ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56938— 2016

Защита информации

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

Общие положения

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2016, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Объекты защиты 3
5 Угрозы безопасности, обусловленные использованием технологий виртуализации 4
5.1 Угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети 4
5.2 Угрозы атаки на виртуальные каналы передачи 4
5.3 Угрозы атаки на гипервизор из виртуальной машины и/или физической сети 4
5.4 Угрозы атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети . . 4
5.5 Угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети . . . 5
5.6 Угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети . . . 5
5.7 Угрозы атаки на систему хранения данных из виртуальной и/или физической сети 5
5.8 Угрозы выхода процесса за пределы виртуальной машины 5
5.9 Угрозы несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение 5
5.10 Угрозы нарушения изоляции пользовательских данных внутри виртуальной машины 5
5.11 Угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия 6
5.12 Угрозы перехвата управления гипервизором 6
5.13 Угрозы перехвата управления средой виртуализации 6
5.14 Угрозы неконтролируемого роста числа виртуальных машин 6
5.15 Угрозы неконтролируемого роста числа зарезервированных вычислительных ресурсов 6
5.16 Угрозы нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин 6
5.17 Угрозы несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации 7
5.18 Угрозы ошибок обновления гипервизора 7
6 Особенности защиты информации при использовании технологий виртуализации 7
6.1 Защита средств создания и управления виртуальной инфраструктурой 7
6.2 Защита виртуальных вычислительных систем 10
6.3 Защита виртуальных систем хранения данных 11
6.4 Защита виртуальных каналов передачи данных 12
6.5 Защита отдельных виртуальных устройств обработки, хранения и передачи данных 13
6.6 Защита виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации 14
Приложение А (справочное) Схема взаимосвязи терминов, применяемых в области виртуализации . 15
Приложение Б (справочное) Типовая структура информационной системы, построенной с использованием технологий виртуализации 16
Приложение В (справочное) Сводные данные об угрозах и мерах защиты информации, обрабатываемой с помощью технологий виртуализации 17

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

Общие положения

Information security. protection. Information security with virtualization technology. General

Дата введения — 2017—06—01

1 Область применения

Настоящий стандарт устанавливает требования по защите информации, обрабатываемой с использованием технологий виртуализации.

В настоящем стандарте рассматриваются только угрозы безопасности и меры защиты информации, обрабатываемой с помощью технологий виртуализации. Меры защиты информации, изложенные в настоящем стандарте, предназначены для применения только в случае обработки информации с использованием технологий виртуализации. Кроме мер защиты информации, изложенных в настоящем стандарте, для обеспечения требуемого уровня защищенности информации, обрабатываемой в информационных системах, построенных с использованием технологий виртуализации, необходимо дополнительно применять меры защиты информации, общеупотребимые для любых автоматизированных систем в защищенном исполнении.

Настоящий стандарт применяют совместно с другими стандартами, устанавливающими характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг в области защиты информации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 27000, ГОСТ 34.003, ГОСТ Р 50922, ГОСТ Р 53114, а также следующие термины с соответствующими определениями:

3.1 **виртуализация:** Группа технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

3.2 **виртуализация программного обеспечения (виртуализация программ):** Технология создания изолированной программной среды (контейнера) со специфическим набором компонентов имитируемой операционной системы, обеспечивающим работу отдельных программ.

3.3 **виртуализация аппаратного обеспечения, виртуализация вычислительных систем:** Технология создания изолированной программной среды (контейнера) со специфическим набором компонентов имитируемого микропрограммного и аппаратного обеспечения, обеспечивающим работу отдельных операционных систем.

3.4 **виртуальная машина;** ВМ: Виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать программное обеспечение и пользовательские данные.

Примечания

1 Виртуальная машина является простейшей формой виртуальных вычислительных систем.

2 Несколько виртуальных машин, объединенных для решения определенных задач, также составляют виртуальную вычислительную систему. В этом случае виртуальная машина выступает в качестве базового элемента при построении (сложных) виртуальных вычислительных систем.

3 Виртуальная машина скрывает настоящую реализацию находящихся в ней процессов и объектов от процессов, запущенных вне виртуальной машины. Верно и обратное — виртуальная машина скрывает настоящую реализацию находящихся вне ее процессов и объектов от процессов, запущенных внутри виртуальной машины.

3.5 **гостевая операционная система:** Операционная система, установленная в виртуальной машине.

3.6 **образ виртуальной машины:** Файл (файлы), содержащий(ие) информацию о конфигурации, настройках и состоянии виртуальной машины, а также хранящиеся в ней программы и данные.

3.7 **виртуализация систем хранения данных:** Технология построения изолированного пространства хранения данных с единым интерфейсом управления на основе машинных накопителей информации, обеспечивающая получение необходимой информации посредством ее передачи по каналам передачи данных.

Примечание — Базовым элементом при построении (сложных) виртуальных систем хранения данных является виртуальный накопитель (виртуальный диск).

