началом доверенной загрузки СЗИ обеспечивает проверку аутентичности микропрограммного кода аппаратной платформы компьютерной системы (например, базовой системы ввода-вывода) используемого при доверенной загрузке.

Микропрограммный код аппаратной платформы компьютерной системы (например, базовая система ввода-вывода), используемый при доверенной загрузке компьютерной системы, защищен от несанкционированной модификации путем реализации следующих мер:

удаления из состава микропрограммного кода компонентов обновления микропрограммного кода, в том числе в привилегированных режимах функционирования аппаратной платформы,

обеспечения неизменности микропрограммного кода аппаратной платформы компьютерной системы (например, полной блокировки изменения содержимого флэш-памяти средствами микросхемы флэш-памяти).

Микропрограммный код аппаратной платформы компьютерной системы передает управление только микропрограммному обеспечению СЗИ.

При попытке загрузки нештатного программного обеспечения СЗИ блокирует загрузку аппаратной платформы компьютерной системы.

Микропрограммный код аппаратной платформы исключает возможность использования программным обеспечением компьютерной системы режимов энергопотребления аппаратной платформы, нарушающих цепочку доверенной загрузки.

Рассмотрим обеспечение доверенной загрузки СЗИ.

Доверенная загрузка СЗИ обеспечивается путем построения цепочки доверенной загрузки, при которой каждый компонент СЗИ, участвующий в цепочке доверенной загрузки СЗИ, по завершению своей инициализации подтверждает целостность следующего компонента перед передачей ему управления.

При отсутствии подтверждения целостности какого - либо компонента СЗИ, участвующего в цепочке доверенной загрузки, дальнейшая загрузка СЗИ и функционирование компьютерной системы прекращаются.

Рассмотрим обеспечение защиты микропрограммного кода аппаратной платформы и исполняемого кода СЗИ от анализа.

Защита микропрограммного кода аппаратной платформы от анализа обеспечивается специальными методами. Например, защита UEFI BIOS от анализа обеспечивается путем

обфускации программного кода,

обезличивания стадии инициализации,

обезличивания хранилища компонентов,

обезличивания формата представления компонентов в составе UEFI BIOS,

и т.д.

Обеспечение защиты исполняемого кода СЗИ от анализа осуществляется путем обфускации исполняемого кода СЗИ.

Рассмотрим обеспечение запрета обновления микропрограммного кода аппаратной платформы, в том числе удаленного.

В аппаратной платформе компьютерной системы реализованы следующие меры по запрету обновления микропрограммного кода, используемого при доверенной загрузке аппаратной платформы компьютерной системы, в том числе удаленного:

из состава микропрограммного кода удалены компоненты обновления микропрограммного кода, в том числе в привилегированных режимах функционирования аппаратной платформы (например, компонентов обновления UEFI BIOS в том числе в режиме SMM),

обеспечена неизменность микропрограммного кода аппаратной платформы компьютерной системы (например, полной блокировкой изменения содержимого флэш-памяти средствами микросхемы флэш-памяти).

Восстановление микропрограммного кода аппаратной платформы, в том числе при сбоях аппаратной платформы компьютерной системы, обеспечивается только в рамках процедур восстановления безопасного состояния аппаратной платформы компьютерной системы.

Рассмотрим реализацию особенностей архитектуры СЗИ.

В компьютерной системе с помощью СЗИ обеспечивается создание защищенной среды функционирования виртуальной машины как совокупности изолированной среды выполнения виртуальной ма-

шины и эмулированных аппаратных ресурсов путем

изоляции исполняемого кода СЗИ, от программного обеспечения компьютерной системы путем установки для него более высоких полномочий (системных привилегий),

установления запрета поддержки файловых систем используемых в компьютерной системе операционных систем со стороны исполняемого кода СЗИ,

энергонезависимого хранения и поддержки аппаратным устройством СЗИ контроля целостности с использованием контрольных сумм/хешей/криптографических значений, хранящихся в аппаратной устройстве СЗИ:

параметров микропрограммного кода аппаратной платформы (например, базовой системы ввода - вывода),

ПРД, связанных с ролями пользователей,

исполняемого кода СЗИ,

контрольных сумм/хэшей/криптографических значений,

списка состава аппаратных ресурсов компьютерной системы, используемого для контроля аппаратной конфигурации, журналов регистрации событий.

Рассмотрим обеспечение очистки областей памяти, содержащих данные СЗИ и виртуальных машин в устройствах хранения, перед их выделением/повторным использованием.

Перед выделением/повторным использованием областей памяти в устройствах хранения, содержащих данные СЗИ и виртуальных машин, СЗИ обеспечивает очистку этих областей, например путем заполнения их случайными значениями или "нулями".

Рассмотрим обеспечение очистки областей оперативной памяти аппаратной платформы компьютерной системы перед их выделением/повторным использованием.

Перед выделением/повторным использованием областей оперативной памяти аппаратной платформы компьютерной системы для СЗИ и виртуальных машин, СЗИ обеспечивает очистку этих областей, например путем их заполнения случайными значениями или "нулями".

Рассмотрим обеспечение изоляции виртуальных машин.

Виртуальным машинам выделяется уникальный набор ресурсов. СЗИ обеспечивает выделение следующих квот для использования их виртуальными машинами:

квот вычислительных ресурсов компьютерной системы (количество ядер центрального процессора, модель процессора и т.д.),

квот на использование ресурсов памяти,

квот на использование ресурсов хранения данных (устройства хранения данных/разделы устройств хранения данных).

Рассмотрим реализацию особенностей передачи информации между виртуальными машинами в компьютерной системе.

Передача информации между виртуальными машинами осуществляется в эксплуатационном режиме работы СЗИ только через виртуальные устройства (виртуальные сетевые адаптеры, виртуальные съемные носители информации и т.п.). Любые другие операции, приводящие к прямой передаче информации между виртуальными машинами запрещены.

Рассмотрим эмуляцию аппаратных устройств компьютерной системы.

СЗИ обеспечивает программную эмуляцию аппаратных ресурсов компьютерной системы. Пример состава вычислительных ресурсов компьютерной системы (с учетом виртуальных вычислительных ресурсов, создаваемых СЗИ) и параметры, характеризующие каждый вычислительный ресурс компьютерной системы, приведен в табл. 1.

СЗИ обеспечивает программную эмуляцию используемого микропрограммного кода (например, базовой системы ввода-вывода).

При эмуляции накопителя информации (например, НЖМД и т.д.) в СЗИ существует возможность обеспечения программной обфускации сохраняемых данных с целью существенного затруднения их анализа.

Рассмотрим регистрацию событий в компьютерной системе.

СЗИ работы обеспечивает регистрацию следующих событий:

событий запуска, функционирования и остановки работы гипервизора и виртуальных машин:

событий запуска и остановки работы гипервизора,

событий запуска и остановки работы виртуальных машин;

событий аутентификации пользователей;

событий, связанных с микропрограммным кодом аппаратной платформы (например, базовой системы ввода-вывода):

событий проверки аутентичности микропрограммного кода аппаратной платформы (например, базовой системы ввода-вывода), используемого при доверенной загрузке,

событий, связанных с передачей управления от микропрограммного кода аппаратной платформы (например, базовой системы ввода-вывода) программному обеспечению, размещенному на соответствующих устройствах хранения данных;

событий, связанных с изменением состава и параметров функционирования аппаратных устройств компьютерной системы;

событий, связанных с изменением состава аппаратных устройств компьютерной системы,

событий, связанных с изменением параметров функционирования аппаратных устройств компьютерной системы;

событий, связанных с нарушениями целостности:

событий, связанных с нарушениями целостности микропрограммных компонентов аппаратной платформы компьютерной системы, участвующих в цепочке доверенной загрузки,

событий, связанных с нарушением целостности исполняемых кодов и данных управления СЗИ, как во время запуска СЗИ, так и в процессе его функционирования,

событий, связанных с действиями, осуществляемыми механизмом автоматического восстановления безопасного состояния аппаратной платформы компьютерной системы;

событий, связанных с попытками нарушения правил разграничения доступа:

событий, связанных с неудачными попытками идентификации и аутентификации пользователя,

событий, связанных с несанкционированным запуском средств конфигурирования СЗИ,

событий, связанных с попытками доступа к аппаратным ресурсам компьютерной системы;

событий, связанных с несанкционированным изменением установленных квот:

событий, связанных с несанкционированным превышением установленных квот вычислительных ресурсов компьютерной системы для виртуальных машин,

событий, связанных с несанкционированным превышением установленных квот ресурсов памяти для виртуальных машин,

событий, связанных с несанкционированным превышением установленных квот по использованию ресурсов хранения данных виртуальными машинами.

Для каждого регистрируемого события в журнале регистрации событий сохраняется следующая информация:

дата и время события,

субъект доступа, вызывающий регистрируемое событие,

тип события (при регистрации события, связанного с доступом, также сохраняется информация об объекте и типе доступа),

успешность осуществления события.

Рассмотрим восстановление безопасного состояния компьютерной системы.

