Программно-аппаратный комплекс «Горизонт-ВС»

Руководство администратора

информационной безопасности

МБРЦ.468313.001.ИЗ.03

Листов: 45

Москва 2022

АННОТАЦИЯ

Настоящий документ, руководство по функциям информационной безопасности (ИБ) МБРЦ.468313.001 ИЗ.03 (далее по тексту – руководство по ИБ), содержит сведения о показателях защищенности согласно руководящему документу ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (далее по тексту – РД ФСТЭК России).

Рассмотрена модель защиты, идентификация и аутентификация, дискреционный принцип контроля доступа, очистка памяти, регистрация событий, контроль целостности ИБ программно-аппаратного комплекса (ПАК) «Горизонт-ВС» МБРЦ.468313.001 (далее по тексту – ПАК «Горизонт-ВС» или изделие).

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

ПАК «Горизонт-ВС» предназначен для организации взаимодействия пользователей *терминалов* с ресурсами *серверов виртуализации*, объединенных в IP-сеть с использованием технологии «клиент-сервер».

1.2 Краткое описание возможностей

Группа *серверов виртуализации* и *терминалов*, в которой работают пользователи, объединены в административную группу (далее по тексту – АГ). Администрирование в рамках АГ выполняют администраторы, используя автоматизированное рабочее место (АРМ) администратора безопасности – *АРМ Администратора*.

ПАК «Горизонт-ВС» является многокомпонентным распределённым комплексом с единой политикой безопасности, в состав которого входит модуль идентификации и контроля доверенной среды (МИиКДС) «Шина» МБРЦ.468264.001 (далее по тексту – МИиКДС «Шина») и комплекс программ (КП) «Терминал-Сервер» RU.МБРЦ.501130.01-01 (далее по тексту – КП «Терминал-Сервер»).

ПАК «Горизонт-ВС» должен соответствовать требованиям РД ФСТЭК России по 5 классу защищенности и реализовывать следующие показатели защищенности:

- дискреционный принцип контроля доступа;
- очистку памяти;
- идентификацию и аутентификацию;
- гарантии проектирования;
- регистрацию;
- целостность комплекса средств защиты (КСЗ);
- тестирование;
- руководство пользователя;
- руководство по КСЗ;
- тестовую документацию;

- конструкторскую и проектную документацию.

Согласно заданию по безопасности МБРЦ.468313.001 ЗБ ПАК «Горизонт-ВС» должен реализовывать следующие функции безопасности:

- идентификация и аутентификация;
- разграничение доступа к управлению изделием;
- управление работой изделия;
- управление параметрами изделия;
- аудит безопасности изделия;
- тестирование, контроль целостности программного обеспечения и параметров изделия;
- контроль компонентов СВТ;
- блокирование загрузки операционной системы СДЗ;
- сигнализация СДЗ;
- дискреционный контроль доступа;
- защита остаточной информации;
- управление компонентами виртуальной инфраструктуры.

Функциям безопасности соответствует состав функциональных требований безопасности, выраженных на основе компонентов требований, приведённых в методическом документе ФСТЭК России «Профиль защиты. Средства доверенной загрузки уровня платы расширения четвёртого класса защиты. ИТ.СДЗ.ПР4.ПЗ», а также дополнительно включенных и сформулированных в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Требования доверия к безопасности ПАК «Горизонт-ВС» соответствуют 4 уровню доверия и взяты из Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденных приказом ФСТЭК России от 30 июля 2018 года № 131.

При разработке средства были выполнены процедуры, предусматривающие:

- разработку модели безопасности средства;
- проектирование архитектуры безопасности средства;
- разработку функциональной спецификации средства;
- проектирование средства;
- разработку представления реализации средства;
- выбор средств, применяемых при разработке средства;
- управление конфигурацией средства;
- разработку документации по безопасной разработке средства;
- разработку руководства пользователя средства;
- разработку руководства администратора средства.

1.3 Уровень подготовки персонала

Администраторы ИБ должны иметь опыт работы с:

- персональным компьютером на уровне квалифицированного пользователя;
- стандартными приложениями на уровне свободного выполнения базовых операций;
- операционными системами:
  - Windows;
  - Unix-подобными ОС.

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Администратору ИБ необходимо ознакомиться со следующими документами:

- Руководство пользователя. МБРЦ.468313.001.ИЗ.01.
- Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина». МБРЦ.468313.001.ИЗ.02-01;

- Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-сервер». МБРЦ.468313.001.ИЗ.02-02;
- Руководство администратора информационной безопасности. МБРЦ.468313.001.ИЗ.03.