3.8 **виртуализация вычислительных сетей (виртуализация каналов передачи данных):** Технология объединения аппаратных и программных сетевых ресурсов и сетевых функций в едином программно администрируемом объекте для реализации их логического взаимодействия через дополнительные виртуальные сетевые ресурсы и функции.

3.9 **виртуальная вычислительная сеть (виртуальный канал передачи данных):** Вычислительная сеть, содержащая один или более виртуальных сетевых ресурсов и/или функций.

Примечание — Базовыми элементами при построении (сложных) виртуальных вычислительных сетей, как и других вычислительных сетей, являются сетевые ресурсы (оконечные и промежуточные узлы [вычислительной сети]) и сетевые функции (фильтрация, кодирование трафика и др.).

3.10 **аппаратная поддержка виртуализации:** Технология, реализованная в процессорах (чипсетах) компьютеров в виде инструкций (команд), служащая для улучшения технических характеристик информационных систем, построенных с использованием технологий виртуализации, и/или повышения безопасности объектов защиты таких систем.

3.11 **гипервизор [вычислительных систем] (монитор виртуальных машин):** Программа, создающая среду функционирования других программ (в том числе других гипервизоров) за счет имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Примечание — Различают гипервизор I типа, гипервизор II типа.

3.12 **хостовая операционная система:** Операционная система, в среде которой функционирует гипервизор.

3.13 **гипервизор I типа:** Гипервизор, устанавливаемый непосредственно на аппаратное обеспечение в качестве системного программного обеспечения.

3.14 **гипервизор II типа:** Гипервизор, устанавливаемый в среде хостовой операционной системы в качестве прикладного программного обеспечения.

3.15 **гипервизор систем хранения данных:** Программа, устанавливаемая непосредственно на аппаратное обеспечение в качестве системного программного обеспечения или в среде хостовой операционной системы в качестве прикладного программного обеспечения, выполняющая функции посредника между логическим и физическим адресными пространствами для обеспечения высокого уровня управления ресурсами хранения данных.

Примечание — Обеспечение наивысшего уровня управления всей совокупностью вычислительных ресурсов достигается за счет совместного использования гипервизора систем хранения данных и гипервизора I или II типа. При этом гипервизор систем хранения данных изменяет способы обработки запросов ввода/вывода гипервизорами I или II типа для повышения производительности, эффективности использования и управления ресурсами хранения данных.

3.16 **виртуальная инфраструктура:** Композиция иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств.

Примечания

1 Группа задействованных аппаратных средств и/или запущенных программ (процессов, потоков), используемых для реализации работы виртуальных устройств обработки, хранения и/или передачи данных, составляет периметр виртуальной инфраструктуры.

2 В виртуальной инфраструктуре различают по меньшей мере три уровня иерархии:

- на первом (нижнем) уровне иерархии (уровне оборудования) расположена аппаратная часть периметра виртуальной инфраструктуры — аппаратные средства, используемые для реализации технологий виртуализации, в том числе с реализованной в них аппаратной поддержкой виртуализации;
- на втором уровне иерархии (уровне виртуализации) расположены гипервизоры и порожденные ими объекты (виртуальные машины, виртуальные сервера, виртуальные процессоры, виртуальные диски, виртуальная память, виртуальное активное и пассивное сетевое оборудование, виртуальные средства защиты информации и др.);
- на третьем (верхнем) уровне иерархии (уровне управления) расположено средство централизованного управления гипервизорами в рамках одной виртуальной инфраструктуры — консоль управления виртуальной инфраструктурой.

3.17 **компонент виртуальной инфраструктуры:** Часть виртуальной инфраструктуры, выделенная по определенному признаку или совокупности признаков и рассматриваемая как единое целое.

Примечание — Схема взаимосвязи терминов приведена в приложении А.

4 Объекты защиты

Под термином «виртуализация» объединяется множество информационных технологий, призванных снижать затраты на разворачивание компьютерной сети организации, повышать отказоустойчивость применяемых серверных решений, а также достигать других преимуществ. Виртуализация представляет собой имитацию программного и/или аппаратного обеспечения, в среде (на базе) которого функционируют различные программы.

Виртуализацию проводят в отношении:

- программ;
- вычислительных систем;
- систем хранения данных;
- вычислительных сетей;
- памяти;
- данных.

При использовании технологий виртуализации создаются (виртуальные и виртуализованные) объекты доступа, подлежащие защите наравне с другими объектами информационных систем, в том

числе аппаратные средства информационных систем, используемые для реализации технологий виртуализации. К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);
- виртуальные вычислительные системы (ВМ, виртуальные сервера и др.);
- виртуальные системы хранения данных;
- виртуальные каналы передачи данных;
- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);
- виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;
- периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

Для защиты перечисленных объектов используют как виртуальные средства ЗИ и средства ЗИ, предназначенные для использования в среде виртуализации, являющиеся разновидностями средств ЗИ, так и другие виды средств ЗИ.