СЗИ обеспечивает восстановление безопасного состояния с осуществлением следующих операций и процедур:

операции остановки выполнения виртуальных машин до восстановления безопасного состояния компьютерной системы;

операции перевода СЗИ в режим обслуживания;

процедур регистрации в журнале событий сведений о нарушении безопасного состояния компьютерной системы, а также действий СЗИ.

СЗИ поддерживает режим обслуживания, в котором выполнение каких-либо действий разрешено только пользователю категории "Администратор защиты", который может выполнять

выявление причин нарушения безопасного состояния аппаратной платформы компьютерной системы;

анализ причин перехода СЗИ в режим обслуживания;

восстановление безопасного состояния аппаратной платформы компьютерной системы в соответствии с процедурами, приведенными в эксплуатационной документации.

Рассмотрим самотестирование механизмов защиты СЗИ.

Для поддержки безопасного состояния компьютерной системы СЗИ выполняет набор процедур самотестирования

в процессе загрузки СЗИ;

периодически в процессе функционирования СЗИ;

в процессе изменения данных управления СЗИ в режиме обслуживания.

Во время самотестирования механизмов защиты СЗИ обеспечивается проверка целостности данных управления и исполняемого кода СЗИ.

В способе защиты компьютерной системы от несанкционированного доступа к информации, реализуемой на уровне аппаратной платформы, в качестве субъектов доступа рассматриваются

виртуальные машины, как особые процессы, создаваемые СЗИ для реализации изолированной виртуальной вычислительной системы, в которой функционирует общесистемное и прикладное программное обеспечение (ПО);

физические аппаратные устройства (шины и устройства) компьютерной системы.

В качестве объектов доступа, подлежащих защите от НСД к информации, реализуемой на уровне аппаратной платформы, рассматриваются

виртуальные машины;

физические аппаратные устройства (шины и устройства) компьютерной системы.

В защищенной компьютерной системе используется аппаратная платформа, в которой предусмотрены

устранение функциональной избыточности нереконфигурируемых устройств аппаратной платформы и функциональной избыточности микропрограммного кода реконфигурируемых устройств аппаратной платформы, участвующих (в том числе и косвенно) в процессе обработки информации;

отключение или нейтрализация устройств, входящих в состав системной (материнской) платы и не участвующих в процессе обработки информации или представляющих угрозу безопасности информации;

устранение функциональной избыточности микропрограммного кода, размещенного в аппаратных платформах (микропрограммного кода базовой системы ввода-вывода, микропрограммного кода чипсета и т.п.);

защита микропрограммного кода (базовой системы ввода-вывода и т.п.) от анализа;

неизменность модифицированного или удаленного микропрограммного кода (микропрограммного кода базовой системы ввода-вывода, микропрограммного кода чипсета и т.п.).

Для защиты компьютерной системы от НСД к информации на уровне аппаратной платформы применяется аппаратно-микропрограммное СЗИ, которое является неотъемлемой частью аппаратной платформы.

Аппаратная часть СЗИ представлена устройством, в том числе в защищенном исполнении, обеспечивающим энергонезависимое хранение

параметров микропрограммного кода аппаратной платформы (например, базовой системы ввода-вывода);

правил разграничения доступа (далее ПРД);

исполняемого кода СЗИ;

контрольных сумм/хэшей/значений обратимого преобразования информации;

данных управления, используемых СЗИ для реализации управления и функций безопасности компьютерной системы;

журналов регистрации событий.

Микропрограммная часть СЗИ может иметь как монолитную, так и модульную архитектуру и состоит из нескольких подсистем.

На фиг. 1 приведена упрощенная базовая схема функционирования встроенного в типовую архитектуру аппаратной платформы СЗИ, обеспечивающего защиту компьютерной системы от НСД к информации, в которой 1 - виртуальная машина, 2 - СЗИ, 3 - аппаратное обеспечение компьютерной системы, т.е. физические аппаратные устройства (устройства/шины). На фиг. 1 приведена только одна виртуальная машина, однако виртуальных машин может быть несколько.

В соответствии со схемой, приведенной на фиг. 1, общесистемное и прикладное ПО компьютерной системы устанавливается и функционирует на уровне виртуальной машины 1.

Основой СЗИ 2 является гипервизор 1-го типа, использующий аппаратные средства виртуализации оперативной памяти и системы команд микропрограммного обеспечения, функционирующего на уровне аппаратной виртуализации, предоставляемом центральным процессором компьютерной системы.

СЗИ предоставляет виртуальной машине интерфейсы взаимодействия только с виртуальными вычислительными ресурсами, созданными СЗИ. При этом виртуальная машина воспринимает виртуальные вычислительные ресурсы, созданные СЗИ, как физические вычислительные ресурсы компьютерной системы. Специализированных интерфейсов взаимодействия с другими подсистемами СЗИ, в том числе с гипервизором 1-го типа, виртуальная машина не имеет.

На фиг. 2 представлена упрощенная архитектура СЗИ, представляющая собой совокупность основных подсистем, а также взаимосвязи между подсистемами, где 4 - подсистема запуска СЗИ (включает в себя поддержку аппаратного устройства СЗИ), 5 - подсистема разграничения доступа, 6 - подсистема администрирования (работы с пользователем), 7 -подсистема регистрации событий (журнал регистрации событий).

Подсистема запуска СЗИ предоставляет следующие основные функции:

поддержку аппаратного устройства СЗИ в составе микропрограммного кода аппаратной платформы (например, базовой системы ввода-вывода);

доверенную загрузку;

контроль целостности микропрограммного кода аппаратной платформы;

хранение параметров микропрограммного кода аппаратной платформы.

Подсистема разграничения доступа предоставляет следующие основные функции:

управление памятью (выделение, освобождение и отображение физической памяти в адресное пространство виртуальной машины);

управление приоритетом выполнения исполняемого кода;

управление программными интерфейсами СЗИ;

управление временем и таймером;

аутентификацию пользователя;

управление режимами работы СЗИ;

контроль состава аппаратных средств компьютерной системы;

защиту оперативной памяти от аппаратных средств компьютерной системы;

самотестирование механизмов защиты СЗИ;

контроль и разграничение доступа между виртуальными устройствами и аппаратными средствами компьютерной системы;

управление носителями информации;

преобразование данных носителей информации;

фильтрация сетевого трафика;

поддержку виртуальных устройств и аппаратных средств компьютерной системы;

гипервизор.

Подсистема администрирования (работы с пользователем) предоставляет следующие основные функции:

установку параметров работы СЗИ, а также виртуальной машины;

работу (например, просмотр) с журналом регистрации событий.

Подсистема регистрации событий (журнал регистрации событий) предоставляет основную функцию ведения журнала регистрации событий.

Базовая схема функционирования СЗИ, встроенного в типовую архитектуру аппаратной платформы и обеспечивающего защиту компьютерной системы от НСД к информации, основана

на обработке запросов от виртуальной машины на доступ к физическим аппаратным устройствам (шинам и устройствам);

на обработке запросов от физических аппаратных устройств, включая устройства аппаратной платформы (шины и устройства), на доступ к виртуальной машине.

СЗИ обеспечивает обработку запросов виртуальной машины на доступ к физическим аппаратным устройствам компьютерной системы в следующем порядке.

1. Виртуальная машина осуществляет запрос на доступ к физическим аппаратным устройствам на основе предоставляемых виртуальных ресурсов.

2. СЗИ осуществляет сбор (перехват) данных/параметров, содержащихся в запросе виртуальной машины.

3. СЗИ на основании собранных (перехваченных) данных/параметров и в соответствии с ПРД субъектов доступа к объектам доступа осуществляет проверку правомочности запроса.

4. При положительном результате проверки СЗИ преобразует данные/параметры виртуальных вычислительных ресурсов в данные/параметры физических вычислительных ресурсов и передает преобразованный запрос соответствующему физическому аппаратному устройству.

5. При отрицательном результате проверки запрос отклоняется.

В этом случае надо понимать, что правила разграничения доступа (ПРД) учитывают\включают проверку

идентификационных данных виртуальной машины, содержащихся в запросе, с данными СЗИ, а также типа виртуального ресурса и типа запроса, осуществленного виртуальной машиной;

соответствия данных/параметров, содержащихся в запросе виртуальной машины, спецификации (например, СЗИ обеспечивает строгое выполнение устройствами инструкций, определенных спецификациями на данные устройства, путем контроля списков разрешенных инструкций и отклонения любых инструкций не соответствующих списку разрешенных инструкций);

дополнительных ПРД субъектов доступа к объектам доступа (например, при доступе к накопителям информации, разделам накопителей информации, сетевой карте);

и т.д.

СЗИ обеспечивает обработку запросов от физических аппаратных устройств компьютерной системы на доступ к виртуальной машине в следующем порядке.

1. Физические аппаратные устройства (шины и устройства) компьютерной системы осуществляют запрос на доступ к виртуальным вычислительным ресурсам на основе параметров физических вычислительных ресурсов.

2. СЗИ осуществляет сбор (перехват) данных/параметров, в запросах от физических аппаратных устройств.

