Общество с ограниченной ответственностью «Нума Технологии»

УТВЕРЖДЕН
643.АМБН.00021-01 90 01-ЛУ

Серверная доверенная виртуальная среда функционирования программных средств Numa vServer

Технические условия

643.АМБН.00021-01 90 01

Выписка

Подп. и дата	
Инв № дубл.	
Взамен инв. №	
Подп. и дата	
Инв № подл.	

2023

Литера

О ДОКУМЕНТЕ

Идентификация документа

Название документа	Технические условия. Выписка
Версия документа	Версия 1.1.0
Обозначение документа	643.АМБН.00021-01 90 01
Идентификация Изделия	Серверная доверенная виртуальная среда функционирования программных средств Numa vServer
Идентификация разработчика	ООО «НумаТех»

Настоящий документ является выпиской из документа «Технические условия» 643.АМБН.00021-01 90 01 для изделия «Серверная доверенная виртуальная среда функционирования программных средств Numa vServer» 643.АМБН.00021-01.

Настоящий документ содержит в себе следующие разделы оригинального документа:

- Аннотация;
- 1. Технические требования;
- 6. Условия транспортирования, хранения и эксплуатации;
- 7. Ограничение прав по использованию программного обеспечения;
- 8. Гарантии изготовителя;
- 9. Техническая поддержка;
- 10. Порядок получения Изделия при электронной поставке;
- 11. Указания по устранению уязвимостей и обновлению;
- Перечень сокращений;
- Приложение Б. Разрешение для базовых ролей пользователей Изделия;
- Приложение В. Перечень мер защиты информации, реализуемых Изделием;
- Приложение Г. Угрозы, которым противостоит Изделие (данные актуальны на 13.06.2023).

В документе сохранена оригинальная нумерация.

АННОТАЦИЯ

Настоящие технические условия (далее - ТУ) распространяются на Изделие серверная доверенная виртуальная среда функционирования программных средств Numa vServer 643.АМБН.00021-01 (далее – Изделие или Numa vServer или доверенная виртуальная среда Numa vServer), разработанное и изготавливаемое обществом с ограниченной ответственностью «Нума Технологии» (196084, г. Санкт-Петербург, ул. Цветочная, д. 18, литера А, оф. 424, лицензия ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации (регистрационной номер 1845 от 25.09.2018, действует бессрочно).

Изделие представляет собой гипервизор гибридного типа, предназначенный для создания защищенной виртуальной инфраструктуры, как на отдельном физическом сервере, так и на группе серверов, объединенных в кластер, включая территориально-распределенные конфигурации серверов, построенных на 64-х разрядных аппаратных платформах Intel или AMD с поддержкой технологии аппаратной виртуализации.

Изделие обеспечивает возможность:

- запуска и исполнения служебных (сервисных) и пользовательских виртуальных машин (далее – ВМ) под управлением операционных систем, предназначенных для использования на типовых СВТ, построенных с использованием процессоров и наборов системной логики (чипсетов) Intel или AMD для архитектуры x86-64 (операционные системы Microsoft Windows, Microsoft Windows Server, Linux, включая специализированные дистрибутивы отечественного производства, а также иные совместимые ОС);
- создания изолированных сред для работы с информацией различной степени конфиденциальности в рамках виртуальной инфраструктуры, обеспечивая, в том числе разделение аппаратных (физических) ресурсов серверного комплекса.

Изделие обеспечивает изоляцию ВМ, контроль потоков исполнения, очистку оперативной памяти, мандатный контроль доступа для ВМ к ресурсам аппаратным (физическим) ресурсам (процессоры, память, порты ввода-вывода, прерывания, периферия, виртуальные каналы связи и т.д.), а также реализацию комплекса функций безопасности (защиты информации) в виртуальной инфраструктуре:

- идентификацию и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрацию событий безопасности;
- управление (фильтрацию, маршрутизацию, контроль соединения, однонаправленную передачу) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;
- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- контроль целостности виртуальной инфраструктуры и ее конфигураций;
- резервное копирование данных и программного обеспечения виртуальной инфраструктуры;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей;
- создание, удаление, запуск, остановку, конфигурацию ВМ и т.д., включая назначение меток безопасности, а также экспорт и импорт ВМ и управление шаблонами ВМ.

Изделие предназначено для обеспечения возможности создания масштабируемой защищенной виртуальной инфраструктуры, вплоть до распределённого частного или гибридного облака, в целях использования:

- в государственных информационных системах до 1 класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.);
- в информационных системах для обеспечения до 1 уровня защищенности персональных данных в соответствии с требованиями документа «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введен в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г);
- в системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);
- при защите значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК России от 25 декабря 2017 г № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»);
- в информационных системах общего пользования 2 класса (Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»).

Конкретный перечень мер защиты информации, реализуемых Изделием в соответствии с документами ФСТЭК России приведен в Приложении В настоящего документа.

Перечень угроз (из БДУ ФСТЭК РФ), которым противостоит Изделие, определен в Приложении Г настоящего документа.

Пример записи Изделия при заказе и ссылках в другой технической документации:

Серверная доверенная виртуальная среда функционирования программных средств Numa vServer 643.АМБН.00021-01

Настоящие ТУ совместно с комплектом разработанной на Изделие документации определяют технические требования к Изделию, требования по безопасности и охране окружающей среды, а также требования к приёмке и контролю, поставке Изделия потребителю, его хранению, транспортированию и эксплуатации, и, кроме того, гарантийные обязательства изготовителя доверенной виртуальной среды Numa vServer 643.АМБН.00021-01.

Настоящий документ разработан в соответствии с ГОСТ 2.114-2016.

Перечень нормативно-методических и эксплуатационных документов, используемых в настоящих ТУ, приведен в Приложении А.

Требования настоящих ТУ обязательны при разработке отдельных (частных) методик при сертификации доверенной виртуальной среды Numa vServer 643.АМБН.00021-01.

СОДЕРЖАНИЕ

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1.1. Общие требования

1.1.1. Изделие должно соответствовать требованиям настоящих технических условий, требованиям документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02 июня 2020 г. № 76 по 4 уровню доверия, а также требованиям документа «Требования по безопасности информации к средствам виртуализации», утвержденного приказом ФСТЭК России от 27 октября 2022 г. №187 по 4 классу защиты.

1.2. Требования назначения

1.2.1. Изделие должно использоваться для создания доверенной виртуальной инфраструктуры корпоративного уровня, с возможностью вертикального и горизонтального масштабирования, включая территориальное распределение, обеспечивающей возможность работы с информацией различной степени конфиденциальности, не содержащей сведений, составляющих государственную тайну.

1.2.2. В рамках доверенной виртуальной инфраструктуры, созданной с использованием Изделия, должна обеспечиваться возможность создания изолированных друг от друга виртуальных сред, в том числе на физическом (аппаратном) уровне, предназначенных для обеспечения работы пользователей, имеющих различные права доступа к разнородной информации (конфиденциальной информации различных типов), обработка которой осуществляется с использованием ресурсов виртуальной инфраструктуры (в виртуальной среде).

1.2.3. Изделие должно функционировать на серверах, построенных на базе 64-х разрядных аппаратных платформ Intel или AMD с поддержкой технологии аппаратной виртуализации, включая кластерные и территориально-распределенные конфигурации.

1.2.4. Изделие должно обеспечивать возможность независимого запуска и функционирования множества гостевых виртуальных машин (далее — ВМ) под управлением операционных систем, предназначенных для исполнения на архитектуре x86-x64 Intel или AMD (операционные системы Microsoft Windows, Microsoft Windows Server, Linux, включая специализированные дистрибутивы отечественного производства, а также иные совместимые ОС).

1.2.5. Изделие должно обеспечивать возможность запуска ВМ под управлением полностью виртуализованных операционных систем, а также частично виртуализованных ОС, и паравиртуальных ОС.

1.3. Требования к структуре и декомпозиции Изделия

1.3.1. Изделие должно быть реализовано в виде гипервизора гибридного типа, структурно состоящего из следующих функциональных модулей:

а) монитор виртуальных машин (далее – МВМ или гипервизор);
б) управляющая виртуальная машина (далее – УВМ).

1.3.2. МВМ должен обеспечивать:

1.3.2.1. запуск и исполнение ВМ;

1.3.2.2. виртуализацию аппаратных ресурсов, функции дискреционного и мандатного контроля в части, касающейся управления доступом к аппаратному обеспечению (процессоры, память, порты ввода-вывода, периферийные устройства) для ВМ;

1.3.2.3. возможность создания изолированных друг от друга виртуальных зон, предназначенных для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, в том числе на физическом (аппаратном) уровне, включая гарантированную изоляцию страниц памяти;

1.3.2.4. создание виртуальной вычислительной сети (виртуальных каналов связи) для ВМ и (или) виртуальных зон, с возможностью контроля и управления информационными потоками, исключающим НСД к защищаемой информации, включая защиту информационно-управляющих сообщений (служебных информационных сообщений) и конфигурационной информации;

1.3.2.5. возможность выполнять поэтапный или параллельный запуск ВМ, в т.ч. первоочередной запуск специализированных служебных ВМ, предназначенных для обеспечения служебных сервисов и функций безопасности для виртуальных сред и объектов (например, средств антивирусной защиты, средств криптографической защиты информации, сенсоров и (или) датчиков систем обнаружения (предотвращения) вторжений), функционирующих в их составе виртуальных сред.

1.3.3. Управление МВМ должно осуществляться через встроенный программный интерфейс из специализированной управляющей ВМ (УВМ), которая предназначена для обеспечения функций управления и администрирования Изделия в комплексе.

1.3.3.1. УВМ должна обеспечивать интерфейс взаимодействия с МВМ для конфигурирования запускаемых ВМ, а также для управления параметрами аппаратного обеспечения виртуальной инфраструктуры, в том числе для:

а) передачи параметров конфигурирования ВМ, выдачи команд МВМ на их запуск, остановку, приостановление и возобновление;

б) конфигурирования виртуальной вычислительной сети (виртуальных каналов связи) для ВМ, а также организации сетевого взаимодействия с внешней по отношению к Изделию средой;

в) сбора, систематизации и анализа журналов регистрации событий, возникающих в ходе эксплуатации Изделия;

г) управления доступом субъектов доступа к объектам доступа и аппаратному обеспечению серверного комплекса, на котором развернуто и эксплуатируется Изделие;

д) мониторинга загрузки мощностей физического и виртуального аппаратного обеспечения;

е) контроля работоспособности (изношенности) машинных носителей информации, серверного комплекса, на котором развернуто и эксплуатируется Изделие;

ж) управления функциями безопасности, реализуемыми Изделием.

1.3.3.2. УВМ должна осуществлять исполнение драйверов устройств аппаратного обеспечения комплекса, на котором развернуто и функционирует Изделие.

1.3.3.3. УВМ должна предоставлять возможность управления периферийными устройствами, напрямую не отданными в использование ВМ;

1.3.3.4. УВМ должна обеспечивать функциональность планировщика процессов и управления памятью для системных процессов внутри УВМ.

1.4. Требования к функциональным характеристикам

1.4.1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

1.4.1.1. Идентификация и аутентификация устройств

1) Изделие должно обеспечивать идентификацию физических и виртуальных устройств по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

2) Изделие должно обеспечивать поддержку протоколов аутентификации iscsi/iser для аутентификации устройств в информационной системе.