5 Угрозы безопасности, обусловленные использованием технологий виртуализации

Использование технологий виртуализации создает предпосылки для появления угроз безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Общий перечень угроз, дополнительно могущих возникать при использовании технологий виртуализации, включает угрозы, описанные далее.

5.1 Угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети

Данные угрозы появляются в связи с ограниченностью функциональных возможностей (наличием слабостей) активного и/или пассивного виртуального и/или физического сетевого оборудования, входящего в состав виртуальной инфраструктуры. На реализацию данных угроз прямое влияние оказывают: наличие уязвимостей программного и/или микропрограммного обеспечения указанного оборудования, наличие у него фиксированного сетевого адреса и другие параметры его настройки, возможность изменения алгоритма работы программного обеспечения (ПО) сетевого оборудования вредоносными программами.

5.2 Угрозы атаки на виртуальные каналы передачи

Данные угрозы связаны со слабостями технологий виртуализации, с помощью которых строят виртуальные каналы передачи данных (сетевых технологий виртуализации). Некорректное использование сетевых технологий виртуализации может обеспечивать возможность несанкционированного перехвата трафика сетевых узлов, недоступных с помощью других сетевых технологий.

5.3 Угрозы атаки на гипервизор из виртуальной машины и/или физической сети

Данные угрозы связаны со слабостями гипервизора, а также слабостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данных угроз приводит к недоступности всей (если гипервизор — один) или части (если используют несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры.

5.4 Угрозы атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети

Данные угрозы связаны с наличием у гипервизоров сетевых программных интерфейсов, предназначенных для удаленного управления составом и конфигурацией виртуальных устройств, созданных

(создаваемых) данными гипервизорами, что позволяет злоумышленнику удаленно осуществлять несанкционированный доступ (НСД) к этим устройствам с помощью сетевых технологий из виртуальной и/или физической сети. Возможный ущерб может быть связан с доступностью данных виртуальных устройств.

5.5 Угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети

Данные угрозы появляются в связи с наличием у создаваемых ВМ сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами как с помощью стандартных сетевых технологий, так и с помощью сетевых технологий виртуализации.

5.6 Угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети

Данные угрозы появляются в связи с наличием у создаваемых ВМ сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами как с помощью стандартных сетевых технологий, так и с помощью сетевых технологий виртуализации.

5.7 Угрозы атаки на систему хранения данных из виртуальной и/или физической сети

Угрозы данного типа реализуются за счет слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и/или виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны со сложностью алгоритмов обеспечения согласованности при реализации процессов распределения информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства.

5.8 Угрозы выхода процесса за пределы виртуальной машины

Данные угрозы связаны с наличием слабостей ПО гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ. В случае запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора, последний, как и запущенные в нем средства защиты, не способен выполнять функции безопасности в отношении программ, функционирующих в собственном гипервизоре.

5.9 Угрозы несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

Данные угрозы связаны с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения программного кода не только защищаемой информации и обрабатывающих ее программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от НСД со стороны вредоносной программы, функционирующей внутри ВМ. В случае осуществления НСД со стороны вредоносной программы, функционирующей внутри ВМ, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной ВМ, вредоносная программа может не только нарушать целостность программного кода своей и/или других ВМ, функционирующих под управлением того же гипервизора, но и изменять параметры его (их) настройки.

5.10 Угрозы нарушения изоляции пользовательских данных внутри виртуальной машины

Данные угрозы связаны с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри ВМ, от НСД со стороны вредоносного ПО, функционирующего вне ВМ. В результате реализации данной угрозы может быть нарушена безопасность пользовательских данных программ, функционирующих внутри ВМ.

5.11 Угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия

Данная угроза связана с наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между ее уровнями. Реализуемость данной угрозы напрямую зависит от качества реализации как самих протоколов, так и механизмов их взаимодействия.

5.12 Угрозы перехвата управления гипервизором

Угрозы перехвата управления гипервизором связаны с наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, с возможностью НСД к данной консоли. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов, зарезервированных и управляемых гипервизором.

5.13 Угрозы перехвата управления средой виртуализации

Угрозы перехвата управления средой виртуализации связаны с наличием у консоли управления виртуальной инфраструктурой, реализуемой в рамках одной из ВМ, а также у управляемых с ее помощью гипервизоров программных интерфейсов взаимодействия с другими программами и, как следствие, с возможностью НСД к указанному ПО уровня управления. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов виртуальной инфраструктуры.

5.14 Угрозы неконтролируемого роста числа виртуальных машин

Данные угрозы связаны с наличием ограниченности объема дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания ВМ, в связи с чем возможно случайное или несанкционированное преднамеренное создание множества ВМ. В результате реализации данной угрозы может быть ограничена или нарушена доступность виртуальных ресурсов для конечных пользователей облачных услуг.

5.15 Угрозы неконтролируемого роста числа зарезервированных вычислительных ресурсов

Данные угрозы связаны со слабостями ПО уровня управления виртуальной инфраструктурой, обеспечивающего выделение компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Реализация данной угрозы возможна за счет НСД к указанному ПО и из-за ошибок в его коде.