3. СЗИ на основании собранных (перехваченных) данных/параметров и в соответствии с ПРД субъектов доступа к объектам доступа осуществляет проверку правомочности запроса.

4. При положительном результате проверки СЗИ преобразует данные/параметры физических вычислительных ресурсов компьютерной системы в данные/параметры виртуальных вычислительных ресурсов и передает преобразованный запрос от физического аппаратного устройства компьютерной системы виртуальной машине.

5. При отрицательном результате проверки запрос отклоняется. В этом случае надо понимать, что ПРД учитывают/включают проверку

идентификационных данных физического аппаратного устройства компьютерной системы и/или определение типа аппаратного устройства и типа запроса;

данных/параметров, содержащихся в запросе от физических аппаратных устройств компьютерной

системы, на их соответствие спецификации (например, СЗИ обеспечивает строгое выполнение устройствами аппаратной платформы инструкций, определенных спецификациями на данные устройства, посредством контроля списков разрешенных инструкций и отклонения любых инструкций не соответствующих списку разрешенных инструкций);

дополнительных ПРД субъектов доступа к объектам доступа (например, при доступе к накопителям информации, разделам накопителей информации, сетевой карте);

и т.д.

Способ защиты компьютерной системы от НСД к информации, реализуемый на уровне аппаратной платформы, предусматривает выполнение следующих функций:

управление конфигурацией аппаратных средств компьютерной системы;

управление доступом;

управление информационными потоками.

Рассмотрим управление конфигурацией аппаратных средств.

СЗИ обеспечивает управление конфигурацией аппаратных средств, при запуске компьютерной системы и в режимах функционирования компьютерной системы, устанавливаемых СЗИ, в том числе

при запуске компьютерной системы:

определение фактического состава всех аппаратных устройств, а также параметров их функционирования;

первичная проверка соответствия фактического состава всех аппаратных устройств компьютерной системы, включая периферийные устройства, списку аппаратных устройств, разрешенных СЗИ для использования в составе компьютерной системы, а также соответствия параметров выявленных в компьютерной системе физических аппаратных устройств атрибутам безопасности (разрешенным параметрам), установленным СЗИ для данного состава аппаратных устройств;

установление для каждой роли, предусматриваемой СЗИ, перечня (списка) разрешенных для использования в рамках данной роли физических аппаратных устройств;

блокирование компьютерной системы при выявлении какого-либо аппаратного устройства, не находящегося в список аппаратных устройств, разрешенных СЗИ к использованию в составе компьютерной системы для ролей пользователей и администраторов;

блокирование компьютерной системы при несоответствии параметров выявленных физических аппаратных устройств атрибутам безопасности (разрешенным параметрам), установленным СЗИ для данного состава аппаратных устройств компьютерной системы для ролей пользователей и администратора безопасности;

в режиме обслуживания:

непрерывный контроль параметров функционирования всех аппаратных устройств компьютерной системы, а также проверки соответствия параметров физических устройств атрибутам безопасности, (разрешенным параметрам), установленным СЗИ для конкретного типа устройств;

поддержка в данных управления СЗИ списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы (белого списка);

поддержка в данных управления СЗИ списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой СЗИ;

возможность изменения списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы (белого списка), и списка аппаратных устройств, разрешенных для каждой роли, предусматриваемой СЗИ;

в режиме аудита:

непрерывный контроль параметров функционирования всех аппаратных устройств компьютерной системы, а также проверки соответствия параметров физических устройств атрибутам безопасности, (разрешенным параметрам), установленным СЗИ для конкретного типа устройств;

поддержка в данных управления СЗИ списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы (белого списка);

поддержка в данных управления СЗИ списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой СЗИ;

отключение аппаратных устройств и/или блокирование работы компьютерной системы при подключении какого-либо аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы;

блокирование работы компьютерной системы со стороны СЗИ при изменении параметров функционирования аппаратных устройств;

в эксплуатационном режиме:

непрерывный контроль параметров функционирования всех аппаратных устройств компьютерной системы, а также проверки соответствия параметров физических устройств атрибутам безопасности, (разрешенным параметрам), установленным СЗИ для конкретного типа устройств;

поддержка в данных управления СЗИ списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы (белого списка);

поддержка в данных управления СЗИ списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой СЗИ;

отключение аппаратных устройств и/или блокирование работы компьютерной системы при подключении какого-либо аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы;

блокирование работы компьютерной системы со стороны СЗИ при изменении параметров функционирования аппаратных устройств.

Рассмотрим управление доступом.

В состав управления доступом входят:

управление доступом на основе ролей;

управление доступом субъектов доступа к объектам доступа, в том числе

базовое управление доступом субъектов доступа к объектам доступа,

управление доступом субъектов доступа к накопителям информации,

управление доступом субъектов доступа (аппаратных устройств компьютерной системы) к оперативной памяти.

Рассмотрим управление доступом на основе ролей.

Управление доступом в компьютерной системе на основе ролей, рассматриваемое в настоящем техническом решении, является основой для управления доступом, поскольку создание виртуальных машин и предоставление виртуальным машинам доступа к физическим аппаратным устройствам компьютерной системы осуществляется в соответствии с ролевой моделью доступа.

Управление доступом в компьютерной системе на основе ролей, рассматриваемое в настоящем техническом решении, характеризуется ключевой особенностью, состоящей в том, что доступ к ресурсам компьютерной системы предоставляется только через роли.

При этом под ролью понимается совокупность возможностей, предоставляемых пользователю в сеансе работы компьютерной системы, в зависимости от обязанностей, выполняемых пользователем (например, обработка и хранение информации).

Роль характеризуется профилем роли и ассоциируется с уникальным идентификатором роли, присваиваемым по результатам идентификации и аутентификации пользователя.

При управлении доступом в компьютерной системе на основе ролей пользователи получают доступ к аппаратным ресурсам компьютерной системы и/или к виртуальным машинам только через присвоенные им роли.

Управление доступом к аппаратным ресурсам компьютерной системы и/или к виртуальным машинам основывается не на принадлежности ресурса, а на выполнении соответствующим пользователем своих обязанностей (например, обработка и хранение информации).

Управление доступом в компьютерной системе на основе ролей, рассматриваемое в настоящем техническом решении, больше связано с управлением доступом к операциям над объектами доступа в компьютерной системе, а не с управлением доступом непосредственно к объектам доступа.

Роль выполняется в конкретном сеансе работы пользователя и основана на статическом разделении обязанностей между категориями пользователей.

Рассмотрим базовое управление доступом субъектов доступа к объектам доступа в компьютерной системе.

Базовое управление доступом субъектов доступа к объектам доступа реализуется в соответствии со схемой функционирования встроенного в типовую архитектуру аппаратной платформы компьютерной системы СЗИ, обеспечивающего защиту компьютерной системы от НСД к информации, приведенной на фиг. 2.

Базовое управление доступом субъектов доступа к объектам доступа в компьютерной системе предусматривает обязательную реализацию следующих правил.

1. Запрос на доступ любого неидентифицированного субъекта доступа к любым объектам доступа однозначно запрещается.

2. Любые запросы на прямой доступ между физическими аппаратными устройствами/шинами компьютерной системы, кроме устройств, сертифицированных по требованиям защиты информации государственными органами страны применения компьютерной системы, и виртуальными машинами должны быть запрещены.

3. Любым субъектам доступа должен быть запрещен доступ

к данным управления СЗИ;

к образам виртуальных машин;

к параметрам виртуальных машин;

к списку аппаратных устройств/шин компьютерной системы, участвующих в обработке информации;

к списку состава аппаратных устройств/шин компьютерной системы, используемому для контроля целостности аппаратных ресурсов компьютерной системы;

к данным, характеризующим виртуальные машины и их состояние;

к журналам регистрации событий.

Базовое управление субъектов доступа к объектам доступа в компьютерной системе является базовой концептуальной основой для обеспечения изоляции данных управления компьютерной системы, используемых СЗИ, и данных, обрабатываемых программным обеспечением, установленным в компьютерной системе, от аппаратных устройств/шин компьютерной системы.

СЗИ создает защищенную среду функционирования для каждой виртуальной машины с помощью базового управления доступом субъектов доступа к объектам доступа в компьютерной системе.

Базовое управление субъектов доступа к объектам доступа в компьютерной системе непосредственно связано с управлением конфигурацией аппаратных средств компьютерной системы, основанной на списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы.

Рассмотрим управление доступом субъектов доступа к накопителям информации.

Управление доступом субъектов доступа к накопителям информации в компьютерной системе предусматривает

управление доступом субъектов доступа к накопителям информации с разделами, разделам накопителей информации;

управление доступом субъектов доступа к накопителям информации без разделов.

Управление доступом субъектов доступа к накопителям информации в компьютерной системе основано на базовой схеме функционирования встроенного в типовую архитектуру аппаратной платформы СЗИ, обеспечивающего защиту компьютерной системы от НСД к информации с учетом того, что

в качестве физического аппаратного устройства выступает физический накопитель информации;

ПРД в том числе учитывают\включают проверку дополнительных ПРД субъектов доступа к объектам доступа (например, при доступе к накопителям информации, разделам накопителей информации).