1.4.1.2. Ролевая модель управления доступом и администрирования Изделия

Изделие должно обеспечивать ролевую модель управления доступом и администрирования Изделия, при которой пользователями Изделия должны являться субъекты доступа, обладающие различными правами по администрированию Изделия при этом:

а) Изделие должно обеспечивать функции управления доступом на основе ролевой модели (Role Based Access Control, RBAC), в соответствии с которой Изделие должно связывать пользователя (или группу пользователей) с определенной ролью, являющейся именованным набором разрешений по доступу к объектам доступа и действиям по администрированию Изделия в соответствии с Приложением Б.

б) Изделие должно поддерживать роль локального администратора (Local Super User, LSU), обладающая всеми (максимальными) правами и полномочиями по управлению Изделием.

1.4.1.3. Идентификация и аутентификация субъектов доступа и объектов доступа

1.4.1.3.1. Изделие должно осуществлять идентификацию и аутентификацию субъектов доступа, являющихся пользователями Изделия, в соответствии с RBAC и процессов, запускаемых (выполняемых) от их имени.

1.4.1.3.2. Идентификация и аутентификация субъектов доступа и объектов доступа должна осуществляться программными модулями, входящими в состав УВМ.

1.4.1.3.3. Субъекты доступа должны однозначно идентифицироваться и аутентифицироваться при доступе к консоли управления УВМ до разрешения каких-либо действий по администрированию Изделия.

1.4.1.3.4. Идентификация и аутентификация субъектов доступа должна осуществляться с использованием логина и пароля.

1.4.1.3.5. Удалённое управление должно осуществляться с использованием протокола SSH, с взаимной аутентификацией.

1.4.1.4. Управление идентификаторами

Изделие должно обеспечивать следующие возможности по управлению идентификаторами пользователей и (или) устройств:

1) формирование (создание) администратором Изделия идентификатора, который однозначно идентифицирует пользователя;

2) присвоение идентификатора пользователю и (или) устройству.

1.4.1.5. Управление средствами аутентификации

Изделие должно осуществлять следующие функции управления средствами аутентификации (аутентификационной информацией) субъектов доступа:

3) конфигурирование (задание/установку) администратором Изделия следующих параметров паролей пользователей Изделия:

а. минимальной сложности пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '’', '”', '.', '?', '<', '>', '«');

б. минимального количества символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);

в. времени действия пароля, в пределах от 60 до 180 дней;

г. максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток.

д. конфигурирование (задание/установку) администратором Изделия следующих параметров автоматической блокировки учетной записи субъекта доступа в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 3 минут до 60 минут.

1.4.1.6. Защита обратной связи при вводе аутентификационной информации

Изделие должно обеспечивать защиту аутентификационной информации (паролей субъектов доступа) в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения действительного значения аутентификационной информации и количества вводимых пользователем символов. Вводимые символы пароля должны отображаться условными знаками «*», или пустыми символами.

1.4.1.7. Защита аутентификационной информации субъектов доступа

Изделие должно обеспечивать защиту аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования. Изделие должно обеспечивать хранение аутентификационной информации субъектов доступа в защищенном формате.

1.4.1.8. Идентификация и аутентификация пользователей в Изделии должна осуществляться с учетом требований разделов 4 – 7 ГОСТ Р 58833 «Защита информации. Идентификация и аутентификация. Общие положения».

1.4.1.9. В Изделии должна обеспечиваться возможность смены установленного администратором Изделия пароля пользователя Изделия после его первичной аутентификации.

1.4.1.10. Изделие должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

1.4.1.11. В случае ввода неправильного значения идентификатора или пароля в Изделии должно выводиться сообщение с приглашением ввести правильные идентификатор и пароль еще раз.

1.4.2. Управление доступом субъектов доступа к объектам доступа

1.4.2.1. Управление доступом для пользователей Изделия должно обеспечиваться средствами УВМ, в соответствии с реализованной в Изделии моделью RBAC. При управлении доступом должны обеспечиваться следующие функциональные возможности:

1) контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

2) контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды.

1.4.2.2. Изделие должно обеспечивать управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа.

1.4.2.3. Изделие должно обеспечивать контроль запуска виртуальных машин на основе заданных администратором правил.

1.4.2.4. Изделие должно обеспечивать контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора, в памяти хостовой

операционной системы, виртуальных машин и (или) иных объектов доступа.

1.4.2.5. Изделие должно обеспечивать реализацию механизмов изоляции программных модулей одного процесса от другого.

1.4.2.6. Изделие должно обеспечивать гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга.

1.4.2.7. Изделие должно обеспечивать функции мандатного контроля доступа для ранжирования и разграничения доступа различных ВМ к виртуальным или аппаратным ресурсам, памяти, процессорам.

1.4.3. Регистрация событий безопасности в виртуальной инфраструктуре

1.4.3.1. Изделие должно обеспечить регистрацию следующих событий:

3) запуск (завершение) работы МВМ и УВМ, а также виртуальных машин, при этом состав и содержание информации, подлежащей регистрации для указанных компонентов виртуальной инфраструктуры, должны включать:

а. дату и время запуска (завершения) работы;

б. результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная);

в. идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры;

г. тип события;

д. идентификатор события.

4) запуск (завершение) программ и процессов в УВМ, при этом регистрации должны подлежать дату и время запуска (завершения) программ и процессов, тип события, идентификатор события.

5) доступ субъектов доступа к УВМ, а также виртуальным машинам, при этом при доступе (входе или выходе) к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать:

а. дату и время доступа субъектов;

б. результат попытки доступа субъектов (успешная или неуспешная),

в. идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры;

г. тип события;

д. идентификатор события.

6) внесение изменений в состав и конфигурацию компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения, при этом состав и содержание информации, подлежащей регистрации, должны включать:

а. дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании;

б. результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры;

в. тип события;

г. идентификатор события.

7) создание/удаление ВМ, при этом состав и содержание информации, подлежащей регистрации, должны включать:

а. дату и время;

б. тип события;

в. идентификатор события.

8) изменение ролевой модели, при этом состав и содержание информации, подлежащей регистрации, должны включать:

а. дату и время;

б. тип события;

в. идентификатор события.

9) факты нарушения целостности объектов контроля, при этом состав и содержание информации, подлежащей регистрации, должны включать:

а. дату и время;

б. тип события;

в. идентификатор события.

1.4.3.2. Изделие должно обеспечивать возможность централизованного сбора, хранения, экспорта и анализа информации о зарегистрированных событиях безопасности виртуальной инфраструктуры;

1.4.3.3. Изделие должно обеспечивать регистрацию событий безопасности, связанных с перемещением и размещением виртуальных машин;

1.4.3.4. Изделие должно обеспечивать возможность резервного копирования журнала регистрации событий.

1.4.3.5. Изделие должно информировать администратора Изделия о событиях безопасности путем произведения записи в журнал аудита.

1.4.3.6. Регистрация событий безопасности в средстве виртуализации должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

1.4.3.7. Журнал аудита Изделия должен быть доступен только для чтения. При исчерпании области памяти, отведенной под журнал аудита Изделия, должно осуществляться архивирование журнала с последующей очисткой высвобождаемой области памяти.

1.4.4. Управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

1.4.4.1. Изделие должно обеспечить следующие функции по управлению потоками информации между компонентами виртуальной инфраструктуры:

1) управление сетевым трафиком (управление информационными потоками) между компонентами виртуальной инфраструктуры;

2) отключение сетевых протоколов неиспользуемых компонентами виртуальной инфраструктуры МВМ, УВМ, а также в виртуальной вычислительной сети;

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

4) обеспечение изоляции потоков данных, передаваемых и обрабатываемых МВМ, УВМ и сетевых потоков виртуальной вычислительной сети;

5) обеспечение изоляции сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях и для каждой виртуальной машины;

6) возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой.

1.4.5. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

1.4.5.1. Изделие должно обеспечивать следующие функции контроля и управления

перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных:

1) управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

2) управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

3) управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

1.4.5.2. Изделие должно обеспечивать реализацию следующих ограничений при управлении перемещениям виртуальных машин:

1) полный запрет перемещения виртуальных машин (контейнеров);

2) ограничение перемещения виртуальных машин (контейнеров) в пределах виртуальных сред, созданных для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментов информационных систем, развернутых в среде виртуализации.

3) ограничение перемещения виртуальных машин (контейнеров) между виртуальными средами, созданными для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментами информационных систем, развернутых в среде виртуализации.

1.4.5.3. Изделие должно обеспечивать возможность централизованного управления механизмами управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

1.4.5.4. Изделие должно обеспечивать обработку отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных;

1.4.5.5. Изделие должно обеспечивать непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения;

1.4.5.6. Изделие должно обеспечивать очистку освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных.

1.4.5.7. Изделие должно обеспечивать стирание остаточной информации, образующейся после удаления:

1) файлов, содержащих настройки виртуального аппаратного обеспечения;

2) файлов-образов ВМ.

1.4.5.8. Очистка памяти должна осуществляться путём генерации случайной последовательности бит и записью их в освобождаемый блок и/или путем записи в освобождаемые блоки нулей.

1.4.5.9. Изделие должно обеспечивать размещение кода Изделия в области памяти, не доступной одновременно для записи и исполнения.

1.4.6. Контроль целостности виртуальной инфраструктуры и ее конфигураций

1.4.6.1. Изделие должно обеспечивать возможность контроля целостности в процессе загрузки и (или) динамически следующих компонентов:

1) УВМ, МВМ, состава и конфигурации виртуального аппаратного обеспечения;

2) файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

3) файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем. Контроль целостности должен проводиться только, когда файлы-образы не задействованы;

4) резервных копий виртуальных машин;

5) состава аппаратной части компонентов виртуализированной инфраструктуры;

6) журнала аудита.

1.4.6.2. Должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

1.4.6.3. Изделие должно информировать администратора Изделия о нарушении контроля целостности объектов контроля путем произведения записи в журнал аудита и (или) выводом сообщения о нарушении контроля целостности в консоль управления Изделием.

1.4.6.4. Изделие должно обеспечивать блокировку запуска компонентов программного обеспечения, не прошедших аутентификацию с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей).

1.4.6.5. Изделие должно блокировать запуск ВМ при выявлении нарушения контроля целостности файлов виртуальной базовой системы ввода-вывода.

1.4.7. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры

1.4.7.1. Изделие должно обеспечивать следующие функциональные возможности по резервному копированию:

1) резервное копирование ВМ, при этом Изделие должно поддерживать следующие механизмы:

а. механизм снимков ВМ (snapshot), который должен обеспечивать возможность создания снимка виртуальной машины, в котором будет зафиксировано ее текущее состояние, и возможность последующего возвращения к этому снимку;

б. механизм экспорта (выгрузки) ВМ на выделенное хранилище;

2) резервное копирование конфигурации виртуальной инфраструктуры;

3) резервное копирование МВМ;

4) резервное копирование УВМ.

5) резервное переназначение мастера пула.

1.4.7.2. Изделие должно обеспечивать возможность резервирования каналов связи, используемых в виртуальной инфраструктуре.

1.4.8. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

1.4.8.1. Изделие должно обеспечивать возможность создание изолированных виртуальных зон, предназначенных для решения выделенных (обособленных) задач.

1.4.8.2. Изделие должно обеспечивать возможность сегментирования виртуальной инфраструктуры (виртуальных вычислительных сетей) посредством создания логических локальных сетей.

1.4.8.3. УВМ должна быть должна быть недоступна со стороны объектов и процессов, исполняющихся на ВМ.

1.4.9. Изделие должно обеспечивать возможность следующих действий: создание, удаление, запуск, остановку, конфигурацию ВМ и т.д., включая назначение меток безопасности, а также экспорт и импорт ВМ и управление шаблонами ВМ.