2 Назначение и условия применения

Изделие предназначено для использования в клиент-серверных системах.

КП «Терминал-Сервер» является гипервизором, устанавливаемым непосредственно на аппаратное обеспечение в качестве системного программного обеспечения, и предназначен для организации исполнения виртуальных машин (ВМ), а также подключения *терминалов* к ВМ, исполняемым на *сервере виртуализации*.

КП «Терминал-Сервер» состоит из трех основных компонентов:

- компонент «Тонкий клиент» (далее по тексту – КТ), который устанавливается на персональные электронные вычислительные машины (ПЭВМ), выполняющие функции *терминала* (компонент 1 согласно формуляру МБРЦ.468313.001.ФО);
- компонент «Сервер виртуальных машин» (далее по тексту – КС), который устанавливается на ПЭВМ, выполняющие функции *сервера виртуализации* (компонент 2 согласно формуляру МБРЦ.468313.001.ФО);
- компонент «Администратор безопасности» (далее по тексту – АБИ), который устанавливается на ПЭВМ, выполняющие функции автоматизированного рабочего места (*АРМ) администратора* (компонент 3 согласно формуляру МБРЦ.468313.001.ФО).

КТ имеет два варианта исполнения:

- исполнение 1 – системный тонкий клиент, поставляемый на USB-накопителе и предназначенный для запуска в качестве общесистемного ПО на терминалах, в том числе и бездисковых рабочих станциях;
- исполнение 2 – программный тонкий клиент, предназначенный для запуска в среде ОС семейства Linux.

3 Подготовка в работе

Установка и настройка системы описана в документах:

- Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина». МБРЦ.468313.001.ИЗ.02-01;
- Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-сервер». МБРЦ.468313.001.ИЗ.02-02.

4 Описание функций безопасности

4.1 Модель защиты

С целью реализации показателей защищенности разработана модель защиты, основанная на следующих принципах:

- защищается информация, хранимая и обрабатываемая в ПАК «Горизонт-ВС»;
- **объектами** доступа являются виртуальные машины (ВМ);
- **субъектами** доступа являются пользователи;
- изделие работает только с идентифицированными и аутентифицированными пользователями;
- механизм аутентификации построен на паре электронный ключ-пароль; доступ разрешается, если ЭК и пароль пользователя совпадают с зарегистрированными в изделии;
- доступ всех субъектов к объектам контролируется согласно **дискреционным принципам контроля доступа**. Дискреционный контроль доступа применяется к каждому субъекту и объекту и заключается в том, что на защищаемые объекты устанавливаются при их создании правила разграничения доступа (ПРД) в виде идентификаторов субъектов, которые вправе распоряжаться доступом к данному объекту и прав доступа к объекту. Права доступа субъектов к объектам представляются посредством матрицы доступа, пример которой приведен в таблице ниже (Таблица 1).

Таблица 1 – Пример матрицы доступа

Субъекты (пользователи)	**Объекты (виртуальные машины)**			
O_1	O2	…	On	
S_1	создание доступ модификация удаление	создание модификация		доступ модификация
S_2	доступ			
…				-
S_n				доступ

Элементами матрицы могут быть любые комбинации из четырех прав: создание, доступ, модификация, удаление. Размерность матрицы доступа зависит от количества субъектов и объектов в системе.

Решение о доступе принимается следующим образом: если субъект имеет по отношению к объекту право на доступ (создание, доступ, модификация или удаление), тогда соответствующий доступ разрешается, в противном случае запрос на доступ отклоняется.

Права доступа могут быть изменены только администратором средства доверенной загрузки (СДЗ).

Правила изменения ПРД:

Для формализации правил изменения ПРД введем ряд обозначений.

- Множество зарегистрированных в системе пользователей U, включающее администратора СДЗ {Uсдз}. Пользователи U представлены в системе посредством множества субъектов S;
- Множество объектов доступа O включает: ВМ администратора СДЗ Осдз, ВМ непривилегированных пользователей Оп. При этом Осдз $\cup$ Оп = О;
- Атрибут владения объектом доступа Ao=<Au0, Au1, Au2, …, AuM>, где Aui – атрибут принадлежности объекта пользователю Ui.

Определим ПРД.