Рассмотрим управление доступом субъектов доступа (аппаратных устройств компьютерной системы) к оперативной памяти.

Управление доступом субъектов доступа (аппаратных устройств компьютерной системы) к оперативной памяти основано на алгоритме защиты оперативной памяти от прямого доступа со стороны аппаратных устройств компьютерной системы.

СЗИ обеспечивает конфигурирование защиты оперативной памяти от прямого доступа со стороны аппаратных устройств компьютерной системы в соответствии с алгоритмом.

1. СЗИ запрашивает и получает из аппаратного устройства СЗИ список и параметры разрешенных устройств компьютерной системы.

2. СЗИ формирует "белый" список устройств с возможностью прямого доступа к памяти.

3. СЗИ получает параметры прямого доступа к памяти от устройств из "белого" списка.

4. СЗИ производит конфигурирование защиты с помощью полученных параметров прямого доступа к оперативной памяти от устройств компьютерной системы из "белого" списка.

Защита оперативной памяти компьютерной системы от прямого доступа со стороны аппаратных устройств компьютерной системы обеспечивается СЗИ в соответствии с алгоритмом.

1. Физические аппаратные устройства компьютерной системы (устройства/шины) генерируют запросы прямого доступа к оперативной памяти.

2. СЗИ осуществляет сбор (перехват) данных (параметров), содержащихся в запросах прямого доступа к оперативной памяти от аппаратных устройств.

3. СЗИ осуществляет проверку собранных (перехваченных) параметров запроса в соответствие с матрицей доступа (пример матрицы доступа приведен в таблице. При соответствии параметров, содержащихся в запросе, параметрам прямого доступа к памяти от устройств из "белого" списка, запрос разрешается. В противном случае осуществляется блокировка запроса.

4. СЗИ регистрирует событие блокировки запроса в журнале регистрации событий.

Рассмотрим управление информационными потоками.

Для каждой виртуальной машины создается своя защищенная среда выполнения (виртуальные машины изолированы друг от друга). Обмен информации между виртуальными машинами возможен только посредством внешних накопителей информации и сетевого взаимодействия.

Для сокращения объема НЖМД в компьютерной системе виртуальными машинами может быть использован совместный доступ виртуальных машин к накопителю информации с разделом (например, НЖМД (разделу НЖМД) и т.д.).

В настоящем техническом решении компьютерной системы от НСД к информации, реализуемой на уровне аппаратной платформы компьютерной системы, предусмотрены следующие виды управления информационными потоками:

управление информационными потоками при совместном использовании накопителя информации, раздела накопителя информации несколькими виртуальными машинами;

управление информационными потоками при сетевом взаимодействии компьютерной системы.

Рассмотрим управление информационными потоками при совместном использовании накопителя информации несколькими виртуальными машинами.

Управление информационными потоками при совместном использовании накопителя информации (например, НЖМД и т.д.) несколькими виртуальными машинами основана на механизмах СЗИ, обеспе-

чивающих возможность использования накопителя информации (например, НЖМД и т.д.) несколькими виртуальными машинами одновременно (например, системного раздела с установленной ОС). СЗИ обеспечивает неизменность совместно используемого накопителя информации (например, НЖМД (раздела НЖМД) и т.д.) предоставляя доступ виртуальных машин к совместно используемому накопителю информации в режиме только чтение.

Обмен информации между виртуальными машинами посредством внешних накопителей информации осуществляется в режиме последовательного использования внешнего накопителя информации виртуальными машинами. С внешним накопителем информации может взаимодействовать только одна виртуальная машина. В случае когда внешний накопитель информации уже используется виртуальной машиной, он становится недоступным для взаимодействия другим виртуальным машинам. Для взаимодействия внешнего накопителя информации с другой виртуальной машиной из первой он должен быть извлечен (например, первую виртуальную машину необходимо выключить). Разграничение доступа к/от внешних носителей информации относится к разграничению доступа к устройствам и было рассмотрено выше.

Рассмотрим управление информационными потоками при сетевом взаимодействии компьютерной системы.

Управление информационными потоками при сетевом взаимодействии компьютерной системы основано на механизмах СЗИ, обеспечивающих фильтрацию сетевого трафика.

СЗИ осуществляет фильтрацию сетевого трафика по каждому протоколу сетевого взаимодействия как при запросах, исходящих от виртуальной машины (исходящие запросы), так и при запросах, исходящих от физической сетевой карты (входящие запросы).

Управление информационными потоками при сетевом взаимодействии компьютерной системы основано на базовой схеме функционирования встроенного в типовую архитектуру аппаратной платформы средства защиты информации (СЗИ), обеспечивающего защиту компьютерной системы от НСД к информации с учетом того, что

в качестве физического аппаратного устройства выступает физическая сетевая карта;

правила разграничения доступа в том числе учитывают\включают проверку

типа запроса, поступившего от виртуальной машины, на его соответствие правилам разграничения доступа, установленным для уровней модели OSI (например, канального, сетевого и транспортного) и\или для соответствующих им протоколов (например, Ethernet, IPv4, ICMP, TCP, UDP);

данных, содержащихся в запросе виртуальной машины, на их соответствие атрибутам доступа (применение правил фильтрации), установленным СЗИ;

и т.д.

СЗИ осуществляет фильтрацию сетевого трафика по каждому протоколу сетевого взаимодействия в соответствии с матрицами доступа как при запросах, исходящих от виртуальной машины (исходящие запросы), так и при запросах, исходящих от физической сетевой карты (входящие запросы).

При наличии в компьютерной системе одной виртуальной машины допускается отключение фильтрации сетевого трафика в СЗИ, если фильтрацию сетевого трафика обеспечивает установленный за компьютерной системой аппаратный маршрутизатор и/или межсетевой экран.

При наличии в компьютерной системе нескольких виртуальных машин, СЗИ обеспечивает фильтрацию сетевого трафика между виртуальными машинами.

В табл. 1 приведен пример состава вычислительных ресурсов компьютерной системы (с учетом виртуальных вычислительных ресурсов, создаваемых СЗИ) и параметры, характеризующие каждый вычислительный ресурс компьютерной системы.

При этом состав и параметры виртуальных ресурсов, созданных СЗИ, отличаются от состава и параметров физических аппаратных устройств компьютерной системы с целью:

гарантированного выявления несанкционированных запросов виртуальной машины на доступ к физическим аппаратным устройствам компьютерной системы, включая устройства аппаратной платформы (шины и устройства);

обеспечения невозможности эксплуатации уязвимостей устройств компьютерной системы для любого ПО, выполняющегося внутри виртуальной машины.

Управление конфигурацией

Рассмотрим управление конфигурацией аппаратных средств компьютерной системы при запуске компьютерной системы.

При запуске компьютерной системы СЗИ обеспечивает управление конфигурацией аппаратных средств в следующей последовательности: сбор данных о фактическом составе всех аппаратных устройств компьютерной системы, а также параметров их функционирования осуществляется посредством запросов к шинам (например, PCI/PCI Express, USB, SATA и т.д.). На основе собранных данных составляется список подключенных устройств и их параметров. Параметры функционирования устройств выбираются исходя из типа устройств.

Пример списка выявляемых аппаратных устройств компьютерной системы и их параметры приведен в табл. 2.

Сбор данных о фактическом составе всех аппаратных устройств компьютерной системы, а также параметров их функционирования, осуществляется при каждом запуске компьютерной системы.

СЗИ сравнивает собранные данные с аналогичными данными, сохраненными ранее в данных управления СЗИ и выполняющими (в части параметров функционирования устройств) роль атрибутов безопасности. В случае обнаружения несоответствия между составом аппаратных устройств и/или параметров функционирования устройств с данными управления СЗИ загрузка СЗИ обеспечивается только в режиме обслуживания.

Контроль состава и параметров функционирования аппаратных устройств компьютерной системы производится для каждого типа устройств и каждого параметра функционирования устройств (пример списка для компьютерной системы приведен ранее в табл. 2, и в соответствии с матрицей, устанавливающей правила проверки соответствия фактического состава всех выявленных аппаратных устройств компьютерной системы, списку аппаратных устройств, разрешенных для использования в составе компьютерной системы, а также соответствия параметров выявленных физических аппаратных устройств атрибутам безопасности (разрешенным параметрам), установленным для данного состава аппаратных устройств. Пример матрицы для устройств, подключаемых к шине PCI/PCI Express, приведен в табл. 3.

СЗИ инициирует установку для каждой роли, предусматриваемой СЗИ, перечня (списка) разрешенных для использования в рамках данной роли физических аппаратных устройств.

СЗИ получает данные, аутентифицирующие пользователя и характеризующих его роль в текущем сеансе работы компьютерной системы (из аппаратного устройства СЗИ) и определяет режим функционирования (режим обслуживания, эксплуатационный режим или режим аудита).