1.5. Комплектность

1.5.1. Изделие должно поставляться в виде установочного образа (в формате image и/или iso), готового к установке на СВТ и комплектоваться необходимой для эксплуатации Изделия документацией (далее – Комплект Изделия).

1.5.2. Должны быть доступны следующие типы Комплектов Изделия:

- Комплект Изделия на материальных носителях – Изделие должно поставляться на электронном носителе с комплектом документов в соответствии с таблицей 1;
- Комплект Изделия в электронном виде – Изделие и документация должны поставляться в виде файлов в соответствии с таблицей 2, которые загружаются по каналам передачи данных с сетевых ресурсов ООО «НумаТех», при условии предоставления ООО «НумаТех» соответствующего доступа.

1.5.3. Количество Комплектов Изделия, передаваемых Конечному пользователю Изделия в рамках конкретной поставки должно определяться условиями лицензионного договора (договора поставки).

1.5.4. Количество лицензий на использование Изделия (число доступных установок (инсталляций) Изделия или количество СВТ, в составе которых может использоваться Изделие) доступных Конечному пользователю должно быть указано в лицензионном сертификате, сопровождающем каждую поставку Изделия.

Примечания:

1. Лицензионный сертификат – документ, оформляемый ООО «НумаТех» на фирменном бланке, подтверждающий легитимность использования Изделия Конечным Пользователем, содержащий информацию о конкретной поставке Изделия, в том числе сведения об исполнении Изделия и типе СВТ, для использования на котором предназначено исполнение Изделия в рамках конкретной поставки.

2. Ограничения прав по использованию Изделия, связанные с наличием Лицензий на использование ПО, реализуемые ООО «НумаТех» в рамках мер по защите авторских прав в отношении программных продуктов собственной разработки, приведены в разделе 10 настоящих Технических условий.

3. Лицензионный сертификат должен передаваться Конечному пользователю при передаче прав на использование Изделия или совместно с СВТ, на которые Изделие было предустановлено производителем (поставщиком) СВТ.

Таблица 1 – Состав комплекта поставки сертифицированного Изделия на материальных носителях

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
1	Компакт диск в составе: 1. Установочный образ Изделия 643.АМБН.00021-01; 2. Документация в составе: 643.АМБН.00021-01 32 01 Руководство администратора. Установка, настройка Numa vServer; 643.АМБН.00021-01 34 01 Руководство пользователя; 643.АМБН.00021-01 94 01 Инструкция по проверке контрольных сумм; 643.АМБН.00021-01 30 02 Формуляр. Приложение А;		На электронном носителе Идентификатор СЗИ: РОСС RU.0001.4580.xxxxxx

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
	643.АМБН.00021-01 30 03 Формуляр. Приложение Б		
2	Конверт для хранения компакт-диска		
3	643.АМБН.00021-01 30 01 Формуляр		В печатном виде
4	Заверенная копия сертификата соответствия требованиям по безопасности информации Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)		В печатном виде
5	Транспортная тара		Пластиковый пакет с застежкой типа zip-lock

Таблица 2 – Состав комплекта поставки сертифицированного Изделия в электронном виде

№ п/п	Наименование составной части Изделия (документа)	Кол-во	Примечание
1	Установочный образ Изделия 643.АМБН.00021-01		В электронном виде Идентификатор СЗИ: РОСС RU.0001.4580.xxxxxx
2	Документация в составе: 643.АМБН.00021-01 32 01 Руководство администратора. Установка, настройка Numa vServer; 643.АМБН.00021-01 34 01 Руководство пользователя; 643.АМБН.00021-01 94 01 Инструкция по проверке контрольных сумм; 643.АМБН.00021-01 30 01 Формуляр; 643.АМБН.00021-01 30 02 Формуляр. Приложение А; 643.АМБН.00021-01 30 03 Формуляр. Приложение Б		В электронном виде
3	Копия сертификата соответствия требованиям по безопасности информации Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)		В электронном виде

Примечание. Порядок получения Изделия при электронной поставке описан в разделе 8 Формуляра 643.АМБН.00021-01 30 01.

1.5.5. Контрольные суммы установочного образа Изделия должны иметь значение, приведённое в таблице 3.

Таблица 3 – Контрольные суммы

Наименование Изделия	Контрольная сумма (ФИКС-UNIX 1.0)	Контрольная сумма **(gost12sum)**
Серверная доверенная виртуальная среда функционирования программных средств Numa vServer 643.АМБН.00021-01	8074638A	71c4d2d351ddc0aad839aaa9078cb81617242976847ada83265612d80ff79fe4

Подсчет контрольных сумм должен осуществляться согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00021-01 94 01 с использованием сертифицированной с использованием сертифицированной программы фиксации и контроля целостности информации

«ФИКС-UNIX 1.0» (Сертификат ФСТЭК России №680 от 30.10.2002 г.), а также с использованием свободно распространяемой утилиты «gost12sum» по алгоритму ГОСТ Р 34.11-2012-256 бит.

1.6. Маркирование

1.6.1. Маркирование Изделия должно соответствовать требованиям настоящих ТУ, эксплуатационной документации и должна содержать:

- идентификатор СЗИ;
- номер экземпляра Комплекта Изделия;
- наименование (обозначение) Изделия;
- наименование предприятия-Изготовителя.

Примечания.

1. Идентификатор СЗИ – идентификатор средства защиты информации, является уникальным параметром для каждой поставки Изделия, который:

- *содержится в Лицензионном сертификате;*
- *наносится на электронные носители, содержащие Изделие;*
- *указывается в формуляре Изделия;*
- *отображается в меню администрирования Изделия.*

2. Идентификатор СЗИ имеет следующий формат РОСС RU.0001.4580.XXXXXX, где:

- *первая группа знаков содержит прописные буквы и цифры РОСС RU.0001, указывающие на систему сертификации ФСТЭК России;*
- *вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;*
- *третья группа знаков указывает на порядковый номер экземпляра СЗИ в системе учета средств защиты информации, произведенных ООО «НумаТех».*

1.6.2. Сертифицированные комплекты Изделия должны маркироваться идентификатором СЗИ. Идентификатор СЗИ должен быть указан:

- в разделе 7 Формуляра 643.АМБН.00021-01 30 01;
- на компакт-диске при поставке на материальных носителях.

Идентификатор СЗИ должен отображаться в оснастке меню администрирования, установленного на СВТ Изделия (поле «SZI ID:»).

1.6.3. Идентификатор СЗИ, соответствующий конкретной поставке Изделия, должен регистрироваться ООО «НумаТех» в «Журнале учета выпущенных Изделий и учета идентификаторов СЗИ» совместно со следующей информацией о поставке Изделия:

- число лицензий и номер лицензии;
- количество экземпляров и тип Комплектации Изделия;
- сведения о конечном пользователе и цепочке поставки Изделия.

Примечания.

Номер лицензии – уникальный номер, приводимый в Лицензионном сертификате, который идентифицирует конкретную поставку Изделия.

1.7. Упаковка Изделия

1.7.1. При поставке Изделия и документации на Изделие на компакт-диске, диск должен быть упакован в конверт и запечатан специальной этикеткой с логотипом изготовителя. Способ заклеивания должен исключать вскрытие конверта без невидимых повреждений упаковки.

1.7.2. Компакт-диск и документация на Изделие, входящая в комплект поставки, должны

быть упакованы в транспортную тару изготовителя, представляющую собой пластиковый пакет с застежкой типа zip-lock.

1.7.3. Упаковка Изделия должна обеспечивать выполнение требований по транспортированию и хранению в соответствии с ТУ.

1.7.4. Тара должна выдерживать без нарушения целостности конструкции воздействие механических нагрузок и климатических факторов, обеспечивать защиту упакованного в неё Изделия.

1.7.5. Упаковке подлежит укомплектованное Изделие, прошедшее приемо-сдаточные испытания.

6. УСЛОВИЯ ТРАНСПОРТИРОВАНИЯ, ХРАНЕНИЯ И ЭКСПЛУАТАЦИИ

6.1. Транспортирование Изделия

6.1.1. Допускается транспортирование Изделия в упакованном виде любым видом транспорта без ограничения скорости и расстояния.

6.1.2. При транспортировании должна быть обеспечена защита Изделия от:

- механических повреждений;
- проникновения влаги;
- проникновения грязи и пыли;
- длительного воздействия прямого солнечного света.

6.1.3. При транспортировании Изделия следует обеспечивать условия:

- температура воздуха – от плюс 10 до плюс 35 °С;
- относительная влажность – от 40 до 80 % при температуре не выше плюс 25 °С;
- атмосферное давление от 8,4×104 до 10,7×104 Па (от 630 до 800 мм. рт.ст.);
- массовая концентрация пыли в воздухе не более 0,75 мг/м3.

Примечание. При попадании носителей информации в экстремальные температурные условия необходимо до начала эксплуатации выдержать их при температуре плюс 25 °С не менее 2-х часов.

6.2. Хранение

6.2.1. Изделие должно храниться в упаковке в отапливаемых помещениях при температуре воздуха от 5 до 40 °С и относительной влажности воздуха не более 80 %.

6.2.2. Изделие должно храниться в капитальных отапливаемых помещениях на стеллаже или в упаковке, поставляемой изготовителем, в условиях, соответствующих условиям эксплуатации Изделия, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей. Также при хранении не допускаются резкие перепады температуры (более 20 °С в час) и воздействия внешних магнитных полей напряженностью более 4000 А/м.

6.3. Указания по эксплуатации

6.3.1. Не допускается использовать Изделие для обработки информации, содержащей сведения, составляющие государственную тайну.

6.3.2. Эксплуатация Изделия возможна только при соблюдении следующих организационно-технических мер:

- для обеспечения правильной эксплуатации Изделия должен быть назначен администратор безопасности, прошедший соответствующую подготовку, ознакомившийся с эксплуатационной документацией на Изделие и не рассматривающийся в качестве нарушителя информационной безопасности;
- учетная запись локального администратора (LSU) должна использоваться только администратором с полными правами доступа;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям пользователей Изделия;
- должны обеспечиваться физическая сохранность и периодический контроль конфигурации аппаратного обеспечения серверного комплекса, на котором установлено Изделие;
- доступ к аппаратному обеспечению серверного комплекса, на котором установлено Изделие, со стороны неавторизованного персонала эксплуатирующей организации и любых

третьих лиц должен быть исключен или ограничен и осуществляться только при непосредственном присутствии администратора безопасности;

- доступ к BIOS СВТ, входящих в состав серверного комплекса, на котором установлено Изделия, а также к загрузчику среды должен быть защищен с использованием парольной защиты, пароль для доступа должен отвечать требованиям по сложности, аналогичным предъявляемым к паролям пользователей Изделия;
- на СВТ, входящих в состав серверного комплекса, на котором установлено Изделия, должна быть исключена возможность использования средств разработки ПО и отладчиков для редактирования кода и анализа оперативной памяти, используемой Изделием;
- при первоначальной настройке Изделия необходимо изменить заводские установки паролей на доступ к функциям администрирования Изделия;
- при удаленном управлении Изделием пара ключей для SSH авторизации должны быть сгенерированы алгоритмами RSA с минимальной длиной ключа 3072 бит или ESDCA – 256 бит или ГОСТ Р 34.11-2012 – 256 бит. Алгоритм DSA запрещен к использованию.
- до перехода Изделия в рабочее состояние должен быть выполнен контроль целостности Изделия сертифицированными ФСТЭК России средствами защиты информации.