5.16 Угрозы нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин

Данные угрозы связаны с отсутствием в ПО виртуализации защитных механизмов, предотвращающих НСД к образам ВМ. В результате реализации данной угрозы могут быть нарушены конфиденциальность обрабатываемой с помощью данных ВМ защищаемой информации, целостность программ, установленных на ВМ, а также доступность ресурсов данных ВМ.

Кроме того, внедрение вредоносного ПО в образы ВМ, используемые в качестве шаблонов (эталонные образы), может быть использовано при создании ботнета в ходе подготовки к проведению атаки типа «отказ в облуживании». В этом случае может быть нарушена безопасность информации, обрабатываемой в других ВМ, сегментов виртуальной инфраструктуры или сторонних информационных систем.

Примечание — Под ботнетом понимают распределенную компьютерную сеть, создаваемую нарушителем путем внедрения специального вредоносного ПО в доступные, но не принадлежащие ему компьютеры и вычислительные системы (в основном — компьютеры, подключенные к сети Интернет), предназначенную для согласованного одновременного проведения распределенной компьютерной атаки на целевую компьютерную систему (компьютер-жертву).

5.17 Угрозы несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации

В связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Следовательно, в подавляющем большинстве случаев последовательное чтение данных с отдельно взятого носителя не позволяет нарушать конфиденциальность защищаемой информации, хранимой в системах хранения данных. В связи с этим меры по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях, практически не применяют.

Тем не менее применение ПО и информационных технологий по обработке распределенной информации позволяет восстанавливать целостность распределенных файлов, содержащих защищаемую информацию, и тем самым нарушать ее конфиденциальность.

5.18 Угрозы ошибок обновления гипервизора

Данные угрозы связаны с зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или ее части, если используют более одного гипервизора) от работоспособности гипервизора. Некорректно обновленный гипервизор может привести к дискредитации функционирующих на его основе защитных механизмов, предотвращающих НСД к образам ВМ. Возможный ущерб может быть связан с нарушением конфиденциальности обрабатываемой с помощью данных ВМ защищаемой информации, целостности программ и доступности ресурсов данных ВМ.

Примечание — Ошибками обновления гипервизора являются:

- сбои в процессе его обновления;
- обновления, в ходе которых внедряются новые ошибки в код гипервизора;
- обновления, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования;
- другие инциденты безопасности информации, происходящие в процессе обновления гипервизора.

6 Особенности защиты информации при использовании технологий виртуализации

Защита информации, обрабатываемой в информационных системах (ИС), построенных с использованием технологий виртуализации, обеспечивается выполнением требований к мерам ЗИ (типовая структура такой системы представлена в приложении Б). В целом меры ЗИ аналогичны мерам, применяемым в ИС, не использующих технологию виртуализации. Далее приведены специфические меры ЗИ, дополнительно применяемые при использовании технологий виртуализации.

Меры ЗИ разделены на несколько групп в зависимости от объекта защиты.

В связи с тем, что защищенность информации определяется требованиями, варьируемыми по уровню и глубине в зависимости от класса защищенности ИС, построенных в том числе с помощью технологий виртуализации, в настоящем стандарте для каждого объекта защиты приводится набор мер ЗИ, соответствующий высшему классу защищенности от НСД.

Меры ЗИ следует выбирать с учетом угроз безопасности, особенностей использования объектов защиты и действующего законодательства в области ЗИ. Сводные данные об угрозах и мерах ЗИ, обрабатываемой с помощью технологий виртуализации, приведены в приложении В.

6.1 Защита средств создания и управления виртуальной инфраструктурой

Мерами защиты средств создания и управления виртуальной инфраструктурой являются:

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;
- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к консолям управления параметрами аппаратного обеспечения;

- контроль ввода (вывода) информации в/из виртуальную(ой) инфраструктуру(ы);

- контроль ввода (вывода) информации в/из ИС;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВМ;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль запуска гипервизора и ВМ на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т. д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т. д.);

- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;

- контроль работоспособности дублирующих ключевых компонентов аппаратного обеспечения ИС;

- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВМ;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности микропрограммного обеспечения аппаратной части ИС;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровне виртуализации и оборудования;

- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- предотвращение задержки или прерывания выполнения в виртуальной инфраструктуре процессов с высоким приоритетом со стороны процессов с низким приоритетом;

- предотвращение задержки или прерывания выполнения процессов ВМ с высоким приоритетом со стороны процессов ВМ с низким приоритетом;

- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в загрузочных областях машинных носителей информации, подключенных к ИС;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВМ;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных систем;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВМ, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка оперативной памяти и файловой системы гипервизора и/или ВМ на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВМ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВМ;

- регистрация входа (выхода) субъектов доступа в/из хостовую(ой) и/или гостевые(х) операционные(х) системы (систем);

- регистрация запуска (завершения работы) гипервизора и/или ВМ, программ и процессов в гипервизоре и/или ВМ;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация и учет изменений в составе программной и аппаратной части ИС во время ее функционирования и/или в период ее аппаратного отключения;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;

- регистрация изменений состава и конфигурации ВМ;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВМ;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВМ;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;

- резервное копирование защищаемой информации в гипервизоре и/или ВМ, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВМ;

- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, обрабатываемых в виртуальной инфраструктуре, содержащих информацию ограниченного доступа,

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВМ;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;

- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации,

- управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО;

- управление установкой (инсталляцией) компонентов ПО, входящего в состав виртуальной инфраструктуры, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е).