В случае обеспечения загрузки СЗИ только в режиме обслуживания и определении эксплуатационного режима или режима аудита осуществляется запись данных о событии, связанном с выявлением неизвестного устройства, в журнал регистрации событий СЗИ с дальнейшей блокировкой работы компьютерной системы.

В случае обеспечения загрузки СЗИ только в режиме обслуживания и определении режима обслуживания СЗИ позволит пользователю, аутентифицированному в качестве администратора защиты осуществить просмотр журнала регистрации событий или выполнить настройки и конфигурирование СЗИ.

В случае отсутствия обеспечения загрузки СЗИ только в режиме обслуживания

при определении СЗИ режима обслуживания СЗИ позволит пользователю, аутентифицированному в качестве администратора защиты осуществить просмотр журнала регистрации событий или выполнить настройки и конфигурирование СЗИ;

при определении СЗИ режима аудита СЗИ позволит пользователю, аутентифицированному в качестве администратора безопасности осуществить работу с журналом регистрации событий;

при определении СЗИ эксплуатационного режима СЗИ функционирует в соответствии с данными, аутентифицирующими пользователя и характеризующими его роль в текущем сеансе работы компьютерной системы.

Далее для обеспечения функционирования компьютерной системы в эксплуатационном режиме на основании полученных данных СЗИ создает виртуальные ресурсы компьютерной системы в соответствии со списком виртуальных устройств, присущим данной роли пользователя. Далее СЗИ осуществляет поддержку физических аппаратных устройств компьютерной системы, строго соответствующих списку виртуальных ресурсов, присущих данной роли пользователя. После создания виртуальных ресурсов компьютерной системы для роли пользователя в текущем сеансе работы и осуществления поддержки физических аппаратных устройств, СЗИ создает виртуальную машину в конфигурации, соответствующей данной роли пользователя в текущем сеансе эксплуатационного режима функционирования.

Рассмотрим управление конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы.

При работе компьютерной системы СЗИ обеспечивает управление конфигурацией аппаратных средств компьютерной системы по двум различным схемам:

по схеме, основанной на механизмах периодической проверки состава аппаратных средств компьютерной системы и параметров их функционирования;

по схеме, основанной на непрерывном анализе запросов от физических аппаратных устройств компьютерной системы на доступ к вычислительным ресурсам компьютерной системы (в том числе связанным с функционированием виртуальной машины).

Рассмотрим схему, основанную на механизмах периодической проверки состава аппаратных средств компьютерной системы и параметров их функционирования.

При проведении периодической проверки состава аппаратных средств компьютерной системы и параметров их функционирования СЗИ осуществляет

запросы к шинам (например, PCI/PCI Express, USB, SATA и т.д.) с целью выявления устройств, подключенных к данным шинам, и их параметров;

определение состава выявленных устройств и их параметров;

получение списка подключенных к компьютерной системе устройств в данном сеансе работы компьютерной системы и списка устройств, разрешенных к использованию в составе компьютерной систе-

мы (белого списка);

определение наличия изменений в составе выявленных устройств и/или их параметров путем сравнения соответствующих данных, в том числе определение выявленного устройства, подключенного в "горячем" режиме, и его параметров.

В режиме обслуживания при выявлении устройства, подключенного в "горячем" режиме и не предусмотренного в списке разрешенных СЗИ устройств для данного сеанса работы, или предусмотренного в списке разрешенных устройств для данного сеанса работы, но имеющего другие параметры функционирования, СЗИ обеспечивает возможность настройки ПРД для обнаруженного устройства и сохранения изменений конфигурации. При сохранении конфигурации происходит формирование нового списка разрешенных СЗИ устройств и сохранение его в конфигурационных данных СЗИ.

В режиме аудита и эксплуатационном режиме при выявлении устройства, подключенного в "горячем" режиме и не предусмотренного в списке разрешенных СЗИ устройств для данного сеанса работы, или предусмотренного в списке разрешенных СЗИ устройств для данного сеанса работы, но имеющего другие параметры функционирования, СЗИ

отражает событие и данные о событии, связанном с выявлением устройства, подключенном в "горячем" режиме, в журнале регистрации событий;

обеспечивает последующее включение компьютерной системы только в режиме обслуживания компьютерной системы;

отражает событие и данные о событии, связанном с переводом СЗИ в режим обслуживания компьютерной системы, в журнале регистрации событий;

блокирует работу компьютерной системы.

В режиме аудита при выявлении устройства, подключенного в "горячем" режиме, и предусмотренного в списке разрешенных СЗИ устройств для данного сеанса работы, а также имеющего разрешенные СЗИ параметры функционирования, СЗИ обеспечивает работу с журналом регистрации событий.

В эксплуатационном режиме при выявлении устройства, подключенного в "горячем" режиме, и предусмотренного в списке разрешенных СЗИ устройств для данного сеанса работы, а также имеющего разрешенные СЗИ параметры функционирования СЗИ продолжает функционирование в рамках текущего сеанса работы компьютерной системы в соответствии с ролью пользователя. Поскольку поддержка виртуальных и физических устройств была осуществлена при запуске компьютерной системы в текущем сеансе эксплуатационного режима, СЗИ создает соответствующее виртуальное устройство в виде виртуального ресурса и обеспечивает управление функционированием виртуальной машины в установленном порядке.

Рассмотрим схему, основанную на непрерывном анализе запросов от физических аппаратных устройств компьютерной системы на доступ к вычислительным ресурсам компьютерной системы (в том числе связанным с функционированием виртуальной машины).

При проведении непрерывного анализа запросов от физических аппаратных устройств компьютерной системы на доступ к вычислительным ресурсам компьютерной системы, СЗИ осуществляет сбор (перехват) данных (параметров), содержащихся в запросах от физических аппаратных устройств компьютерной системы.

Пример общеизвестных параметров физических вычислительных ресурсов компьютерной системы, содержащихся в запросах на доступ от физических аппаратных устройств компьютерной системы, ранее был приведен в табл. 1.

На основании собранных (перехваченных) данных СЗИ осуществляет идентификацию физического аппаратного устройства компьютерной системы, в т.ч. устройства аппаратной платформы компьютерной системы (шины или устройства), от которого был произведен запрос, и правомочность запроса от данного физического аппаратного устройства компьютерной системы.

В режиме обслуживания, при невозможности СЗИ идентифицировать физическое аппаратное устройство компьютерной системы и/или невозможности подтверждения СЗИ правомочности запроса от данного физического аппаратного устройства компьютерной системы, данный запрос отклоняется. При этом СЗИ обеспечивает возможность настройки ПРД для обнаруженного устройства и сохранения изменений конфигурации. При сохранении конфигурации происходит формирование нового списка разрешенных СЗИ устройств и сохранение его в конфигурационных данных СЗИ.

В режиме аудита и эксплуатационном режиме, при невозможности СЗИ идентифицировать физическое аппаратное устройство компьютерной системы и/или невозможности подтверждения СЗИ правомочности запроса От данного физического аппаратного устройства компьютерной системы, данный запрос отклоняется.

При этом СЗИ:

отражает событие и данные о событии, связанном с выявлением неизвестного устройства в журнале регистрации событий;

обеспечивает последующее включение компьютерной системы только в режиме обслуживания компьютерной системы;

отражает событие и данные о событии, связанном с переводом СЗИ в режим обслуживания компь-

ютерной системы, в журнале регистрации событий;

блокирует работу компьютерной системы.

В режиме аудита в случае успешной идентификации физического аппаратного устройства компьютерной системы и подтверждения правомочности запроса от данного физического аппаратного устройства компьютерной системы, СЗИ обеспечивает работу с журналом регистрации событий.

В эксплуатационном режиме, в случае успешной идентификации физического аппаратного устройства компьютерной системы и подтверждения правомочности запроса от данного физического аппаратного устройства компьютерной системы, СЗИ, используя данные/параметры физических вычислительных ресурсов, содержащихся в СЗИ:

осуществляет проверку данных, содержащихся в запросе физического аппаратного устройства компьютерной системы, на соответствие спецификации разрешаемых СЗИ;

осуществляет преобразование данных, содержащихся в запросе физического аппаратного устройства компьютерной системы, в данные виртуального устройства;

создает соответствующее виртуальное устройство в виде виртуального ресурса и обеспечивает управление функционированием виртуальной машины в установленном порядке (поддержка виртуальных и физических устройств была осуществлена при запуске компьютерной системы в текущем сеансе эксплуатационного режима);

транслирует данные/параметры виртуальных вычислительных ресурсов виртуальной машине.

Одновременная реализация в СЗИ двух схем управления конфигурацией обеспечивает эшелонированную защиту от несанкционированного изменения конфигурации аппаратных средств компьютерной системы, от создания скрытых каналов несанкционированного доступа, как к вычислительным ресурсам компьютерной системы, так и к программной среде виртуальной машины и к пользовательским обрабатываемым данным, подлежащим защите от НСД к информации.

Управление доступом

В настоящем техническом решении компьютерной системы от НСД к информации, реализуемой на уровне аппаратной платформы, предусмотрены следующие категории пользователей:

категория "Пользователь" - пользователь, выполняющий обязанности по созданию, обработке и хранению информации, составляющей государственную тайну;

категория "Администратор защиты" - пользователь, выполняющий конфигурирование СЗИ;

категория "Администратор безопасности" - пользователь, выполняющий работу с журналом регистрации событий СЗИ.