6.3.3. Для обеспечения выполнения требований по безопасности информации, предъявляемых к объекту информатизации, в состав которого входит Изделие, в виртуальной среде, созданной с использованием Изделия, могут применяться средства защиты информации, не входящие в состав Изделия:

- функционирующие в среде операционных систем гостевых ВМ;
- разворачиваемые на базе гостевых ВМ (служебные ВМ), выделенных для обеспечения целевых функций: например, программный межсетевой экран, средства централизованного управления антивирусной защитой, средства криптографической защиты информации, сенсоров и (или) датчиков систем обнаружения (предотвращения) вторжений.

6.3.4. Все сетевые подключения к Изделию должны быть ограничены сертифицированным ФСТЭК России межсетевым экраном, класс которого должен быть определен исходя из требований по безопасности информации, предъявляемых к объекту информатизации, в состав которого входит Изделие.

6.3.5. Удаленное управление Изделием должно осуществляться со СВТ, в отношении которых реализованы организационно-технические меры по защите информации, соответствующие требованиям по безопасности информации, предъявляемых к объекту информатизации, в состав которого входит Изделие, при этом:

- каналы передачи данных, используемые для доступа к Изделию и расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами;
- для защиты каналов передачи данных, используемых для доступа к Изделию и выходящих за пределы контролируемой зоны, должны применяться методы и средства, устойчивые к пассивному и (или) активному прослушиванию сети и сертифицированные в установленном порядке.

6.3.6. В целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средству виртуализации должны применяться средства криптографической защиты информации, прошедшие процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

7. ОГРАНИЧЕНИЕ ПРАВ ПО ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЗДЕЛИЯ

Для обеспечения возможности использования экземпляра ПО на конкретном лицензированном устройстве необходимо выполнить процедуру активации ПО с использованием уникального ключевого файла. В ходе проведения активации экземпляр ПО закрепляется за конкретным лицензированным устройством.

Ключевой файл является уникальным, вырабатывается и предоставляется Правообладателем по запросу конечного пользователя ПО для использования на конкретном лицензируемом устройстве.

Выработка ключевого файла осуществляется с учетом уникальных параметров лицензируемого устройства (конкретной аппаратной платформы).

Порядок формирования запроса ключевого файла приведен в документе «Руководство администратора. Установка, настройка Numa vServer» 643.АМБН.00021-01 32 01.

Лицензионный ключ (ключевой файл) содержит сведения, которые впоследствии используются для проверки прав использования ПО и могут включать в свой состав:

- сведения о конечном пользователе ПО;
- версию ПО;
- сведения о сроках использования ПО конечным Пользователем – сроке действия лицензии;
- идентификационный номер экземпляра ПО;
- уникальные параметры аппаратного обеспечения лицензируемого устройства.

8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Изготовитель гарантирует соответствие качества Изделия требованиям настоящих ТУ при соблюдении пользователем условий транспортирования, хранения и эксплуатации.

В случае если во время эксплуатации Пользователь Изделия внес изменения (пытался внести изменения) в программное обеспечение Изделия, нарушил правила его транспортирования, эксплуатации и хранения, указанные в документации на Изделие, то действие сертификата соответствия и гарантии на Изделие прекращается с момента внесения изменений и (или) нарушения правил транспортировки, эксплуатации и хранения.

9. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

9.1. Изготовитель осуществляет техническую поддержку Изделия в соответствии с пакетами услуг технической поддержки, состав и содержание сервисов которых закрепляется Изготовителем в Политике сервисного сопровождения Продуктов производства компании «НумаТех», публикуемой на официальном сайте Изготовителя (www.numatech.ru).

9.2. В течение срока действия Сертификата соответствия требованиям по безопасности информации на Изделие Изготовитель осуществляет его базовую техническую поддержку. В рамках базовой технической поддержки Изделия изготовитель осуществляет:

- поиск ошибок реализации и уязвимостей в Изделии;
- информирование пользователя Изделия об обнаруженных ошибках и уязвимостях, путем проведения рассылок и (или) размещением соответствующей информации на сайте изготовителя Изделия;
- доведение до пользователя Изделия необходимых обновлений программного обеспечения, обеспечивающих нейтрализацию выявленных ошибок реализации и уязвимостей в Изделии (далее – обновление безопасности), путем предоставления возможности безопасной загрузки обновлений безопасности по средствам сети Интернет с соответствующих ресурсов изготовителя Изделия и (или) путем предоставления обновлений безопасности на материальных носителях.

9.3. Обязательный срок действия базовой технической поддержки Изделия определяется сроком действия сертификата соответствия на Изделие (согласно Государственного реестра сертифицированных средств защиты информации ФСТЭК России № РОСС RU.0001.01БИ00). По решению изготовителя срок действия технической поддержки может превышать сроком действия сертификата соответствия на Изделие, до информирования ФСТЭК России об окончании технической поддержки Изделия.

9.4. Потребители и ФСТЭК России будут проинформированы не позднее чем за 1 год до окончания производства и (или) поддержки безопасности Изделия об окончании производства и (или) поддержке безопасности Изделия.

9.5. Услуги технической поддержки уровня «Стандарт» доступны приобретающей организации в течение 12 месяцев от даты приемки Изделия представителем приобретающей организации.

9.6. Срок действия технической поддержки Изделия и качество сервисов технической поддержки указывается в Сервисном сертификате Изделия, наличие которого обеспечивает возможность обращения в сервисную службу Изготовителя.

9.7. Иные виды технической поддержки (расширение сервисов технической поддержки) предоставляются изготовителем на возмездной основе, в соответствии с Политикой сервисного сопровождения.

9.8. Контактные данные сервисной службы ООО «НумаТех»:

Адрес:	196084, г. Санкт-Петербург, ул. Цветочная, д. 18, лит. А, оф. 424, БЦ «Бизнес-Парк»
Телефон:	(812) 3090601, доб.220
E-mail:	support@numatech.ru
Портал:	support.numatech.ru
Режим работы:	Пн. – Пт.: 10:00 – 19:00

10. ПОРЯДОК ПОЛУЧЕНИЯ ИЗДЕЛИЯ ПРИ ЭЛЕКТРОННОЙ ПОСТАВКЕ

10.1. Порядок получения Изделия в электронном виде

Получение электронной версии Изделия осуществляется путем загрузки установочного образа и пакета документов, указанных в таблице 2 с портала сервисной службы https://support.numatech.ru, либо по ссылке, предоставляемой ООО «НумаТех». Подлинность и целостность обеспечивается применением электронной подписи.

10.2. Порядок эксплуатации Изделия

После загрузки установочного образа и эксплуатационных документов по каналам передачи данных с сетевых ресурсов ООО «НумаТех», необходимо произвести проверку его подлинности и целостности путем проверки электронной подписи согласно прилагаемой инструкции.

После успешной проверки подлинности и целостности загруженных материалов, необходимо:

- записать полученные данные на физический носитель и промаркировать физический носитель идентификатором СЗИ, указанным в разделе 7 Формуляра 643.АМБН.00021-01 30 01, а также номером экземпляра Комплекта Изделия, приведённым в разделе 18 Формуляра 643.АМБН.00021-01 30 01;
- распечатать полученный Формуляр.

11. УКАЗАНИЯ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ И ОБНОВЛЕНИЮ

11.1. Изготовитель осуществляет поиск уязвимостей Изделия, в том числе с использованием общедоступных баз данных уязвимостей ФСТЭК России (http://bdu.fstec.ru/) и баз данных уязвимостей CVE. При выявлении критичной уязвимости изготовитель незамедлительно разрабатывает меры, направленные на нейтрализацию выявленной уязвимости, и доводит содержание уязвимости, а также этих мер до заказчика, ФСТЭК России, БДУ ФСТЭК России. При необходимости (для нейтрализации выявленной уязвимости) внесения изменений в Изделие процедура выполняется в соответствии с пунктами 71-74 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55.

11.2. Доведение информации об обнаруженных недостатках Изделия, разработка компенсирующих мер по защите информации или ограничений по применению Изделия, а также доведение информации о таких мерах и ограничениях до потребителей сертифицированного Изделия, осуществляются в срок не более 48 часов с момента выявления недостатка, путем отправки сообщений на электронные адреса потребителей (или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически).

11.3. Информация о выходе обновлений и мер, направленных на нейтрализацию выявленной уязвимости, публикуется на сайте изготовителя Изделия (https://www.numatech.ru/), а также доводится до каждого пользователя путем отправки сообщений на электронные адреса потребителей, указанных при заказе Изделия, с использованием электронной цифровой подписи для обеспечения подлинности и целостности информационного сообщения.

11.4. При выходе обновления, исправляющего критические уязвимости, указывается обязательность обновления Изделия или применения мер, направленных на нейтрализацию выявленной уязвимости. Также на сайте изготовителя размещается информация о контрольной сумме обновления необходимой для верификации обновления, а также контрольная сумма Изделия с примененным обновлением.

11.5. Обновление Изделия должно осуществляться только с использованием предоставляемых изготовителем обновлений, в т.ч. скачанных с его официального сайта, с соблюдением соответствующих Инструкций изготовителя.

11.6. Загрузка обновления осуществляется с сервера изготовителя с соблюдением требуемых мер, обеспечивающих безопасность его получения. Ссылка для загрузки предоставляется при обращении в сервисную службу изготовителя. Обновление Изделия может быть получено при наличии у пользователя действующего сертификата (ключа) технической поддержки. Также, по запросу, может быть выслано заверенное извещение об изменении формуляра, содержащее контрольные суммы установленного средства защиты информации с примененным обновлением.

11.7. Обновление Изделия осуществляется в соответствии инструкцией ООО «НумаТех», сопровождающей каждое выпускаемое обновление. Подлинность и целостность файла-обновления и документации обеспечивается ЭЦП.

11.8. Обновление комплекса выполняется в следующем порядке:

- получение дистрибутива обновления и инструкции по его применению;
- проведение верификации продукта – проверка ЭЦП загруженных файлов;
- выполнение обновления продукта. По результатам применения обновления делается запись в разделе 18 документа «Формуляр» 643.АМБН.00021-01 30 01.

11.9. При информировании и доведении информации о выявленных недостатках,

обновлении Изделия следует руководствоваться документом «Регламент обновления Изделия и информирования пользователей» 643.АМБН.00021-01 87 01.

12. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

CVE	–	common vulnerabilities and exposures
IP	–	internet protocol
LSU	–	local super user
MAC	–	media access control
RBAC	–	role based access control
АРМ	–	автоматизированное рабочее место
ВМ	–	виртуальная машина
МВМ	–	монитор виртуальной машины
НСД	–	несанкционированный доступ
ОС	–	операционная система
СВТ	–	средство вычислительной техники
СЗИ	–	средство защиты информации
ТУ	–	технические условия
УВМ	–	управляющая виртуальная машина
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭЦП	–	электронная цифровая подпись

ПРИЛОЖЕНИЕ А.
ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

Таблица А.1 – Перечень ссылочных документов

Обозначение	**Наименование**	**Пункт ТУ**
	Журнал учета выпущенных Изделий и учета идентификаторов СЗИ	1.6.3
643.АМБН.00021-01 30 01	Формуляр	1.5.4 1.6.2 10.2 11.8
643.АМБН.00021-01 94 01	Инструкция по проверке контрольных сумм	1.5.5 **Ошибка! Источник ссылки не найден.**
643.АМБН.00021-01 51 01	Программа и методика испытаний	**Ошибка! Источник ссылки не найден.** **Ошибка! Источник ссылки не найден.**
643.АМБН.00021-01 83 01	Технология производства	**Ошибка! Источник ссылки не найден.**

ПРИЛОЖЕНИЕ Б.
РАЗРЕШЕНИЯ ДЛЯ БАЗОВЫХ РОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ ИЗДЕЛИЯ

Таблица Б.1 –Разрешения для базовых ролей пользователей Изделия

Разрешение	**Pool Admin**	**Pool Operator**	**VM Power Admin**	**VM Admin**	**VM Operator**	**Read Only**
Назначение и изменение ролей пользователей	X					
Резервное копирование / восстановление	X					
Импорт / экспорт OVF / OVA контейнеров и образов дисков ВМ	X					
Преобразование виртуальных машин с помощью диспетчера преобразования Numa vServer	X					
Отключение активных пользователей от управления (завершение сеанса работы)	X	X				
Создание и снятие оповещений для пользователей	X	X				
Отмена задачи любого пользователя	X	X				
Управление пулом	X	X				
Управление блокировками подключений	X	X				
Расширенные операции по управлению ВМ	X	X	X			
Создание и удаление ВМ	X	X	X	X		
Изменение подключенных CD образов в ВМ	X	X	X	X	X	
Получение доступа к консоли ВМ	X	X	X	X	X	
Управление операциями отображения для графических инструментов управления	X	X	X	X	X	
Отмена собственных задач	X	X	X	X	X	X

Разрешение	**Pool Admin**	**Pool Operator**	**VM Power Admin**	**VM Admin**	**VM Operator**	**Read Only**
Чтение журналов работы	X	X	X	X	X	X
Подключение к пулу и чтение метаданных пула	X	X	X	X	X	X

ПРИЛОЖЕНИЕ В.
ПЕРЕЧЕНЬ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, РЕАЛИЗУЕМЫХ ИЗДЕЛИЕМ

1. Перечень мер защиты информации, реализуемых Изделием в соответствии с документами:

- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17) [1];
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21) [2];

приведён в таблице 4.

Таблица 4 - Сопоставление мер защиты и заявленных ФБО

Меры защиты	Условное обозначение, согласно приказам ФСТЭК России № 17 [1], № 21 [2]	Пункт ТУ
ИАФ.1	ИАФ.1 [1, 2]	1.4.1.3.1 1.4.1.3.3 1.4.1.3.4
ИАФ.2	ИАФ.2 [1, 2]	1.4.1.1
ИАФ.3	ИАФ.3 [1, 2]	1.4.1.4
ИАФ.4	ИАФ.4 [1, 2]	1.4.1.5
ИАФ.5	ИАФ.5 [1, 2]	1.4.1.6
УПД.1	УПД.1 [1, 2]	1.4.1.2
УПД.2	УПД.2 [1, 2]	1.4.1.2
УПД.6	УПД.6 [1, 2]	1.4.1.5
РСБ.7	РСБ.7 [1, 2]	1.4.3.4 1.4.6.1 (6)
ОЦЛ.1	ОЦЛ.1[1, 2]	1.4.6.2
ЗСВ.1	ЗСВ.1 [1, 2]	1.4.1
ЗСВ.2	ЗСВ.2 [1, 2]	1.4.2
ЗСВ.3	ЗСВ.3 [1, 2]	1.4.3
ЗСВ.4	ЗСВ.4 [1, 2]	1.4.4
ЗСВ.6	ЗСВ.6 [1, 2]	1.4.5
ЗСВ.7	ЗСВ.7 [1, 2]	1.4.6
ЗСВ.8	ЗСВ.8 [1, 2]	1.4.7
ЗСВ.10	ЗСВ.10 [1, 2]	1.4.8
ЗИС.19	ЗИС.19 [1, 2]	1.4.2.5 1.4.2.6

1.1. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ЗСВ.1***:

- Изделие обеспечивает идентификацию и аутентификацию управления средствами виртуализации (пп.1.4.1.3.1);

- Изделие обеспечивает идентификацию и аутентификацию субъектов доступа при их локальном и удаленном обращении к объектам (пп.1.4.1.3.1, пп.1.4.1.3.5);
- Изделие обеспечивает блокировку доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации (пп.1.4.5.1 (2));
- Изделие обеспечивает защиту аутентификационной документации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения и модифицирования (пп.1.4.1.7);
- Изделие обеспечивает защиту аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющим на это полномочий (пп.1.4.1.6);
- Изделие обеспечивает взаимную идентификацию и аутентификацию пользователя и сервера виртуализации при удаленном доступе (пп.1.4.1.3.5).

1.2. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.1***:

- Изделие осуществляет идентификацию и аутентификацию субъектов доступа и объектов доступа, являющихся пользователями Изделия, в соответствии с RBAC и процессов, запускаемых от их имени (пп.1.4.1.3.1).
- Субъекты доступа должны однозначно идентифицироваться и аутентифицироваться при доступе к консоли управления УВМ до разрешения каких-либо действий по администрированию Изделия (пп. 1.4.1.3.3).
- Аутентификация субъектов доступа осуществляется с использованием паролей (пп.1.4.1.3.4).

1.3. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.2***:

- Изделие обеспечивает идентификацию устройств по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства (пп.1.4.1.1).
- Изделие обеспечивает поддержку протоколов аутентификации (iscsi/iser) для аутентификации устройств в информационной системе(пп.1.4.1.1).

1.4. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.3***:

- Изделие обеспечивает следующие возможности по управлению идентификаторами пользователей и (или) устройств:
  1) формирование (создание) администратором Изделия идентификатора, который однозначно идентифицирует пользователя;
  2) присвоение идентификатора пользователю и (или) устройству (пп.1.4.1.4).

1.5. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.4:***

- Изделие обеспечивает следующие функции управления средствами аутентификации (аутентификационной информацией) субъектов доступа:

1) конфигурирование (задание/установку) администратором Изделия следующих параметров паролей пользователей Изделия:

- минимальной сложности пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '’', '”', '.', '?', '<', '>', '«');
- минимального количества символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);
- времени действия пароля, в пределах от 60 до 180 дней;
- максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток.

2) конфигурирование (задание/установку) администратором Изделия следующих параметров автоматической блокировки учетной записи субъекта доступа в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 3 минут до 60 минут (пп.1.4.1.5).

1.6. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.5:***

- Изделие обеспечивает защиту аутентификационной информации (паролей субъектов доступа) в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения действительного значения аутентификационной информации и количества вводимых пользователем символов. Вводимые символы пароля отображаются условными знаками «*», или пустыми символами (пп.1.4.1.6).

1.7. Изделие реализует уникальные заявленные функции безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации:

- Идентификация и аутентификация субъектов доступа и объектов доступа осуществляется программными модулями, входящими в состав УВМ (пп.1.4.1.3.2).
- Субъекты доступа однозначно идентифицируются и аутентифицируются при доступе к консоли управления УВМ до разрешения каких-либо действий по администрированию Изделием (пп.1.4.1.3.3).

1.8. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации* ***ЗСВ.2:***

- Изделие обеспечивает контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры (пп.1.4.2.1 (1));
- Изделие обеспечивает контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды (пп.1.4.2.1 (2));
- Изделие обеспечивает управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа (пп.1.4.2.2);
- Изделие обеспечивает управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектам доступа (1.4.2.3);
- Изделие обеспечивает контроль запуска виртуальных машин на основе заданных правил администратора (пп.1.4.2.3).

1.9. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на управление доступом субъектов доступа к объектам доступа:

- Изделие обеспечивает контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора, в памяти хостовой операционной системы, виртуальных машин и (или) иных объектов доступа (пп.1.4.2.4).
- Изделие обеспечивает функции мандатного контроля доступа для ранжирования и разграничения доступа различных ВМ к виртуальным или аппаратным ресурсам, памяти, процессорам (пп.1.4.2.7).

1.10. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации* ***УПД.1***:

- Изделие обеспечивает ролевую модель управления доступом и администрирования Изделия, при которой пользователями Изделия должны являться субъекты доступа, обладающие различными правами по администрированию Изделия при этом:

а. Изделие должно обеспечивать функции управления доступом на основе ролевой модели (Role Based Access Control, RBAC), в соответствии с которой Изделие должно связывать пользователя (или группу пользователей) с определенной ролью, являющейся именованным набором разрешений по доступу к объектам доступа и действиям по администрированию Изделия в соответствии с Приложением Б.

б. Изделие должно поддерживать роль локального администратора (Local Super User, LSU), обладающая всеми (максимальными) правами и полномочиями по управлению Изделием (пп.1.4.1.2).

1.11. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации* ***УПД.2***:

- Изделие обеспечивает ролевую модель управления доступом и администрирования Изделия, при которой пользователями Изделия должны являться субъекты доступа, обладающие различными правами по администрированию Изделия (пп. 1.4.1.2).

1.12. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации* ***УПД.6***:

- Изделие обеспечивает следующие функции управления средствами аутентификации (аутентификационной информацией) субъектов доступа:

1) конфигурирование (задание/установку) администратором Изделия следующих параметров паролей пользователей Изделия:

- минимальной сложности пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '”', '”', '.', '?', '<', '>', '«');
- минимального количества символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);
- времени действия пароля, в пределах от 60 до 180 дней;
- максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток.

2) конфигурирование (задание/установку) администратором Изделия следующих параметров автоматической блокировки учетной записи субъекта доступа в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 3 минут до 60 минут (пп.1.4.1.5).

1.13. Изделие реализует ряд функций безопасности, направленные на регистрацию событий безопасности в виртуальной инфраструктуре *в части следующих требований к мере защиты информации **ЗСВ.3**:*

- Изделие обеспечивает регистрацию запуска (завершения) работы компонентов виртуальной машины (МВМ и УВМ), а также виртуальных машин (пп.1.4.3.1 (1)), при этом состав и содержание информации, подлежащей регистрации для указанных компонентов виртуальной инфраструктуры, включены:
  - дату и время запуска (завершения) работы;
  - результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная);
  - идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры;
  - тип события;
  - идентификатор события (пп.1.4.3.1. (1а-1д)).
- Изделие обеспечивает регистрацию запуска (завершения) программ и процессов в УВМ (как компонент виртуальной инфраструктуры), при этом регистрации подлежат дата и время запуска (завершения) программ и процессов, тип события, идентификатор события (пп.1.4.3.1 (2)).
- Изделие обеспечивает регистрацию доступа субъектов доступа к компонентам виртуальной инфраструктуры (УВМ, а также виртуальным машинам) (пп.1.4.3.1 (3)), при этом при доступе (входе или выходе) к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают:
  - дату и время доступа субъектов;
  - результат попытки доступа субъектов (успешная или неуспешная),
  - идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры;
  - тип события;
  - идентификатор события (пп.1.4.3.1 (3а-3д)).
- Изделие обеспечивает регистрацию внесения изменений в состав и конфигурацию компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения (пп.1.4.3.1 (4)), при этом состав и содержание информации, подлежащей регистрации, включены:
  - дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании;
  - результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры;
  - тип события;
  - идентификатор события (пп.1.4.3.1 (4а-4г)).
- Изделие обеспечивает регистрацию создания/удаления ВМ, при этом состав и содержание информации, подлежащей регистрации, должны включать:
  - дату и время;
  - тип события;
  - идентификатор события (пп.1.4.3.1 (5а-5в).
- Изделие обеспечивает регистрацию изменения ролевой модели, при этом состав и содержание информации, подлежащей регистрации, должны включать:

- дату и время;
- тип события;
- идентификатор события (пп.1.4.3.1 (6а-6в).