6.2 Защита виртуальных вычислительных систем

Мерами защиты виртуальных вычислительных систем являются:

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВМ;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль запуска гипервизора и ВМ на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т. д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т. д.);

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВМ;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВМ;

- контроль целостности файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- предотвращение задержки или прерывания выполнения процессов ВМ с высоким приоритетом со стороны процессов ВМ с низким приоритетом;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВМ;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных систем;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВМ, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем,

- проверка оперативной памяти и файловой системы гипервизора и/или ВМ на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВМ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВМ;

- регистрация входа (выхода) субъектов доступа в/из хостовую(ой) и/или гостевые(х) операционные(х) системы (систем);

- регистрация запуска (завершения работы) гипервизора и/или ВМ, программ и процессов в гипервизоре и/или ВМ;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации ВМ;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВМ;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВМ;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервное копирование защищаемой информации в гипервизоре и/или ВМ, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВМ;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВМ;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов-образов ВМ, в которых обрабатывалась информация ограниченного доступа;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);

- шифрование файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

6.3 Защита виртуальных систем хранения данных

Мерами защиты виртуальных систем хранения данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль ввода (вывода) информации в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры;

- контроль доступа субъектов доступа к средствам конфигурирования системы хранения данных, входящей в состав виртуальной инфраструктуры;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль работоспособности (изношенности) машинных носителей информации, подключенных к виртуальной инфраструктуре, переход на дублирующие при необходимости;

- контроль целостности данных, хранимых на машинных носителях информации, подключенных к виртуальной инфраструктуре;

- контроль целостности файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- обеспечение доверенных (защищенных) канала, маршрута передачи данных в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- проверка наличия вредоносных программ в операционной среде гипервизора системы хранения данных;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВМ, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- разделение данных в зависимости от уровня конфиденциальности обрабатываемой информации между компонентами системы хранения данных, отдельными машинными носителями информации, входящими в состав виртуальной инфраструктуры, логическими дисками или между папками файлов;

- размещение системы хранения данных в защищенном сегменте информационной системы;

- регистрация изменений прав доступа к информации, хранящейся в системе хранения данных, входящей в состав виртуальной инфраструктуры;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному и физическому аппаратному обеспечению системы хранения данных;

- регистрация изменений состава и конфигурации виртуального и физического аппаратного обеспечения системы хранения данных;

- резервное копирование файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- управление доступом к аппаратному обеспечению системы хранения данных, контроль подключения (отключения) машинных носителей информации к/от виртуальной инфраструктуре(ы);

- шифрование файлов-образов виртуализованного ПО и ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

6.4 Защита виртуальных каналов передачи данных

Мерами защиты виртуальных каналов передачи данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;
- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;
- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;
- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;
- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;
- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;
- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;
- передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией ограниченного доступа, обрабатываемой в виртуальной инфраструктуре, при обмене информацией с иными ИС;
- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;
- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;
- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;
- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);
- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи гипервизора;
- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи хостовой операционной системы.

6.5 Защита отдельных виртуальных устройств обработки, хранения и передачи данных

Мерами защиты виртуальных устройств обработки, хранения и передачи данных являются:
- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;
- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;
- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;
- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;
- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;
- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;
- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВМ;
- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;
- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;
- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;
- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;
- разделение физических ресурсов между компонентами виртуальной инфраструктуры в зависимости от уровня конфиденциальности обрабатываемой информации;
- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;
- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;
- регистрация и учет изменений в составе программной и аппаратной частей ИС во время ее функционирования и/или в период ее аппаратного отключения;
- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;
- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;
- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВМ;
- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;
- резервное копирование защищаемой информации, хранимой на физических и виртуальных носителях информации;
- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;
- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;
- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;
- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации.

6.6 Защита виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации

Мерами защиты виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации, являются:
- автоматическое восстановление всех функций средств ЗИ, входящих в состав ИС;
- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;
- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;
- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;
- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;
- обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами ЗИ (функциями безопасности средств ЗИ).

Приложение А
(справочное)

Схема взаимосвязи терминов, применяемых в области виртуализации

Схема взаимосвязи терминов, применяемых в области виртуализации, представлена на рисунке А.1.