Роли назначаются только для вышеуказанных категорий пользователей.

При этом под профилем роли для категории "Пользователь" понимается совокупность характеристик виртуальной машины и прав, устанавливаемых для роли по доступу к физическим аппаратным устройствам компьютерной системы, и их соответствие виртуальным ресурсам, доступных виртуальной машине.

При этом под профилем роли для категории "Администратор защиты" понимается совокупность прав доступа для программ по настройке профиля роли для категории "Пользователь" и по обработке данных журнала регистрации событий СЗИ.

При этом под профилем роли для категории "Администратор безопасности" понимается совокупность прав доступа для программы по обработке данных журнала регистрации событий СЗИ.

Пример профиля роли для категории "Пользователь" приведен в табл. 4, 5.

При назначении характеристик виртуальной машины, ассоциированной с уникальным идентификатором роли для категории "Пользователь", их значения, в последующем предоставляемые по запросу виртуальной машины, должны в обязательном порядке отличаться от реальных характеристик системных ресурсов компьютерной системы.

Пример прав доступа для программ, характеризующих профиль роли для категории "Администратор защиты" приведен в табл. 6.

Роли "Администратор защиты" по умолчанию запрещается доступ к любым виртуальным машинам.

Пример прав доступа для программы по обработке данных журнала регистрации событий СЗИ, характеризующие профиль роли для категории "Администратор безопасности" приведен в табл. 7.

Роли "Администратор безопасности" по умолчанию запрещается запуск любых виртуальных машин и доступ к их настройкам.

Пример матрицы доступа, в соответствии с которой обеспечивается разграничение доступа субъектов доступа к объектам доступа при реализации базового управления доступом, приведен в табл. 8.

Дополнительные ПРД, указанные в Матрице доступа, в соответствии с которой обеспечивается разграничение доступа субъектов доступа к объектам доступа при реализации базового управления доступом, применяются только по отношению к накопителям информации и сетевым адаптерам.

Управление доступом субъектов доступа к накопителям информации с разделами, разделам накопителей информации осуществляется в соответствии с матрицей доступа (пример матрицы доступа представлен в табл. 9).

Управление доступом субъектов доступа к накопителям информации без разделов осуществляется

в соответствии с матрицей доступа (пример матрицы доступа представлен в табл. 10).

Пример матрицы доступа, в соответствии с которой обеспечивается управление доступом субъектов доступа (аппаратных устройств компьютерной системы) к оперативной памяти, приведен в табл. 11).

Управление информационными потоками

Управление информационными потоками при сетевом взаимодействии компьютерной системы основано на механизмах СЗИ, обеспечивающих фильтрацию сетевого трафика. Пример уровней модели OSI, на которых СЗИ обеспечивает фильтрацию сетевого трафика приведен в табл. 12.

Пример матрицы доступа, в соответствии с которой осуществляется фильтрация сетевого трафика на канальном уровне модели OSI для протокола Ethernet, приведен в табл. 13.

Таблица 1. Пример состава вычислительных ресурсов компьютерной системы и параметров, характеризующих каждый вычислительный ресурс компьютерной системы

Наименование вычислительных ресурсов компьютерной системы	**Параметры, характеризующие вычислительный ресурс**
Оперативная память	Адрес памяти, размер памяти, параметры доступа (чтение или запись)
Порты ввода – вывода	Номер порта, разрядность порта
Виртуальные прерывания	Вектор прерывания
Исключительные ситуации в виртуальной машине	Вектор исключения
Прерывания от устройств	Вектор прерывания
Регистры центрального процессора	Идентификатор регистра, тип (чтение, запись), значение
Параметры центрального процессора	Информация (данные) о центральном процессоре (инструкции, возможности)
Счетчик центрального процессора	Значение счетчика
Команды центрального процессора	Параметры команд
Прямой доступ к оперативной памяти (DMA) со стороны устройств	Адрес устройства, адрес памяти, размер памяти

Таблица 2. Пример списка выявляемых аппаратных устройств компьютерной системы и их параметров

Наименование (тип) устройства	**Параметры функционирования устройства**
Устройства шины PCI/PCI Express	адрес устройства на шине (шина, устройство, функция); идентификатор производителя; идентификатор устройства; идентификатор класса устройства (класс, подкласс, интерфейс); версия устройства
Устройства шины USB	идентификатор производителя (числовой и строковый); идентификатор устройства (числовой и строковый); серийный номер устройства

USB накопители информации	Дополнительно к атрибутам устройств шины USB: строковый идентификатор производителя носителя информации; строковый идентификатор носителя информации; строковый идентификатор версии носителя информации
НЖМД, подключенные к шине SATA	номер порта, к которому подключен НЖМД; строковый идентификатор производителя; строковый идентификатор устройства; серийный номер; версия прошивки
CD/DVD-ROM, подключенные к шине SATA	номер порта, к которому подключен CD/DVD-ROM; строковый идентификатор производителя; строковый идентификатор устройства; версия прошивки
Устройства ввода PS/2	тип устройства ввода: клавиатура или мышь
Сетевые адаптеры	MAC-адрес сетевого адаптера
COM-порты	номер порта
Системный динамик	–

Таблица 3. Пример формы матрицы, устанавливающей правила проверки соответствия фактического состава всех выявленных аппаратных устройств, подключаемых к шине PCI/PCI Express, списку аппаратных устройств, разрешенных для использования в составе компьютерной системы, а также соответствия параметров выявленных физических аппаратных устройств атрибутам безопасности, установленным для данного состава аппаратных устройств

Наименование (тип) устройства	**Контролируемые параметры физического устройства**	**Атрибуты безопасности для устройств, установленные СЗИ**	**Результат сравнения параметров физического устройства с атрибутами безопасности**	**Реакция СЗИ по результатам сравнения**
Устройства шины PCI/PCI Express	адрес устройства на шине (шина, устройство, функция)	адрес устройства на шине (шина, устройство, функция)	соответствие/ несоответствие	разрешение функционирования/ блокирование компьютерной системы
	идентификатор производителя;	идентификатор производителя;	соответствие/ несоответствие	разрешение функционирования/ блокирование компьютерной системы
Устройства шины PCI/PCI Express	идентификатор устройства	идентификатор устройства	соответствие/ несоответствие	разрешение функционирования/ блокирование компьютерной системы
	идентификатор класса устройства (класс, подкласс, интерфейс)	идентификатор класса устройства (класс, подкласс, интерфейс)	соответствие/ несоответствие	разрешение функционирования/ блокирование компьютерной системы
	версия устройства	версия устройства	соответствие/ несоответствие	разрешение функционирования/ блокирование компьютерной системы

Таблица 4. Пример характеристик виртуальной машины, ассоциированной с уникальным идентификатором роли для категории "Пользователь"

Характеристика виртуальной машины	**Предоставляемое значение по запросу виртуальной машины**
Производитель системной платы	Наименование производителя эмулируемой системной платы
Модель системной платы	Наименование модели эмулируемой системной платы
Тип BIOS	Тип эмулируемого BIOS (PC-BIOS или UEFI-BIOS)
Поставщик BIOS	Наименование производителя эмулируемого BIOS
Версия BIOS	Версия эмулируемого BIOS
Дата выпуска BIOS	Дата выпуска эмулируемого BIOS
Модель центрального процессора	Наименование модели эмулируемого центрального процессора и его технические характеристики
Количество ядер центрального процессора	Количество ядер эмулируемого центрального процессора
Оперативная память	Размер виртуальной оперативной памяти в МБ

Таблица 5. Пример прав, устанавливаемых для роли по доступу к физическим аппаратным устройствам компьютерной системы, и их соответствие виртуальным ресурсам, доступных виртуальной машине

Тип и наименование физических устройств компьютерной системы	**Совокупность параметров физического устройства**	**Права доступа пользователя к операциям, связанным с физическим устройством**	**Совокупность параметров виртуального устройства, соответствующего физическому устройству компьютерной системы**
Накопители информации:			
НЖМД № 1, подключенный к шине SATA	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
НЖМД № 2, подключенный к шине SATA	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
НЖМД № n, подключенный к шине SATA	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
устройство чтения CD/DVD-ROM, подключенное к шине SATA	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
Периферийные устройства компьютерной системы, подключаемые к портам USB:			
устройство «мышь»	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
клавиатура	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
концентратор	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
USB – накопитель	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
принтер	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
многофункциональное устройство	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
сканер	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3

Внутренние ресурсы компьютерной системы:			
сетевой адаптер	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
COM-порты	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
VGA – контроллер (подключение монитора)	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
системный динамик	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
Устройства ввода, подключаемые к портам PS/2:			
устройство «мышь»	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3
клавиатура	В соответствии с таблицей 3	разрешено/ запрещено	В соответствии с таблицей 3