- Субъекты множества Sсдз имеют неограниченный доступ к множеству объектов доступа Осдз для эффективного управления ПРД.
- Субъекты множества Sп не имеют доступа к объектам множества Осдз.
- Субъекты, принадлежащие множеству Sсдз, имеют доступ к объектам из множества Оп.

Правила изменения ПРД.

- Asi назначается для пользователя Ui пользователем Uсдз.
- Модификации {Ao} могут выполняться пользователем {Uсдз} произвольно.

Такие правила изменения ПРД определяют, что перечень неиерархических категорий объекта доступа не может быть произвольно или непроизвольно расширен. То есть, если начальное состояние системы

безопасно, то и все состояния, достижимые из него путем применения конечной последовательности изменений ПРД, безопасны. Таким образом, система, реализующая представленную модель доступа, безопасна.

- согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО) на одном *терминале* может быть зарегистрирован только один пользователь. В свою очередь каждый *терминал* конфигурируется на доступ только к одной виртуальной машине. Таким образом, пользователь может получить доступ только к одной виртуальной машине;
- для контроля действий пользователей и администраторов используется **система аудита** с функцией протоколирования фактов несанкционированного доступа / нарушений модели безопасности в реальном времени. В изделии регистрируются:
  - запуск и завершение функций аудита;
  - использование идентификационного и аутентификационного механизма;
  - запрос на доступ к защищаемому ресурсу (ВМ);
  - создание и уничтожение объекта;
  - действия по изменению ПРД.

контроль целостности выполняется платой МИиКДС «Шина». Контролируются файлы и загрузочные сектора загружаемых USB-носителей. Контрольные суммы на содержимое файла рассчитываются в соответствии с алгоритмом CRC32. На *сервере виртуализации,* системные файлы которого копируются на жесткий диск, после успешного выполнения контроля целостности USB-носителей платой МИиКДС «Шина» производится контроль целостности неизменяемой части корневой файловой системы на жестком диске. Для каждого файла, находящегося в директории ***/usr***, вычисляется MD5-hash функция, которая сравнивается с аналогичной суммой, вычисленной для данного файла на этапе сборки.

Также в ПАК «Горизонт-ВС» реализована **изолированная программная среда**. Процесс закрытия программной среды основан на следующих

положениях. При установке системы запускается скрипт *initialize*, которым автоматически генерируется пара закрытый и открытый ключ. В процессе инициализации, для всех без исключения инсталлируемых на жёсткий диск файлов ПАК «Горизонт-ВС» системой автоматически подсчитывается хеш-сумма по алгоритму sha-1, которая подписывается сгенерированным закрытым ключом. После этого подписанная хеш-сумма сохраняется в расширенных атрибутах файловой системы, для каждого файла в отдельности.

После завершения процесса инсталляции закрытый ключ и инсталляционный скрипта *initialize* автоматически уничтожаются. В системе остаётся только открытый ключ, в случае удаления или подмены которого, загрузка и функционирование системы будет невозможна.

При попытке доступа к файлу проверяется его целостность, т.е. подсчитывается хеш-сумма файла и сравнивается с сохранённой в процессе инсталляции в расширенных атрибутах файловой системы. Если хеш-суммы не совпадают, запуск файла блокируется ядром системы на начальном этапе загрузки. Также заблокирован запуск для всех файлов, которые не имеют подписанной контрольной суммы в расширенных атрибутах.

Вследствие того, что закрытый ключ, которым были подписаны файлы при инсталляции, при её завершении уничтожается, подписать контрольную сумму какого-либо файла после процедуры инсталляции, в ходе эксплуатации изделия, не возможно. В связи с этим, после инсталляции изделия, в среде ПАК «Горизонт-ВС», невозможно выполнить какой-либо файл, не инсталлированный в ходе процедуры начальной установки, либо изменённый в процессе эксплуатации.

- **очистка памяти** осуществляется при создании образа диска ВМ посредством перезаписи каждого байта нулями.

4.2 Идентификация и аутентификация

Функция безопасности идентификации и аутентификации пользователей в ПАК «Горизонт-ВС» основывается на паре электронный ключ-пароль.

В изделии поддерживаются два типа пользователей, основанных на ролях безопасности: администраторы СДЗ и пользователи.

При регистрации в изделии каждому пользователю присваивается электронный ключ идентификации (далее по тексту – ЭК), пароль и системное имя. Системное имя связывается в КП «Терминал-Сервер» с идентификатором пользователя — UID (User ID) и должно совпадать с заданным в МИиКДС «Шина».