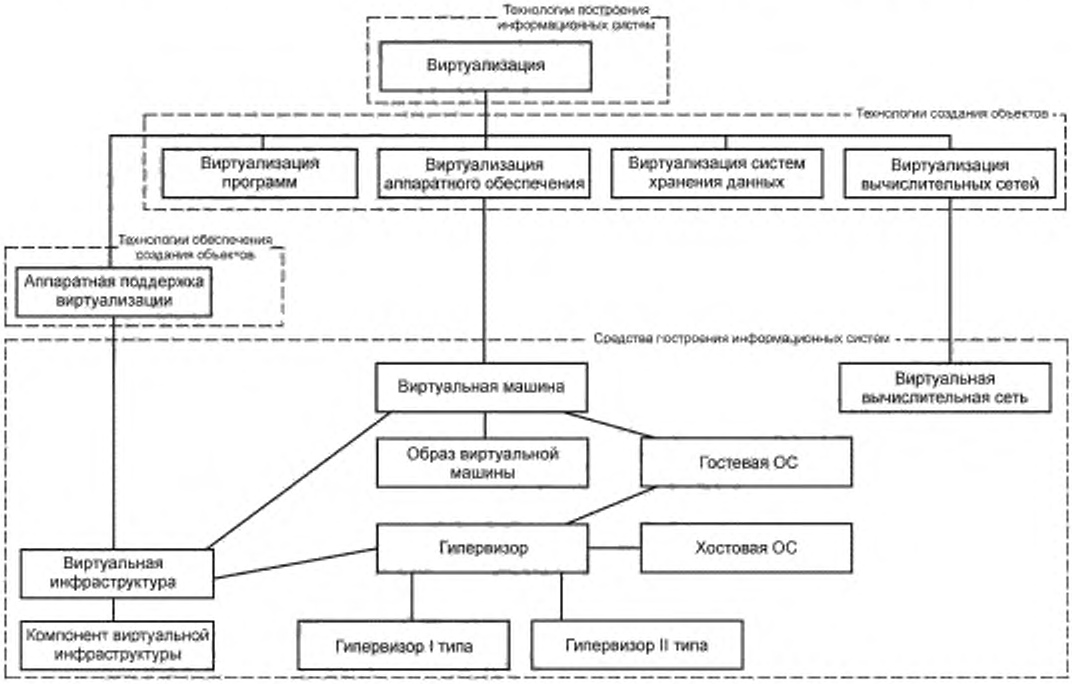
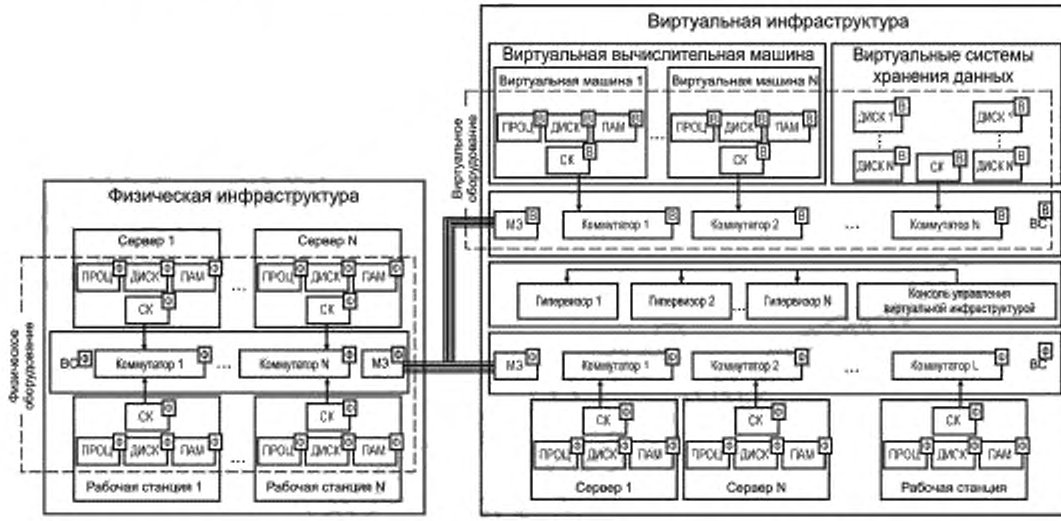


Рисунок А.1

Приложение Б
(справочное)

Типовая структура информационной системы, построенной с использованием технологий виртуализации

Типовая структура информационной системы, построенной с использованием технологий виртуализации, представлена на рисунке Б.1.