Таблица 6. Пример прав доступа для программы по настройке профиля роли для категорий "Пользователь" и программы по обработке данных журнала регистрации событий СЗИ, характеризующих профиль роли для категории "Администратор защиты"

Наименование программ СЗИ, доступных роли «Администратор защиты»	**Права доступа к физическим устройствам компьютерной системы**	**Права доступа к данным программ**	
		Чтение (R)	**Запись (W)**
Программа настройки ролей «Пользователь»	разрешено	разрешено	разрешено
Программа по обработке данных журнала регистрации событий СЗИ	запрещено	разрешено	запрещено

Таблица 7. Пример прав доступа для программы по обработке данных журнала регистрации событий СЗИ, характеризующие профиль роли для категории "Администратор безопасности"

Наименование программ СЗИ, доступных роли «Администратор безопасности»	**Права доступа к данным журнала регистрации событий**	
	Чтение (R)	**Запись (W)**
Программа по обработке данных журнала регистрации событий СЗИ	разрешено	разрешено

Таблица 8. Пример матрицы доступа, в соответствии с которой обеспечивается разграничение доступа субъектов доступа к объектам доступа при реализации базового управления доступом

Идентификатор роли	Субъект доступа	Тип объекта доступа (физического устройства)	Совокупность параметров объекта доступа (физического устройства)	Совокупность параметров объекта доступа, представленного виртуальным устройством	Права доступа субъекта доступа к объекту доступа	Наличие дополнительных правил разграничения доступа
Пользователь 1	VM1	НЖМД WD1003FZEX	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к разделам виртуального НЖМД
	VM1	CD/DVD-ROM	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к виртуальному CD/DVD-ROM
	VM1	клавиатура	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM1	устройство «мышь»	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM1	принтер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM1	сетевой адаптер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к сетевому трафику
	VM1	VGA – контроллер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM1	USB – накопитель KingstonDataTrave-ler 10	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к разделам виртуального USB – накопителя
	.....	.....	.....	.....	.....	.....
Пользователь 2	VM2	НЖМД WD1003FZEX	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к разделам виртуального НЖМД
	VM2	CD/DVD-ROM	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к виртуальному CD/DVD-ROM
	VM2	клавиатура	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
Пользователь 2	VM2	устройство «мышь»	В соответствии с таблицей 3	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM2	принтер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM2	сетевой адаптер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к сетевому трафику
	VM2	VGA – контроллер	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	–
	VM2	USB – накопитель KingstonDataTraveler 10	В соответствии с таблицей 3.	В соответствии с таблицей 3.	разрешено/ запрещено	ПРД к разделам виртуального USB – накопителя
	.....	.....	.....	.....	.....	.....

Таблица 9. Пример матрицы доступа, характеризующая управление доступом к разделам накопителей информации

Идентификатор роли	Субъект доступа	Объект доступа (раздел физического накопителя информации)	Подмена идентификаторов раздела накопителя информации в виртуальной машине	Подменяемые идентификаторы раздела накопителя информации в виртуальной машине	Тип доступа			
					Видимость	Обратимое преобразование	Чтение	Запись
Пользователь 1	VM1	НЖМД 1 / раздел 1	+/-	модель серийный номер версия прошивки	+/-	+/-	+/-	+/-
	VM1	……	……	……	……	……	……	……
	VM1	НЖМД n / раздел k	+/-	модель серийный номер версия прошивки	+/-	+/-	+/-	+/-
	VM1	USB – накопитель	+/-	VID; PID; строка VID; строка PID; серийный номер; производитель; модель; версия прошивки	+/-	+/-	+/-	+/-
Пользователь 2	VM2	НЖМД 2 / раздел 1	+/-	модель серийный номер версия прошивки	+/-	+/-	+/-	+/-
	VM2	USB – накопитель	+/-	VID; PID; строка VID; строка PID; серийный номер; производитель; модель; версия прошивки	+/-	+/-	+/-	+/-

Таблица 10. Пример матрицы доступа, характеризующая управление доступом к накопителям информации без разделов

Идентификатор роли	Субъект доступа	Объект доступа (физический накопитель информации)	Тип доступа		
			Обратимое преобразование	Чтение	Запись
«Пользователь 1»	VM1	накопитель CD/DVD/Blu-ray 1	+/-	+/-	+/-
	VM1	……	+/-	+/-	+/-
	VM1	накопитель CD/DVD/Blu-ray k	+/-	+/-	+/-
«Пользователь 2»	VM2	накопитель CD/DVD/Blu-ray 1	+/-	+/-	+/-

Таблица 11. Пример матрицы доступа, в соответствии с которой обеспечивается управление доступом субъектов доступа (аппаратных устройств компьютерной системы) к оперативной памяти

Идентификатор роли	Субъект доступа (физическое устройство компьютерной системы, имеющее возможность прямого доступа к оперативной памяти)	Объект доступа	Права доступа субъекта доступа к объекту доступа	Атрибуты доступа			
				Адрес памяти	Размер памяти	Тип доступа	
						Чтение	Запись
«Пользователь 1»	Сетевая карта	VM1	разрешено/ запрещено	0x1000	0x100	+/-	+/-
«Пользователь 1»	Видеоадаптер	VM1	разрешено/ запрещено	0x42000	0x1000	+/-	+/-
«Пользователь 2»	Сетевая карта	VM2	разрешено/ запрещено	0x1000	0x100	+/-	+/-
«Пользователь 2»	Видеоадаптер	VM2	разрешено/ запрещено	0x42000	0x1000	+/-	+/-
«Пользователь 2»	Контроллер USB	VM2	разрешено/ запрещено	0x7000	0x2000	+/-	+/-

Таблица 12. Пример уровней модели OSI, на которых СЗИ обеспечивает фильтрацию сетевого трафика

Уровень модели OSI	Протокол сетевого взаимодействия
Канальный уровень	Ethernet
Сетевой уровень	IP
	IPv6
	ICMP
	ICMPv6
Транспортный уровень	TCP/IP
	TCP/IPv6
	UDP/IP
	UDP/IPv6

Таблица 13. Пример матрицы доступа, в соответствии с которой осуществляется фильтрация сетевого трафика на канальном уровне модели OSI для протокола Ethernet

Субъект доступа	Тип объекта доступа	Атрибуты доступа						
		Локальный адрес	Удаленный адрес	Формат кадра	Тип кадра	OUI (уникальный идентификатор организации)	Направление сетевого трафика	
							Входящий	Исходящий
VM1	Сетевая карта 1	fe:fd:de:ad:ff:ff	fe:fa:de:ad:ff:ff	-	-	-	+/-	+/-
VM1	Сетевая карта 2	fe:fd:de:ad:ff:af	fe:fa:de:af:ff:ff	Ethernet II	0x800	-	+/-	+/-
VM1	Сетевая карта n	fe:fd:de:ad:ff:af	-	802.3 SNAP	0x800	-	+/-	+/-

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ защиты компьютерной системы от несанкционированного доступа к информации, реализуемый на уровне аппаратной платформы посредством механизмов виртуализации, включающий

предварительную подготовку аппаратной платформы, состоящую из

нейтрализации устройств аппаратной платформы компьютерной системы, не участвующих в обработке, хранении и передаче информации или представляющих угрозу безопасности информации,

устранения избыточности исполняемого кода микропрограммного кода аппаратной платформы,

устранения избыточности исполняемого кода привилегированных режимов функционирования ап-

паратной платформы компьютерной системы и его защита от модификации;

доверенную загрузку аппаратной платформы компьютерной системы;

доверенную загрузку системы защиты информации;

обеспечение защиты микропрограммного кода аппаратной платформы от анализа;

обеспечение защиты исполняемого кода системы защиты информации от анализа;

запрет обновления микропрограммного кода аппаратной платформы, в том числе удаленного;

очистку областей памяти, содержащих данные системы защиты информации и виртуальных машин в устройствах хранения, перед их выделением или повторным использованием;

очистку областей оперативной памяти аппаратной платформы компьютерной системы перед их выделением или повторным использованием;

реализацию особенностей архитектуры СЗИ;

изоляцию виртуальных машин;

реализацию особенностей передачи информации между виртуальными машинами в компьютерной системе;

эмуляцию аппаратных устройств компьютерной системы;

самотестирование механизмов защиты системы защиты информации;

восстановление безопасного состояния компьютерной системы;

определение субъектов и объектов доступа на уровне аппаратной платформы;

обработку системой защиты информации запросов виртуальной машины на доступ к физическим аппаратным устройствам компьютерной системы в следующем порядке:

виртуальная машина осуществляет запрос на доступ к физическим аппаратным устройствам на основе предоставляемых виртуальных ресурсов,

система защиты информации осуществляет сбор данных или параметров, содержащихся в запросе виртуальной машины,

система защиты информации на основании собранных данных или параметров и в соответствии с правилами разграничения доступа субъектов доступа к объектам доступа осуществляет проверку правомочности запроса,

при положительном результате проверки система защиты информации преобразует данные или параметры виртуальных вычислительных ресурсов в данные или параметры физических вычислительных ресурсов и передает преобразованный запрос соответствующему физическому аппаратному устройству, а при отрицательном результате проверки запрос отклоняется;