- Изделие обеспечивает регистрацию нарушения целостности объектов контроля, при этом состав и содержание информации, подлежащей регистрации, должны включать:
  - дату и время;
  - тип события;
  - идентификатор события (пп.1.4.3.1 (7а-7в).
- Изделие обеспечивает возможность централизованного сбора, хранения, экспорта и анализа информации о зарегистрированных событиях безопасности виртуальной инфраструктуры (пп.1.4.3.2);
- Изделие обеспечивает регистрацию событий безопасности, связанных с перемещением и размещением виртуальных машин (пп.1.4.3.3).

1.14. Изделие реализует ряд функций безопасности, направленные на защиту информации о событиях безопасности *в части следующих требований к мере защиты информации* ***РСБ.7:***

- Изделие обеспечивает возможность резервного копирования журнала регистрации событий (пп.1.4.3.4).
- Изделие обеспечивает возможность контроля целостности в процессе загрузки и (или) динамически журнала аудита (пп.1.4.6.1 (6)).

1.15. Изделие реализует ряд функций безопасности, направленные на управлении потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры *в части следующих требований к мере защиты информации* ***ЗСВ.4:***

- Изделие обеспечивает отключение сетевых протоколов неиспользуемых компонентами виртуальной инфраструктуры (МВМ, УВМ), а также в виртуальной вычислительной сети (пп.1.4.4.1 (2));
- Изделие обеспечивает подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов (пп.1.4.4.1 (3));
- Изделие обеспечивает изоляцию потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (МВМ, УВМ) и сетевых потоков виртуальной вычислительной сети (1.4.4.1 (4));
- Изделие обеспечивает изоляцию сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях и для каждой виртуальной машины (пп.1.4.4.1 (5));
- Изделие обеспечивает возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой (пп.1.4.4.1 (6)).

1.16. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры:

- Изделие обеспечивает управление потоками между компонентами виртуальной инфраструктуры (пп.1.4.4.1(1)).

1.17. Изделие реализует ряд функций безопасности, направленные на управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных *в части следующих требований к мере защиты информации* ***ЗСВ.6:***

- Изделие обеспечивает управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных) (пп.1.4.5.1 (1));

- Изделие обеспечивает управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации (пп.1.4.5.1 (2));
- Изделие обеспечивает управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных) (пп.1.4.5.1 (3));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) полный запрет перемещения виртуальных машин (контейнеров) (пп.1.4.5.2 (1));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) ограничение перемещения виртуальных машин (контейнеров) в пределах виртуальных сред, созданных для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментов информационных систем, развернутых в среде виртуализации (пп.1.4.5.2 (2));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) ограничение перемещения виртуальных машин (контейнеров) между виртуальными средами, созданными для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментами информационных систем, развернутых в среде виртуализации (пп.1.4.5.2 (3));
- Изделие обеспечивает возможность централизованного управления механизмами управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.3);
- Изделие должно обеспечивать обработку отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.4);
- Изделие должно обеспечивать непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения (пп.1.4.5.5);
- Изделие должно обеспечивать очистку освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.6).

Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на управление перемещением виртуальных машин (контейнеров и обрабатываемых на них данных):

- Изделие обеспечивает стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуального аппаратного обеспечения (пп.1.4.5.7 (1)), файлов-образов ВМ (пп.1.4.5.7 (2)).

1.18. Изделие реализует ряд функций безопасности, направленные на контроль целостности виртуальной инфраструктуры и ее конфигурации *в части следующих требований к мере защиты информации **ЗСВ.7:***

- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически состава и конфигурации виртуального аппаратного обеспечения (пп.1.4.6.1 (1));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин (пп.1.4.6.1 (2));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем. Контроль целостности должен проводиться только, когда файлы-образы не задействованы (пп.1.4.6.1 (3));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически резервных копий виртуальных машин (пп.1.4.6.1 (4));

- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически состава аппаратной части компонентов виртуализированной инфраструктуры (пп.1.4.6.1 (5))
- Изделие обеспечивает возможность контроля целостности в процессе загрузки и (или) динамически журнала аудита (пп.1.4.6.1 (6)).

1.19. Изделие реализует ряд функций безопасности направленных на контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации *в части следующих требований к мере защиты информации* ***ОЦЛ.1:***

- Изделие обеспечивает блокировку запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности (пп. 1.4.6.2).

1.20. Изделие реализует ряд функций безопасности, направленные на резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры *в части следующих требований к мере защиты информации* ***ЗСВ.8:***

- Изделие обеспечивает резервное копирование виртуальных машин (пп.1.4.7.1 (1));
- Изделие обеспечивает резервное копирование конфигурации виртуальной инфраструктуры (1.4.7.1 (2));
- Изделие обеспечивает резервное копирование данных, обрабатываемых в виртуальной инфраструктуре (пп.1.4.7.1 (1), пп.1.4.7.1 (3), пп.1.4.7.1(4)).

1.21. Изделие реализует ряд функций безопасности, направленные на изоляцию процессов (выполнение программ) в выделенной области памяти, *в части следующих требований к мере защиты информации* ***ЗИС.19:***

- Изделие должно обеспечивать реализацию механизмов изоляции программных модулей одного процесса от другого (пп.1.4.2.5);
- Изделие должно обеспечивать гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга (пп.1.4.2.6).

1.22. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры:

- Изделие обеспечивает резервное копирование ВМ, при этом Изделие поддерживает следующие механизмы:

6) механизм снимков ВМ (snapshot), который обеспечивает возможность создания снимка виртуальной машины, в котором будет зафиксировано ее текущее состояние, и возможность последующего возвращения к этому снимку (пп1.4.7.1 (1а));

7) механизм экспорта (выгрузки) ВМ на выделенное хранилище (пп.1.4.7.1 (1б)).

- Изделие обеспечивает резервное переназначение мастер пула (пп.1.4.7.1 (5));
- Изделие обеспечивает возможность резервирование каналов связи, используемых в виртуальной инфраструктуре (пп.1.4.7.2).

1.23. Изделие реализует ряд уникальных функции безопасности, направленные на разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей:

- Изделие обеспечивает возможность создание изолированных виртуальных зон, предназначенных для решения выделенных (обособленных) задач (пп.1.4.8.1).
- Изделие обеспечивает возможность сегментирования виртуальной инфраструктуры (виртуальных вычислительных сетей) посредством создания логических локальных сетей (пп.1.4.8.2).

- УВМ обеспечивает недоступность со стороны объектов и процессов, исполняющихся на ВМ (пп.1.4.8.3).

1.24. Изделие реализует ряд уникальных заявленных функций безопасности, направленных на обеспечение возможности следующих действий: создание, удаление, запуск, остановку, конфигурацию ВМ и т.д., включая назначение меток безопасности, а также экспорт и импорт ВМ и управление шаблонами ВМ (пп.1.4.9).

2. Конкретный перечень мер защиты информации, реализуемых Изделием в соответствии с документами:

- «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (утвержденные приказом ФСТЭК России от 14 марта 2014 № 31) [1];
- «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утвержденные приказом ФСТЭК России от 25 декабря 2017 г. №239) [2],

приведён в таблице 5.

Таблица 5 - Сопоставление мер защиты и ФБО

Меры защиты	Условное обозначение, согласно приказам ФСТЭК России № 31 [1], № 239 [2]	Пункт ТУ
ИАФ.1	ИАФ.1 [1, 2]	1.4.1.3.1 1.4.1.3.3 1.4.1.3.4
ИАФ.2	ИАФ.2 [1, 2]	1.4.1.1
ИАФ.3	ИАФ.3 [1, 2]	1.4.1.4
ИАФ.4	ИАФ.4 [1, 2]	1.4.1.5
ИАФ.7	ИАФ.7 [1, 2]	1.4.1.6
УПД.1	УПД.1 [1, 2]	1.4.1.2
УПД.2	УПД.2 [1, 2]	1.4.1.2
УПД.6	УПД.6 [1, 2]	1.4.1.5
АУД.4	АУД.4 [1, 2]	1.4.3.1 1.4.3.2 1.4.3.3
АУД.6	АУД.6 [1, 2]	1.4.3.4 1.4.6.1 (6)
ОЦЛ.1	ОЦЛ.1 [1, 2]	1.4.6.1 1.4.6.2
ОДТ.2	ОДТ.2 [1, 2]	1.4.7.1 1.4.7.2
ЗИС.4	ЗИС.4 [1, 2]	1.4.8.1 1.4.8.2 1.4.8.3
ЗИС.12	ЗИС.12 [1, 2]	1.4.2.5 1.4.2.6
ЗИС.39	ЗИС.39 [1, 2]	1.4.5.1 1.4.5.2

Меры защиты	Условное обозначение, согласно приказам ФСТЭК России № 31 [1], № 239 [2]	Пункт ТУ
		1.4.5.3 1.4.5.4 1.4.5.5 1.4.5.6 1.4.5.7

2.1. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.1***:

- Изделие осуществляет идентификацию и аутентификацию субъектов доступа и объектов доступа, являющихся пользователями Изделия, в соответствии с RBAC и процессов, запускаемых от их имени (пп.1.4.1.3.1).
- Субъекты доступа должны однозначно идентифицироваться и аутентифицироваться при доступе к консоли управления УВМ до разрешения каких-либо действий по администрированию Изделия (пп. 1.4.1.3.3).
- Аутентификация субъектов доступа осуществляется с использованием паролей (пп.1.4.1.3.4).

2.2. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.2***:

- Изделие обеспечивает идентификацию устройств по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства (пп.1.4.1.1).
- Изделие обеспечивает поддержку протоколов аутентификации (isici/iser) для аутентификации устройств в информационной системе(пп.1.4.1.1).

2.3. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.3***:

- Изделие обеспечивает следующие возможности по управлению идентификаторами пользователей и (или) устройств:

1) формирование (создание) администратором Изделия идентификатора, который однозначно идентифицирует пользователя;
2) присвоение идентификатора пользователю и (или) устройству (пп.1.4.1.4).

2.4. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации* ***ИАФ.4:***

- Изделие обеспечивает следующие функции управления средствами аутентификации (аутентификационной информацией) субъектов доступа:

1) конфигурирование (задание/установку) администратором Изделия следующих параметров паролей пользователей Изделия:

- минимальной сложности пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '”', '”', '.', '?', '<', '>', '«');
- минимального количества символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);
- времени действия пароля, в пределах от 60 до 180 дней;
- максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток.

2) конфигурирование (задание/установку) администратором Изделия следующих параметров автоматической блокировки учетной записи субъекта доступа в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 3 минут до 60 минут (пп.1.4.1.5).

2.5. Изделие реализует ряд функций безопасности, направленные на идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации *в части следующих требований к мере защиты информации **ИАФ.7:***

Изделие обеспечивает защиту аутентификационной информации (паролей субъектов доступа) в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения действительного значения аутентификационной информации и количества вводимых пользователем символов. Вводимые символы пароля отображаются условными знаками «*», или пустыми символами (пп.1.4.1.6).

2.6. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации **УПД.1***:

- Изделие обеспечивает ролевую модель управления доступом и администрирования Изделия, при которой пользователями Изделия должны являться субъекты доступа, обладающие различными правами по администрированию Изделия при этом:
  - Изделие должно обеспечивать функции управления доступом на основе ролевой модели (Role Based Access Control, RBAC), в соответствии с которой Изделие должно связывать пользователя (или группу пользователей) с определенной ролью, являющейся именованным набором разрешений по доступу к объектам доступа и действиям по администрированию Изделия в соответствии с Приложением Б.
  - Изделие должно поддерживать роль локального администратора (Local Super User, LSU), обладающая всеми (максимальными) правами и полномочиями по управлению Изделием (пп.1.4.1.2).

2.7. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации **УПД.2***:

- Изделие обеспечивает ролевую модель управления доступом и администрирования Изделия, при которой пользователями Изделия должны являться субъекты доступа, обладающие различными правами по администрированию Изделия (пп. 1.4.1.2).

2.8. Изделие реализует ряд функций безопасности, направленные на управление доступом субъектов доступа к объектам доступа *в части следующих требований к мере защиты информации **УПД.6***:

- Изделие обеспечивает следующие функции управления средствами аутентификации (аутентификационной информацией) субъектов доступа:

1) конфигурирование (задание/установку) администратором Изделия следующих параметров паролей пользователей Изделия:

- минимальной сложности пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '’', '”', '.', '?', '<', '>', '«');
- минимального количества символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);
- времени действия пароля, в пределах от 60 до 180 дней;
- максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток.
- конфигурирование (задание/установку) администратором Изделия следующих параметров автоматической блокировки учетной записи субъекта доступа в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 3 минут до 60 минут (пп.1.4.1.5).

2.9. Изделие реализует ряд функций безопасности, направленные на защиту информации о событиях безопасности *в части следующих требований к мере защиты информации* ***АУД.6:***

- Изделие обеспечивает возможность резервного копирования журнала регистрации событий (пп.1.4.3.4).
- Изделие обеспечивает возможность контроля целостности в процессе загрузки и (или) динамически журнала аудита (пп.1.4.6.1 (6)).

2.10. Изделие реализует ряд функций безопасности, направленные на регистрацию событий безопасности *в части следующих требований к мере защиты информации* ***АУД.4:***

- Изделие обеспечивает регистрацию запуска (завершения) работы компонентов виртуальной машины (МВМ и УВМ), а также виртуальных машин (пп.1.4.3.1 (1)), при этом состав и содержание информации, подлежащей регистрации для указанных компонентов виртуальной инфраструктуры, включены:
  - дату и время запуска (завершения) работы;
  - результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная);
  - идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры;
  - тип события;
  - идентификатор события (пп.1.4.3.1. (1а-1д)).
- Изделие обеспечивает регистрацию запуска (завершения) программ и процессов в УВМ (как компонент виртуальной инфраструктуры), при этом регистрации подлежат дата и время запуска (завершения) программ и процессов, тип события и идентификатор события (пп.1.4.3.1 (2)).
- Изделие обеспечивает регистрацию доступа субъектов доступа к компонентам виртуальной инфраструктуры (УВМ, а также виртуальным машинам) (пп.1.4.3.1 (3)), при этом при доступе (входе или выходе) к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают:
  - дату и время доступа субъектов;
  - результат попытки доступа субъектов (успешная или неуспешная),
  - идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры;
  - тип события;
  - идентификатор события (пп.1.4.3.1 (3а-3д)).

- Изделие обеспечивает регистрацию внесения изменений в состав и конфигурацию компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения (пп.1.4.3.1 (4)), при этом состав и содержание информации, подлежащей регистрации, включены:
    - дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании;
    - результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры;
    - тип события;
    - идентификатор события (пп.1.4.3.1 (4а-4г));
- Изделие обеспечивает регистрацию создания/удаления ВМ, при этом состав и содержание информации, подлежащей регистрации, должны включать:
    - дату и время;
    - тип события;
    - идентификатор события (пп.1.4.3.1 (5а-5в).
- Изделие обеспечивает регистрацию изменения ролевой модели, при этом состав и содержание информации, подлежащей регистрации, должны включать:
    - дату и время;
    - тип события;
    - идентификатор события (пп.1.4.3.1 (6а-6в).
- Изделие обеспечивает регистрацию нарушения целостности объектов контроля, при этом состав и содержание информации, подлежащей регистрации, должны включать:
    - дату и время;
    - тип события;
    - идентификатор события (пп.1.4.3.1 (7а-7в).
- Изделие обеспечивает возможность централизованного сбора, хранения, экспорта и анализа информации о зарегистрированных событиях безопасности виртуальной инфраструктуры (пп.1.4.3.2);
- Изделие обеспечивает регистрацию событий безопасности, связанных с перемещением и размещением виртуальных машин (пп.1.4.3.3).

2.11. Изделие реализует ряд функций безопасности направленных на Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации *в части следующих требований к мере защиты информации* ***ОЦЛ.1:***

- Изделие обеспечивает блокировку запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности (пп. 1.4.6.2).
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически состава и конфигурации виртуального аппаратного обеспечения (пп.1.4.6.1 (1));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин (пп.1.4.6.1 (2));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем.

Контроль целостности должен проводиться только, когда файлы-образы не задействованы (пп.1.4.6.1 (3));

- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически резервных копий виртуальных машин (пп.1.4.6.1 (4));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически состава аппаратной части компонентов виртуализированной инфраструктуры (пп.1.4.6.1 (5));
- Изделие обеспечивает контроль целостности в процессе загрузки и (или) динамически журнала аудита (пп.1.4.6.1 (6)).

2.12. Изделие реализует ряд функций безопасности, направленные на резервирование систем и средств, *в части следующих требований к мере защиты информации* ***ОДТ.2:***

- Изделие обеспечивает резервное копирование виртуальных машин (пп.1.4.7.1 (1));
- Изделие обеспечивает резервное копирование конфигурации виртуальной инфраструктуры (1.4.7.1 (2));
- Изделие обеспечивает резервное копирование данных, обрабатываемых в виртуальной инфраструктуре (пп.1.4.7.1 (1), пп.1.4.7.1 (3), пп.1.4.7.1(4)).

2.13. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры:

- Изделие обеспечивает резервное копирование ВМ, при этом Изделие поддерживает следующие механизмы:
  - механизм снимков ВМ (snapshot), который обеспечивает возможность создания снимка виртуальной машины, в котором будет зафиксировано ее текущее состояние, и возможность последующего возвращения к этому снимку (пп1.4.7.1 (1а));
  - механизм экспорта (выгрузки) ВМ на выделенное хранилище (пп.1.4.7.1 (1б)).
- Изделие обеспечивает резервное переназначение мастер пула (пп.1.4.7.1 (5));
- Изделие обеспечивает возможность резервирование каналов связи, используемых в виртуальной инфраструктуре (пп.1.4.7.2).

2.14. Изделие реализует ряд функций безопасности, направленные на сегментирование информационной системы, *в части следующих требований к мере защиты информации* ***ЗИС.4***:

- Изделие обеспечивает возможность создание изолированных виртуальных зон, предназначенных для решения выделенных (обособленных) задач (пп.1.4.8.1).
- Изделие обеспечивает возможность сегментирования виртуальной инфраструктуры (виртуальных вычислительных сетей) посредством создания логических локальных сетей (пп.1.4.8.2).
- УВМ обеспечивает недоступность со стороны объектов и процессов, исполняющихся на ВМ (пп.1.4.8.3).

2.15. Изделие реализует ряд функций безопасности, направленные на изоляцию процессов (выполнение программ) в выделенной области памяти, *в части следующих требований к мере защиты информации* ***ЗИС.12:***

- Изделие должно обеспечивать реализацию механизмов изоляции программных модулей одного процесса от другого (пп.1.4.2.5);
- Изделие должно обеспечивать гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга (пп.1.4.2.6).

2.16. Изделие реализует ряд функций безопасности, направленные на управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных *в части следующих требований к мере защиты информации* ***ЗИС.39:***

- Изделие обеспечивает управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных) (пп.1.4.5.1 (1));
- Изделие обеспечивает управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации (пп.1.4.5.1 (2));
- Изделие обеспечивает управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных) (пп.1.4.5.1 (3));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) полный запрет перемещения виртуальных машин (контейнеров) (пп.1.4.5.2 (1));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) ограничение перемещения виртуальных машин (контейнеров) в пределах виртуальных сред, созданных для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментов информационных систем, развернутых в среде виртуализации (пп.1.4.5.2 (2));
- Изделие обеспечивает в рамках управления перемещением виртуальных машин (контейнеров) ограничение перемещения виртуальных машин (контейнеров) между виртуальными средами, созданными для запуска и исполнения ВМ, предназначенных для обработки разнородной информации, или сегментами информационных систем, развернутых в среде виртуализации (пп.1.4.5.2 (3));
- Изделие обеспечивает возможность централизованного управления механизмами управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.3);
- Изделие должно обеспечивать обработку отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.4);
- Изделие должно обеспечивать непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения (пп.1.4.5.5);
- Изделие должно обеспечивать очистку освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных (пп.1.4.5.6).
- Изделие обеспечивает стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуального аппаратного обеспечения (пп.1.4.5.7 (1)), файлов-образов ВМ (пп.1.4.5.7 (2)).

2.17. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на управление перемещением виртуальных машин (контейнеров и обрабатываемых на них данных):

- Изделие обеспечивает стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуального аппаратного обеспечения (пп.1.4.5.7 (1)), файлов-образов ВМ (пп.1.4.5.7 (2)).

2.18. Изделие обеспечивает реализацию уникальных заявленных функций безопасности направленных на управление информационными потоками между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры:

- Изделие обеспечивает управление информационными потоками между компонентами виртуальной инфраструктуры (пп.1.4.4.1(1)).

2.19. Изделие обеспечивает реализацию уникальных заявленных функций безопасности, направленных на обеспечение возможности следующих действий: создание, удаление, запуск, остановку, конфигурацию ВМ и т.д., включая назначение меток безопасности, а также экспорт и импорт ВМ и управление шаблонами ВМ (пп.1.4.9).

ПРИЛОЖЕНИЕ Г.
УГРОЗЫ, КОТОРЫМ ПРОТИВОСТОИТ ИЗДЕЛИЕ

Нумерация и наименование угроз, соответствует угрозам, зарегистрированным в Банке данных угроз безопасности информации ФСТЭК России https://bdu.fstec.ru.

Примечание. Данные актуальны на 13.06.2023.

УБИ.008 Угроза восстановления и (или) повторного использования аутентификационной информации

Описание угрозы

Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хеша пароля, для восстановления сеанса.

Данная угроза обусловлена следующими недостатками:

- значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой (время подбора хеш-кодов меньше времени полного перебора аутентификационной информации);
- слабостями алгоритма расчёта хеш-кода, допускающими его повторное использование для выполнения успешной аутентификации.

Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную».

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя.

Последствия реализации угрозы

Нарушение конфиденциальности.

Применяемые меры противодействия угрозе:

Для противодействия визуального перехвата вводимой аутентификационной информации в Изделии реализован метод защиты обратной связи при вводе аутентификационной информации при доступе к функциональным возможностям программного Изделия (мера защиты информации ИАФ.5): Вводимые символы пароля отображаются условными знаками. Для минимизации вероятности получения доступа методом подбора пароля программное Изделие имеет возможность задания параметров сложности парольной информации, наложения ограничений на количество неуспешных попыток аутентификации и время между последовательными попытками неуспешной аутентификации (в рамках реализации требований мер защиты информации ИАФ.4, УПД.6). Аутентификационная информация не передается в открытом виде.

УБИ.010 Угроза выхода процесса за пределы виртуальной машины

Описание угрозы

Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора.

Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора.

Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора.

Источник угрозы

Внутренний нарушитель со средним потенциалом.
Внешний нарушитель со средним потенциалом.

Объект воздействия

Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга.

Для противодействия данной угрозы Изделие обеспечивает возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой, согласно требованиям, предъявляемой мерой ЗСВ.4.

Обеспечивается контроль целостности файлов-образов, визуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем в соответствии с требованиями, предъявляемыми мерами защиты ЗСВ.7.

УБИ.031 Угроза использования механизмов авторизации для повышения привилегий

Описание угрозы

Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки.

Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам.

Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение.

Последствия реализации угрозы

Нарушение конфиденциальности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе, в Изделии все операции, связанные с определением уровня полномочий пользователей программного Изделия (ролей), производятся администраторами Изделия. Полномочия администраторов и пользователей программного Изделия разделены и регламентированы (в соответствии с требованиями, предъявляемыми мерами защиты информации УПД.2 (ролевой доступ), ЗСВ.1.

УБИ.044 Угроза нарушения изоляции пользовательских данных внутри виртуальной машины

Описание угрозы

Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины.

Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины.

Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Виртуальная машина, гипервизор.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга. Обеспечивается контроль целостности файлов-образов, визуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем в соответствии с требованиями, предъявляемыми мерами защиты ЗСВ.7.

УБИ.046 Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия

Описание угрозы

Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия.

Данная угроза обусловлена 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 её уровнями.

Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает идентификацию и аутентификацию физических и виртуальных устройств по логическим именам (имя устройства и (или) ID), логическим адресам, и (или) по физическим адресам устройства или по комбинации имени, логического и (или) физического адреса, в соответствии с требованиями, предъявляемыми мерами ИАФ.2, ЗСВ.1. Изделие обеспечивает поддержку протоколов аутентификации iscsi/iser для аутентификации устройств в информационной системе. Субъекты доступа однозначно идентифицируются и аутентифицируются при доступе к консоли управления Изделием до разрешения каких-либо действий по администрированию Изделием. Аутентификация субъектов доступа осуществляется с использованием паролей, согласно требованиям, предъявляемыми мерами защиты ЗСВ.1. В случае удаленного подключения обеспечивается использование протокола ssh с взаимной аутентификацией.

УБИ.048 Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин

Описание угрозы

Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин.

Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации.

Реализация данной угрозы может привести:

- к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов;

- к нарушению целостности программ, установленных на виртуальных машинах;
- к нарушению доступности ресурсов виртуальных машин;
- к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы).

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды в соответствии с RBAC (мера ЗСВ.1).

Изделие обеспечивает контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем, согласно требованиям, предъявляемой мерой ЗСВ.7.

Изделие обеспечивается блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности, согласно требованиям, предъявляемой мерой ОЦЛ.1.

УБИ.058 Угроза неконтролируемого роста числа виртуальных машин

Описание угрозы

Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин.

Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин.

Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура.

Последствия реализации угрозы

Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы в Изделии предусмотрены и задокументированы рекомендации к минимальному объему для того, чтобы Изделие могло функционировать в штатном режиме.

При достижении заявленного лимита Изделие не позволит создать новые ВМ, и продолжит свою работу в штатном режиме.

УБИ.073 Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети

Описание угрозы

Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования.

Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса.

Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает контроль целостности МВМ, УВМ, состава и конфигурации виртуального оборудования, файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин, файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем, согласно требованиям, предъявляемой мерой ЗСВ.7.

Обеспечивается блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности (ОЦЛ.1).

УБИ.075 Угроза несанкционированного доступа к виртуальным каналам передачи

Описание угрозы

Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий.

Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных).

Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Сетевое программное обеспечение, сетевой трафик, виртуальные устройства.

Последствия реализации угрозы

Нарушение конфиденциальности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает возможность резервирования каналов связи, используемых в виртуальной инфраструктуре, согласно требованиям, предъявляемой мерой ЗСВ.8.

Изделие обеспечивает управление сетевым трафиком между компонентами виртуальной инфраструктуры, отключение сетевых протоколов, неиспользуемых компонентами виртуальной инфраструктуры, а также виртуальной вычислительной сети, согласно требованиям, предъявляемой мерой ЗСВ.4.

Обеспечивается подлинность сетевых соединений внутри ВИ, в том числе для защиты от подмены сетевых устройств и сервисов, обеспечивается изоляции потоков данных, передаваемых и обрабатываемых МВМ, УВМ и сетевых потоков виртуальной вычислительной сети, изоляция сетевого трафика от (к) каждой гостевой ОС в виртуальных сетях и для каждой виртуальной машины, согласно требованиям, предъявляемой мерой ЗСВ.4.

УБИ.076 Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети

Описание угрозы

Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети.

Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности.

Реализация данной угрозы возможна в одном из следующих случаев:

- наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин;
- наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Гипервизор.

Последствия реализации угрозы

Нарушение доступности.

Применяемые меры противодействия угрозе:

Для предотвращений данной угрозы Изделие обеспечивает отключение сетевых протоколов, неиспользуемых компонентами виртуальной инфраструктуры (МВМ УВМ), а также виртуальной вычислительной сети. Обеспечивается изоляция потоков данных, передаваемых и обрабатываемых МВМ УВМ и сетевых протоколов внутри виртуальной вычислительной сети, обеспечивается запрет прямого воздействия ВМ между собой, согласно требованиям, предъявляемым мерой ЗСВ.4.

УБИ.077 Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

Описание угрозы

Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки.

Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины.

Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины.

Источник угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом

Объект воздействия

Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные.

Последствия реализации угрозы

Нарушение целостности. Нарушение доступности

Применяемые меры противодействия угрозе:

Обеспечивается изоляция потоков данных, передаваемых и обрабатываемых МВМ УВМ и сетевых протоколов внутри виртуальной вычислительной сети, обеспечивается запрет прямого воздействия ВМ между собой, согласно требованиям, предъявляемым мерой ЗСВ.4.

УБИ.078 Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети

Описание угрозы

Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации.

Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами.

Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Виртуальная машина.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделием обеспечивается контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды, согласно требованиям, предъявляемой мерой ЗСВ.7.

Обеспечивается контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы), согласно требованиям, предъявляемой мерой ЗСВ.7.

УБИ.079 Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин

Описание угрозы

Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с

помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе.

Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре.

Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Виртуальная машина.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой, согласно требованиям, предъявляемой мерой ЗСВ.4.

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

УБИ.080 Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети

Описание угрозы

Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации.

Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами.

Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Виртуальные устройства хранения, обработки и передачи данных.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой, согласно требованиям, предъявляемой мерой ЗСВ.4.

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

УБИ.084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети

Описание угрозы

Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных).

Данная угроза обусловлена наличием 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 с высокой сложностью алгоритмов обеспечения согласованности действий по распределению 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.

Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.).

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Виртуальные устройства хранения данных, виртуальные диски.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает возможность контроля (запрета) прямого взаимодействия виртуальных машин между собой, согласно требованиям, предъявляемой мерой ЗСВ.4.

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

Также для противодействия данной угрозы Изделие обеспечивает гарантированную изоляцию страниц памяти разных виртуальных машин друг от друга.

УБИ.085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации

Описание угрозы

Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации.

Данная угроза обусловлена тем, что 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.

Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Носитель информации, объекты файловой системы.

Последствия реализации угрозы

Нарушение конфиденциальности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозы Изделие обеспечивает возможность создания виртуальной вычислительной сети (виртуальных каналов связи) для ВМ и (или) виртуальных зон, с возможностью контроля и управления информационными потоками, исключающим НСД к защищаемой информации, включая защиту информационно-управляющих сообщений (служебных информационных сообщений) и конфигурационной информации.

Изделие обеспечивает стирание остаточной информации, образующейся после удаления фалов образов ВМ.

Обеспечивается контроль целостности файлов-образов, визуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем в соответствии с требованиями, предъявляемыми мерами защиты ЗСВ.7.

УБИ.086 Угроза несанкционированного изменения аутентификационной информации

Описание угрозы

Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.

Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации.

Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр.

Последствия реализации угрозы

Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе, в Изделии все операции с идентификаторами пользователей, со средствами аутентификации – производятся администраторами (в части реализации мер защиты ИАФ.3, ИАФ.4). Полномочия администраторов и пользователей программного Изделия разделены и регламентированы (в соответствии с требованиями, предъявляемыми мерами защиты информации ролевой доступ. В соответствии с требованиями меры защиты информации.

УБИ.090 Угроза несанкционированного создания учётной записи пользователя

Описание угрозы

Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам).

Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации.

Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе).

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе в Изделии все операции, связанные с созданием, модификацией и удалением учетных записей пользователей Изделия выполняются администраторами (в части реализации мер защиты ИАФ.3, ЗСВ.1, УПД.1, ЗСВ.2). Полномочия администраторов и пользователей программного Изделия разделены и регламентированы.

УБИ 100 Угроза обхода некорректно настроенных механизмов аутентификации

Описание угрозы

Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата).

Данная угроза обусловлена в случае некорректных значений параметров конфигурации средств аутентификации и (или) отсутствием контроля входных данных.

Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации.

Источники угрозы

Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение, сетевое программное обеспечение.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе в Изделии реализован механизм контроля аутентификационной информации при ее вводе, реализована настройка параметров сложности парольной информации, не допускающая применения «пустых» паролей, или паролей, обладающих низкой сложностью (в части реализации меры защиты ИАФ.4), настройка параметров парольной защиты выполняется администратором Изделия. Для противодействия специальным программным средствам также реализованы требования меры защиты информации УПД.6, в части задания количества неуспешных попыток аутентификации, и времени, на которое блокируется используемый идентификатор пользователя при достижении данного ограничения. В соответствии с требованиями меры защиты информации РСБ.3 осуществляется регистрация событий безопасности, связанных с аутентификацией пользователей и администраторов.

УБИ.108 Угроза ошибки обновления гипервизора

Описание угрозы

Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления.

Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора.

Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора:

- сбоев в процессе его обновления;
- обновлений, в ходе которых внедряются новые ошибки в код гипервизора;
- обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования;
- других инцидентов безопасности информации.

Источники угрозы

Внутренний нарушитель с низким потенциалом.

Объект воздействия

Системное программное обеспечение, гипервизор.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Обновление Изделия осуществляется только путем обновления файл-прошивки, скачанной с официальных ресурсов предприятия-разработчика, у которых организован процесс безопасной разработки ПО. Файл-обновление дополнительно подписывается согласно ГОСТ Р 34.10, при обновлении Изделие проводит контроль целостности файла путем проверки валидности и верифицированности цифровой подписи по ГОСТ Р 34.10-2012.

УБИ.119 Угроза перехвата управления гипервизором

Описание угрозы

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём эксплуатации уязвимостей консоли управления гипервизором.

Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.

Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Системное программное обеспечение, гипервизор, консоль управления гипервизором.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе Изделие обеспечивает доступ к компонентам Изделия согласно утвержденной ролевой модели (ИАФ.1, УПД.1, ЗСВ.1).

Изделие обеспечивает функции мандатного контроля доступа для ранжирования и разграничения доступа различных ВМ к виртуальным или аппаратным ресурсам, памяти, процессорам.

УБИ.120 Угроза перехвата управления средой виртуализации

Описание угрозы

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и

управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой.

Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.

Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой.

Источники угрозы

Внутренний нарушитель со средним потенциалом. Внешний нарушитель со средним потенциалом.

Объект воздействия

Информационная система, системное программное обеспечение.

Последствия реализации угрозы

Нарушение конфиденциальности. Нарушение целостности. Нарушение доступности.

Применяемые меры противодействия угрозе:

Для противодействия данной угрозе Изделие обеспечивает доступ к компонентам Изделия согласно утвержденной ролевой модели (ИАФ.1, УПД.1, ЗСВ.1).

Изделие обеспечивает функции мандатного контроля доступа для ранжирования и разграничения доступа различных ВМ к виртуальным или аппаратным ресурсам, памяти, процессорам.