Условные обозначения:

ПРОЦ – физический процессор;
ПАМ – физическая память;
ДИСК – физический накопитель;
СК – физическая сетевая карта;
МЭ – физический межсетевой экран;
ВС – физическая вычислительная сеть;

ПРОЦ – виртуальный процессор;
ПАМ – виртуальная память;
ДИСК – виртуальный накопитель;
СК – виртуальная сетевая карта;
МЭ – виртуальный межсетевой экран;
ВС – виртуальная вычислительная сеть;

Коммутатор – виртуальный коммутатор;
Коммутатор – физический коммутатор;
– объекты, подлежащие защите при использовании технологий виртуализации;
– канал передачи данных

Рисунок Б.1

Приложение В
(справочное)

Сводные данные об угрозах и мерах защиты информации, обрабатываемой с помощью технологий виртуализации

В разделе 5 настоящего стандарта приведена единая номенклатура угроз, которые могут быть вызваны применением технологий виртуализации. Однако на наличие угроз оказывают влияние особенности обработки информации с помощью различных объектов защиты (перечисленных в разделе 4 настоящего стандарта). Обобщенная схема зависимости наличия угроз от используемых объектов защиты приведена в таблице В.1.

Таблица В.1

Угроза безопасности информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети		+			+	+
Угрозы атаки на виртуальные каналы передачи				+		
Угрозы атаки на гипервизор из ВМ и/или физической сети	+					
Угрозы атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети					+	+
Угрозы атаки на защищаемые ВМ из виртуальной и/или физической сети		+				+
Угрозы атаки на защищаемые ВМ со стороны других ВМ		+				+
Угрозы атаки на систему хранения данных из виртуальной и/или физической сети			+			
Угроза выхода процесса за пределы ВМ	+	+				
Угроза НСД к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение		+			+	
Угроза нарушения изоляции пользовательских данных внутри ВМ		+				

Окончание таблицы В.1

Угроза безопасности информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	+	+	+			+
Угроза перехвата управления гипервизором	+					
Угроза перехвата управления средой виртуализации	+	+				
Угроза неконтролируемого роста числа ВМ	+					
Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	+					
Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы ВМ		+	+			
Угроза НСД к хранимой в виртуальном пространстве информации ограниченного доступа					+	
Угроза ошибки обновления гипервизора	+					

В подразделах 6.1—6.6 настоящего стандарта определены номенклатуры мер защиты информации, реализация которых необходима для нейтрализации угроз, приведенных в таблице В.1. Обобщенная схема зависимости подлежащих к применению мер защиты информации от используемых объектов защиты приведена в таблице В.2.

Таблица В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Автоматическое восстановление всех функций средств ЗИ, входящих в состав ИС						+
Автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов			+			

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора	+			+		
Блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации	+	+	+	+	+	
Выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов	+			+		
Защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации	+	+	+	+	+	+
Защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа	+	+	+	+	+	+
Идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры	+	+	+	+	+	+
Идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к консолям управления параметрами аппаратного обеспечения	+					
Контроль ввода (вывода) информации в/из виртуальной инфраструктуре(ы)	+					
Контроль ввода (вывода) информации в/из ИС	+					
Контроль ввода (вывода) информации в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры			+			
Контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора	+	+				

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы	+	+				
Контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения	+				+	
Контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВМ	+	+				
Контроль доступа субъектов доступа к средствам конфигурирования системы хранения данных, входящей в состав виртуальной инфраструктуры			+			
Контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем	+	+				
Контроль доступа субъектов доступа к файлам-образам ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем		+	+		+	
Контроль запуска гипервизора и ВМ на основе заданных критериев обеспечения безопасности информации (режима запуска, типа используемого носителя и т. д.)	+	+				
Контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности информации (режима запуска, типа используемого носителя и т. д.)	+	+				
Контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.	+			+		
Контроль работоспособности (изношенности) машинных носителей информации, подключенных к виртуальной инфраструктуре, переход на дублирующие при необходимости			+			

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Контроль работоспособности дублирующих ключевых компонентов аппаратного обеспечения ИС	+					
Контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры	+				+	
Контроль целостности данных, хранимых на машинных носителях информации, подключенных к виртуальной инфраструктуре			+			
Контроль целостности компонентов, критически важных для функционирования гипервизора и ВМ	+	+				
Контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем	+	+				
Контроль целостности микропрограммного обеспечения аппаратной части ИС	+					
Контроль целостности файлов, содержащих настройки ВМ		+			+	
Контроль целостности файлов-образов ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем		+	+			
Мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения	+			+	+	
Обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования	+				+	+
Обеспечение доверенных (защищенных) канала, маршрута передачи данных в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры				+		
Обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами ЗИ (функциями безопасности средств ЗИ)						+

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы	+			+		
Обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов	+		+	+	+	
Отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы	+			+	+	
Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией ограниченного доступа, обрабатываемой в виртуальной инфраструктуре, при обмене информацией с иными ИС				+		
Предотвращение задержки или прерывания выполнения в виртуальной инфраструктуре процессов с высоким приоритетом со стороны процессов с низким приоритетом	+					
Предотвращение задержки или прерывания выполнения процессов ВМ с высоким приоритетом со стороны процессов ВМ с низким приоритетом	+	+				
Применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры	+				+	
Проверка наличия вредоносных программ в загрузочных областях машинных носителей информации, подключенных к ИС	+					
Проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения	+	+			+	
Проверка наличия вредоносных программ в операционной среде гипервизора системы хранения данных			+			