обработку системой защиты информации запросов от физических аппаратных устройств компьютерной системы на доступ к виртуальной машине в следующем порядке:

физические аппаратные устройства компьютерной системы осуществляют запрос на доступ к виртуальным вычислительным ресурсам на основе параметров физических вычислительных ресурсов,

система защиты информации осуществляет сбор данных или параметров, в запросах от физических аппаратных устройств, система защиты информации на основании собранных данных и в соответствии с правилами распределения доступа субъектов доступа к объектам доступа осуществляет проверку правомочности запроса,

при положительном результате проверки система защиты информации преобразует данные или параметры физических вычислительных ресурсов компьютерной системы в данных или параметров виртуальных вычислительных ресурсов и передает преобразованный запрос от физического аппаратного устройства компьютерной системы виртуальной машине, а при отрицательном результате проверки запрос отклоняется;

управление конфигурацией аппаратных средств компьютерной системы при запуске компьютерной системы, реализующее

определение системой защиты информации фактического состава всех аппаратных устройств, а также параметров их функционирования,

первичную проверку соответствия фактического состава всех аппаратных устройств компьютерной системы, включая периферийные устройства, списку аппаратных устройств, разрешенных системой защиты информации для использования в составе компьютерной системы, а также соответствия параметров, выявленных в компьютерной системе физических аппаратных устройств, разрешенным параметрам, установленным системой защиты информации для данного состава аппаратных устройств,

установление для каждой роли, предусматриваемой системой защиты информации, списка разрешенных для использования в рамках данной роли физических аппаратных устройств,

блокирование компьютерной системы при выявлении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных системой защиты информации к использованию в составе компьютерной системы для ролей пользователей и администраторов,

блокирование компьютерной системы при несоответствии параметров выявленных физических аппаратных устройств разрешенным параметрам, установленным системой защиты информации для данного состава аппаратных устройств компьютерной системы для ролей пользователей и администраторов;

управление конфигурацией аппаратных средств компьютерной системы при работе компьютерной

системы, обеспечивающее эшелонированную защиту от несанкционированного изменения конфигурации аппаратных средств компьютерной системы, от создания скрытых каналов несанкционированного доступа, как к вычислительным ресурсам компьютерной системы, так и к программной среде виртуальной машины и к пользовательским обрабатываемым данным, подлежащим защите от несанкционированного доступа к информации, и основанное на

периодической проверке состава аппаратных средств компьютерной системы и параметров их функционирования,

непрерывном анализе запросов от физических аппаратных устройств компьютерной системы на доступ к вычислительным ресурсам компьютерной системы, в том числе связанным с функционированием виртуальной машины;

управление конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в режиме обслуживания, реализующее

осуществление непрерывного контроля системой защиты информации параметров функционирования всех аппаратных устройств компьютерной системы, а также проверки соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защиты информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

возможность изменения списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы и списка аппаратных устройств, разрешенных для каждой роли, предусматриваемой системой защиты информации;

управление конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в режиме аудита, реализующее

осуществление системой защиты информации непрерывного контроля параметров функционирования всех аппаратных устройств компьютерной системы, а также проверку соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защиты информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

отключение аппаратных устройств и блокирование работы компьютерной системы при подключении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

блокирование работы компьютерной системы со стороны системы защиты информации при изменении параметров функционирования аппаратных устройств;

управление конфигурацией аппаратных средств компьютерной системы при работе компьютерной системы в эксплуатационном режиме, реализующее

осуществление системой защиты информации непрерывного контроля параметров функционирования всех аппаратных устройств компьютерной системы, а также проверку соответствия параметров физических устройств разрешенным параметрам, установленным системой защиты информации для конкретного типа устройств,

поддержку в данных управления системы защиты информации списка аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

поддержку в данных управления системы защиты информации списка аппаратных устройств компьютерной системы, разрешенных для каждой роли, предусматриваемой системой защиты информации,

отключение аппаратных устройств и блокирование работы компьютерной системы при подключении аппаратного устройства, не находящегося в списке аппаратных устройств, разрешенных к использованию в составе компьютерной системы,

блокирование работы компьютерной системы со стороны системы защиты информации при изменении параметров функционирования аппаратных устройств;

предоставление доступа пользователям к ресурсам компьютерной системы или к виртуальным машинам только через роли с уникальными идентификаторами, присваиваемыми по результатам идентификации и аутентификации пользователя;

однозначный запрет на запрос доступа любого не идентифицированного субъекта доступа к любым объектам доступа,

запрет на любые запросы на прямой доступ между физическими аппаратными устройствами или шинами компьютерной системы, кроме устройств, сертифицированных по требованиям защиты информации государственными органами страны применения компьютерной системы, и виртуальными машинами;

конфигурирование защиты оперативной памяти с помощью системы защиты информации от пря-

мого доступа со стороны аппаратных устройств компьютерной системы, а именно

получение из аппаратного устройства системой защиты информации списка и параметров разрешенных устройств компьютерной системы,

формирование системой защиты информации списка разрешенных к использованию в составе компьютерной системы устройств с возможностью прямого доступа к памяти,

получение системой защиты информации параметров прямого доступа к памяти от устройств, разрешенных к использованию в составе компьютерной системы,

конфигурирование системой защиты информации защиты с помощью полученных параметров прямого доступа к оперативной памяти от устройств, разрешенных к использованию в составе компьютерной системы;

защиту оперативной памяти компьютерной системы от прямого доступа со стороны аппаратных устройств компьютерной системы, обеспечиваемую системой защиты информации и включающую

генерацию запросов прямого доступа к оперативной памяти от физических аппаратных устройств компьютерной системы,

сбор системой защиты информации данных или параметров, содержащихся в запросах прямого доступа к оперативной памяти от аппаратных устройств,

осуществление проверки системой защиты информации собранных параметров запроса в соответствии с матрицей доступа при соответствии параметров, содержащихся в запросе, параметрам прямого доступа к памяти от устройств, разрешенных к использованию в составе компьютерной системы,

выполнение разрешения запроса, в противном случае осуществление блокировки запроса,

регистрацию системой защиты информации события блокировки запроса в журнале регистрации событий;

разграничение доступа к внешним носителям информации или от внешних носителей информации, включающее

разрешение взаимодействия с внешним накопителем информации только одной виртуальной машине, при этом внешний накопитель информации становится недоступен для взаимодействия с другими виртуальными машинами,

последовательное использование внешнего накопителя информации виртуальными машинами при обмене информацией между виртуальными машинами,

обеспечение доступа нескольких виртуальных машин к совместно используемому накопителю информации в режиме только чтение;

осуществление системой защиты информации фильтрации сетевого трафика по каждому протоколу сетевого взаимодействия в соответствии с матрицами доступа как при запросах, исходящих от виртуальной машины, так и при запросах, исходящих от физической сетевой карты, с учетом проверки типа запроса, поступившего от виртуальной машины, на его соответствие правилам разграничения доступа, установленным для уровней модели OSI или для соответствующих им протоколов, а также с учетом проверки данных, содержащихся в запросе виртуальной машины, на их соответствие атрибутам доступа, установленным системой защиты информации,

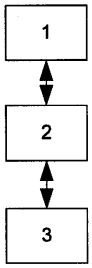
осуществление системой защиты информации регистрации событий во всех режимах работы, для каждого регистрируемого события в журнале регистрации событий сохраняется следующая информация: о дате и времени события, субъекте доступа, вызывавшем регистрируемое событие, типе события при регистрации события, связанного с доступом, также сохраняется информация об объекте и типе доступа, успешности осуществления события.

2. Устройство защиты компьютерной системы от несанкционированного доступа, включающее систему защиты информации, включающую подключенные к компьютерной шине контроллер и память, содержащую программные инструкции, обеспечивающие выполнение этапов способа по п.1, гипервизор первого типа с подсистемой запуска, подсистемой разграничения доступа, подсистемой администрирования и подсистемой регистрации событий, реализуемые на базе одного или нескольких центральных процессоров, а также чипсет, память, компьютерные шины, накопитель на жестком магнитном диске, твердотельный накопитель, USB-флэш накопитель, клавиатуру, мышь, оптический диск, сетевую карту, видеокарту, монитор, принтер, сканер, многофункциональное устройство.

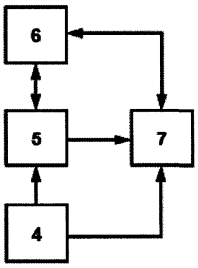
3. Устройство по п.2, отличающееся тем, что оно может быть выполнено в защищенном исполнении.

4. Устройство по п.2, отличающееся тем, что в качестве компьютерных шин могут быть использованы PCI, PCIExpress, SMBus, USB, ATA, SATA, PS/2, SCSI, SAS, FibreChannel, InfiniBand, I2C, SPI, FireWire, DMI, HyperTransport, Thunderbolt.

5. Устройство по п.2, отличающееся тем, что в устройстве могут быть использованы CD/DVD/Blu-ray оптические диски.



Фиг. 1



Фиг. 2

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2