Функция безопасности идентификация и аутентификация пользователей решается следующим методом. Для получения доступа к *терминалам*, *серверам виртуализации* и *АРМ администратора* пользователями предъявляется ЭК и вводится пароль. Процедура идентификации и аутентификации обеспечивается программой «Прошивка FPGA» из состава КП «Прошивка МИиКДС» RU.МБРЦ.501410.02-01. Доступ разрешается, если ЭК и пароль пользователя совпадают с зарегистрированными в изделии.

Далее осуществляется подключение *терминала* к виртуальной машине, исполняемой на *сервере виртуализации*.

Терминал выдает требование плате МИиКДС «Шина» сгенерировать сессионную маскирующую последовательность (сессионный ключ) и по внутреннему каналу передать ее на плату МИиКДС «Шина» *сервера виртуализации*. Модуль *сервера виртуализации vmacd* получает событие о получении сессионного ключа и выдает плате МИиКДС «Шина» команду готовности к принятию и размаскированию полученных данных. Плата МИиКДС «Шина» *сервера виртуализации*, получив маскированное сообщение от *терминала*, размаскирует его и производит инициализацию сессии клиент-сервер.

Если процедура размаскирования прошла успешно, *терминал* считается доверенным, и подключение к виртуальной машине разрешается. Запуск ВМ осуществляется с UID пользователя, аутентифицированного на *терминале*, в соответствии с назначенными ПРД.

Если процедура размаскирования прошла неуспешно, то в соединении отказывается.

В КП «Терминал-Сервер» функция идентификации и аутентификации пользователей решается следующим методом. На *сервере виртуализации* пользователи создаются при помощи утилиты *VSUSERS*. База пользователей

и паролей записывается в файл, находящийся в директории ***/etc/shadow***. Кроме этого, создается теневая база пользователей и паролей, доступ к которой имеет утилита *VMACD*.

При запуске *терминала* стартует утилита *START-SPICE*, которая выводит окно для ввода имени пользователя и пароля. После заполнения пользователем своих идентификационных данных утилита *START-SPICE* подключается к утилите *VMACD* на *сервере виртуализации* и передает ей имя и пароль пользователя, после чего проходит аутентификацию на утилите *VMACD* с использованием SASL, механизма digest-md5. Введённые имя пользователя и пароль кэшируются в оперативной памяти *терминала*. В случае получения правильного имени пользователя и пароля утилита *VMACD* направляет на *терминал*, в утилиту *START-SPICE*, список доступных для данного пользователя ВМ. Пользователь выбирает нужную ВМ из списка, после чего происходит запуск этой ВМ через утилиту *LIBVIRTD* от имени пользователя, аутентифицированного на *терминале* и подключение *терминала* к этой ВМ. Кэшированная пара логин/пароль уничтожается после подключения.

Если утилитой *VMACD* на *сервере виртуализации* были получены неверные имя и пароль пользователя, то соединение разрывается, и запись об этом помещается в журнал регистрации событий.

В системе полностью исключена возможность работы не прошедшего процедуру аутентификации пользователя, так как «гостевых» или иных учетных записей, позволяющих осуществить вход в систему даже с ограниченными правами, не предусмотрено.

Процедура входа в систему для пользователя выглядит как приглашение по предъявлению электронного ключа и вводу пароля, а на системном уровне представляет собой интерактивную сессию, все процессы в которой исполняются от имени выполнившего вход пользователя. Для каждого процесса хранятся все данные, связанные с аутентификацией: номер ЭК, имя пользователя и UID, – что позволяет изделию заносить информацию об идентификации и аутентификации, а также дальнейших действиях пользователя в журнал регистрации событий.

Для аутентификации пользователей используются пароли, которые могут быть заданы администратором СДЗ вручную либо сгенерированы при помощи физического датчика случайных чисел. Пароли отвечают следующей метрике качества:

1) длина пароля – 8 символов;
2) в пароле должны присутствовать символы из следующих категорий:
   - прописные буквы английского алфавита от A до Z;
   - строчные буквы английского алфавита от a до z;
   - десятичные цифры от 0 до 9;
   - специальные символы, не принадлежащие алфавитно-цифровому набору;
3) в пароле должны отсутствовать повторяющиеся символы;
4) пароль не должен иметь смысловой нагрузки.