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВМ	+	+				
Проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных системе	+	+				
Проверка наличия вредоносных программ в файлах-образах ВМ, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем	+	+	+			
Проверка оперативной памяти и файловой системы гипервизора и/или ВМ на наличие вредоносных программ	+	+				
Проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ	+	+				
Разделение данных в зависимости от уровня конфиденциальности обрабатываемой информации между компонентами системы хранения данных, отдельными машинными носителями информации, входящими в состав виртуальной системы, логическими дисками или между папками файлов			+			
Разделение физических ресурсов между компонентами виртуальной инфраструктуры в зависимости от уровня конфиденциальности обрабатываемой информации					+	
Размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении	+	+			+	
Размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВМ	+	+				
Размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах	+	+				
Размещение системы хранения данных в защищенном сегменте ИС			+			

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры	+				+	
Регистрация входа (выхода) субъектов доступа в/из гипервизор(ра) и/или ВМ	+	+				
Регистрация входа (выхода) субъектов доступа в/из хостовую(ой) и/или гостевую(ых) операционные(ых) системы (систем)	+	+				
Регистрация запуска (завершения работы) гипервизора и/или ВМ, программ и процессов в гипервизоре и/или ВМ	+	+				
Регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах	+	+				
Регистрация и учет изменений в составе программной и аппаратной части ИС во время ее функционирования и/или в период ее аппаратного отключения	+				+	
Регистрация изменений прав доступа к информации, хранящейся в системе хранения данных, входящей в состав виртуальной инфраструктуры			+			
Регистрация изменений прав доступа к файлам-образам ВМ, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем		+	+			
Регистрация изменений правил доступа к виртуальному аппаратному обеспечению	+	+			+	
Регистрация изменений правил доступа к виртуальному и физическому аппаратному обеспечению системы хранения данных			+			
Регистрация изменений состава и конфигурации виртуального аппаратного обеспечения	+				+	
Регистрация изменений состава и конфигурации виртуального и физического аппаратного обеспечения системы хранения данных			+			

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Регистрация изменений состава и конфигурации ВМ	+	+				
Регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВМ	+	+			+	
Регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах	+	+			+	
Регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВМ	+	+				
Регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах	+	+				
Резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора	+			+		
Резервное копирование защищаемой информации в гипервизоре и/или ВМ, хранимой на физических и/или виртуальных носителях информации	+	+				
Резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации	+	+				
Резервное копирование защищаемой информации, хранимой на физических и виртуальных носителях информации					+	
Резервное копирование файлов-образов машин, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем		+	+			
Резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВМ	+	+				

Продолжение таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Своевременное обнаружение отказов компонентов виртуальной инфраструктуры	+				+	
Создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации	+	+	+	+	+	
Обнуление резервируемого под выделение виртуальных ресурсов хранения данных для нового пользователя (организации) адресного пространства, в котором хранилась информация ограниченного доступа других пользователей (организаций)			+			
Стирание остаточной информации, образующейся после удаления данных, обрабатываемых в виртуальной инфраструктуре, содержащих информацию ограниченного доступа	+					
Стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВМ	+	+				
Стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах	+	+				
Стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуального аппаратного обеспечения	+				+	
Стирание остаточной информации, образующейся после удаления файлов-образов ВМ, в которых обрабатывалась информация ограниченного доступа		+				
Управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации	+				+	
Управление доступом к аппаратному обеспечению системы хранения данных, контроль подключения (отключения) машинных носителей информации к/от виртуальной инфраструктуре(ы)			+			

Окончание таблицы В.2

Мера защиты информации	Объект защиты					
	Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства обработки, хранения и передачи данных	Виртуальное средство ЗИ и средство ЗИ, предназначенное для использования в среде виртуализации
Управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО	+					
Управление установкой (инсталляцией) компонентов ПО, входящего в состав виртуальной инфраструктуры, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО	+					
Установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов	+	+				
Фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования	+			+		
Фильтрация сетевого трафика от/к каждой гостевой операционной системы(е)	+	+		+		
Шифрование данных, хранимых в виртуальной инфраструктуре и содержащих информацию ограниченного доступа						
Шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи гипервизора				+		
Шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи хостовой операционной системы				+		
Шифрование файлов-образов ВМ, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа		+	+			

Примечания

1 Знак «+» обозначает, что мера защиты информации подлежит реализации для нейтрализации угроз безопасности конкретного объекта защиты.

2 Меры защиты информации, не обозначенные знаком «+», допускается применять дополнительно.

УДК 004.056:004.358:004.94:006.354 ОКС 35.020

Ключевые слова: защита информации, защита информации от несанкционированного доступа, технологии виртуализации, информационные системы

Редактор *Е.В. Яковлева*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 26.11.2018 Подписано в печать 06.12.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru