Общество с ограниченной ответственностью «Нума Технологии»

Серверная доверенная виртуальная среда функционирования программных средств Numa vServer

Технические условия

643.АМБН.00021-01 90 01

Краткая выписка

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

2021

Литера

О ДОКУМЕНТЕ

Идентификация документа

Название документа	Технические условия. Краткая выписка
Версия документа	Версия 1.0.0.
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 краткой выпиской из документа «Технических условий» 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;
- Приложение Б. Разрешение для базовых ролей пользователей Изделия;
- Приложение В. Перечень мер защиты информации, реализуемых Изделием;
- Приложение Г. Угрозы, которым противостоит Изделие.

В документе сохранена оригинальная нумерация.

СОДЕРЖАНИЕ

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 обществом с ограниченной ответственностью «Нума Технологии» (196084, г. Санкт-Петербург, ул. Цветочная, д. 18, литера А, оф. 424).

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 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.

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.

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

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:

1) 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.

2) 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. Аутентификация субъектов доступа должна осуществляться с использованием паролей.

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) 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:

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.

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.

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 изоляция 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:

1) 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.

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

3) 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.

4) 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;

6. 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.

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.

1.4.4. 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.

1.4.6. Контроль целостности виртуальной инфраструктуры и ее конфигураций

1.4.6.1. Изделие должно обеспечивать возможность контроля целостности:

1) 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.

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.

1.4.7. 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:

a. 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.

1.5. Комплектность

1.5.1. Изделие должно поставляться в виде установочного образа, 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 пользователя643.АМБН.00021-01 94 01 Инструкция по проверке контрольных сумм 643.АМБН.00021-01 30 02 Формуляр. Приложение А 643.АМБН.00021-01 30 03 Формуляр. Приложение Б		На электронном носителе Идентификатор СЗИ: РОСС RU.0001.xxxx.xxxxxx
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.xxxx.xxxxxx
2	Документация в составе: 643.АМБН.00021-01 32 01 Руководство администратора. Установка, настройка Numa vServer 643.АМБН.00021-01 34 01 Руководство пользователя643.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.

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 Б.
РАЗРЕШЕНИЯ ДЛЯ БАЗОВЫХ РОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ ИЗДЕЛИЯ

ТаблицаБ.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					
Локальное администрирование Numa vServer	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
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 5.

Таблица 5 - 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 1.4.1.3.4
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
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

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 6.

Таблица 6 - 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 1.4.1.3.4
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
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

Меры защиты	Условное обозначение, согласно приказам ФСТЭК России № 31 [1], № 239 [2]	Пункт ТУ
ЗИС.39	ЗИС.39 [1, 2]	1.4.5.1 1.4.5.2 1.4.5.3 1.4.5.4 1.4.5.5 1.4.5.6 1.4.5.7

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 19.04.2022.

- УБИ.008 Угроза восстановления и/или повторного использования аутентификационной информации;
- УБИ.010 Угроза выхода процесса за пределы виртуальной машины;
- УБИ.031 Угроза использования механизмов авторизации для повышения привилегий;
- УБИ.044 Угроза нарушения изоляции пользовательских данных внутри виртуальной машины;
- УБИ.046 Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;
- УБИ.048 Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;
- УБИ.058 Угроза неконтролируемого роста числа виртуальных машин;
- УБИ.073 Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;
- УБИ.075 Угроза несанкционированного доступа к виртуальным каналам передачи;
- УБИ.076 Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;
- УБИ.077 Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;
- УБИ.078 Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;
- УБИ.079 Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;
- УБИ.080 Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;
- УБИ.084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;
- УБИ.085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;
- УБИ.086 Угроза несанкционированного изменения аутентификационной информации;
- УБИ.090 Угроза несанкционированного создания учётной записи пользователя;
- УБИ 100 Угроза обхода некорректно настроенных механизмов аутентификации;
- УБИ.108 Угроза ошибки обновления гипервизора;

- УБИ.119 Угроза перехвата управления гипервизором;
- УБИ.120 Угроза перехвата управления средой виртуализации.