Если число неуспешных попыток аутентификации достигает 3, то происходит блокировка загрузки изделия. Если число неудачных попыток входа достигает 8 подряд или 10 в общем, то пользователь блокируется (кроме учетной записи администратора СДЗ). Кроме того, в изделии есть возможность принудительной блокировки *терминалов* и *серверов виртуализации* для входа всех пользователей, кроме администратора СДЗ, путем блокировки пользователя с *АРМ администратора*. Информация о данных действиях заносится в журнал регистрации событий платы МИиКДС «Шина».

4.3 Дискреционный принцип контроля доступа

В ПАК «Горизонт-ВС» реализована функция безопасности дискреционного контроля доступа субъектов (пользователей) к объектам (виртуальным машинам). Реализация механизма дискреционных ПРД обеспечивает наличие для каждой пары субъект-объект явное и недвусмысленное перечисление допустимых типов доступа.

С каждым пользователем системы связан уникальный идентификатор – идентификатор пользователя (UID), который используется для определения прав доступа. Каждая ВМ в системе запускается с UID запустившего ВМ пользователя. При обращении пользователя к объекту доступ предоставляется

по результатам процедуры авторизации, то есть обработки запроса на основе дискреционных правил разграничения доступа.

Согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО, п. 6.4) на одном *терминале* может быть зарегистрирован только один пользователь. В свою очередь каждый *терминал* конфигурируется на доступ только к одной ВМ. Таким образом, пользователь может получить доступ только к одной ВМ.

Дискреционный контроль доступа применяется к каждому объекту и каждому субъекту и заключается в том, что на защищаемые объекты устанавливаются при их создании базовые ПРД в виде идентификаторов субъектов (UID), которые вправе распоряжаться доступом к данному объекту и прав доступа к объекту. Состояние прав доступа при дискреционном контроле описывается матрицей, в строках которой перечислены субъекты, в столбцах – объекты, а в ячейках – операции, которые субъект может выполнить над объектом (Создание, Доступ, Модификация, Удаление). Матрица доступа для ПАК «Горизонт-ВС» приведена в таблице ниже (Таблица 2).

Таблица 2 – Матрица доступа

Объект / **Субъект**	**Виртуальная машина 1**	**Виртуальная машина 2**	**…**	**Виртуальная машина N**
Администратор СДЗ	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление
Пользователь 1	Доступ	—	—	—
Пользователь 2	—	Доступ	—	—
…	…	…	…	…
Пользователь N	—	—	—	Доступ

При обращении субъекта к объекту система проверяет совпадение идентификаторов субъекта (UID), запрашивающего доступ и назначенного в соответствии с ПРД. По результатам проверки доступ либо разрешается, либо запрещается. При запросе администратора СДЗ на доступ к объекту этот вид доступа предоставляется ему вне зависимости от правил. Доступ к объекту

явно запрещается субъектам с несоответствующими ЭК, так как в этом случае они не могут пройти процедуру аутентификации.

Механизм, реализующий дискреционное разграничение доступа, обеспечивает возможность санкционированного изменения списка пользователей и списка защищаемых объектов. Право изменения ПРД предоставлено администратору СДЗ.

Процедура изменения списка пользователей и назначения правил доступа к объектам описана в руководстве администратора МБРЦ.468313.001 Д2.1 (п.п. 2.5, 2.11).

Права на доступ к объектам никаким образом не распространяются, кроме случая явного их присвоения администратором СДЗ.

Таким образом, реализованный в ПАК «Горизонт-ВС» механизм, регулирующий дискреционный принцип контроля доступа, предусматривает санкционированное изменение дискреционных ПРД, включая санкционированное изменение списка субъектов и списка защищаемых объектов.

Подсистемой регистрации событий КП «Терминал-Сервер» протоколируются следующие события, связанные с дискреционным контролем доступа:

- запрос на доступ к защищаемому ресурсу (виртуальной машине);
- создание и уничтожение объекта (ВМ);
- действия по изменению ПРД.

4.4 Очистка памяти

Требование показателя защищенности «Очистка памяти» при первоначальном назначении или при перераспределении внешней памяти предотвращать доступ субъекту к остаточной информации решается следующим методом.

При создании образа диска на *сервере виртуализации* согласно условиям по безопасности создается дисковое пространство, заполненное нулями.

Очистка осуществляется посредством перезаписи каждого байта создаваемого образа диска ВМ нулями.

Очистка памяти используется при создании и удалении виртуальных машин (при создании образа диска для ВМ), таким образом предотвращается доступ субъектов к остаточной информации.

4.5 Регистрация событий

Функция безопасности «Аудит безопасности изделия» реализуется платой МИиКДС «Шина» и КП «Терминал-Сервер». Список событий, регистрируемых функцией аудита, приведен в приложении А.

В плате МИиКДС «Шина» реализован журнал регистрации событий (ЖРС), организованный как кольцевой буфер записей фиксированной длины (размер журнала - 1024 записи). По каждому событию в ЖРС формируется строка, состоящая из следующих полей:

- Имя пользователя – имя зарегистрированного пользователя, выполнившего действие;

***Примечание**. Если к моменту наступления события имя пользователя не определено, то в данное поле выводится константа «Неопределен».*

- Событие – условное название события;
- ID сессии – идентификатор сессии;
- Дата и время – ДД/ММ/ГГ ЧЧ:ММ:СС,

  где
  - ДД/ММ/ГГ – дата/месяц/ год;
  - ЧЧ:ММ:СС –час:минута:секунда;
- Серийный № ЭК – заводской номер ЭК, который участвовал в событии.

Записи приводятся в порядке возрастания времени регистрации события.

На *сервере виртуализации* с установленным КП «Терминал-Сервер» реализована подсистема регистрации событий, с помощью которой можно получить подробную информацию обо всех системных событиях. Все события в системе не могут произойти без системных вызовов ядра. Подсистема аудита (демон *auditd*) перехватывает системные вызовы и таким образом отслеживает все работу КП «Терминал-Сервер».

Настройки подсистемы регистрации событий хранятся в конфигурационном файле ***etc/one/oned.conf***. При первоначальной настройке, задаются следующие параметры:

- *file* — файл, в котором будут храниться логи подсистемы аудита (***var/log/one/oned.log***);
- *MONITORING_INTERVAL* — время между опросами серверов виртуализации и состояний виртуальных машин (***60***, сек).

По умолчанию для журнала установлен размер 6Мб, по достижении которого осуществляется его перезапись.

Регистрация событий создания, запуска, остановки и удаления виртуальных машин осуществляется в файл ***var/log/one/oned.log***.

Требования РД ФСТЭК России для 5 класса защищенности в части регистрации событий и способ их реализации в ПАК «Горизонт-ВС» приводятся в таблице ниже (Таблица 3).

Таблица 3 – Регистрация событий

Требования РД ФСТЭК России	**Способ реализации ПАК «Горизонт-ВС» требований РД ФСТЭК России в части регистрации событий**
ПАК «Горизонт-ВС» должен быть в состоянии осуществлять регистрацию следующих событий: – использование идентификационного и аутентификационного механизма;	Регистрация событий использования идентификационного и аутентификационного механизма осуществляется платой МИиКДС «Шина» и КП «Терминал-Сервер» в файле **var/log/one/oned.log**. В журнале регистрации событий фиксируются: – успешная аутентификация пользователя/администратора – -ошибка при выполнении аутентификации пользователя (неверный ЭК или пароль).
запрос на доступ к защищаемому ресурсу (ВМ);	Регистрация запросов на доступ к защищаемому ресурсу осуществляется КП «Терминал-Сервер». События сохраняются в файл **var/log/one/oned.log**.
создание и уничтожение объекта;	Регистрация создания и уничтожения объектов осуществляется КП «Терминал-Сервер». События сохраняются в файл **var/log/one/oned.log**.
действия по изменению ПРД.	Регистрация действий по изменению ПРД осуществляется КП «Терминал-Сервер».

	События сохраняются в файл **var/log/one/oned.log**.
Для каждого из этих событий должна регистрироваться следующая информация: – дата и время; – субъект, осуществляющий регистрируемое действие; – тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа); успешно ли осуществилось событие (обслужен запрос на доступ или нет)	Для каждого события в журнале регистрации событий платы МИиКДС «Шина» и подсистемы регистрации событий КП «Терминал-Сервер» регистрируется дата, время, пользователь, осуществляющий действия, тип события и результат (успешное выполнение или ошибка).

4.6 Контроль целостности

Для обеспечения контроля целостности в ПАК «Горизонт-ВС» реализованы средства:

- подсчета контрольных сумм файлов на USB-носителе;
- контроля загрузочных секторов USB-носителя;
- контроля целостности неизменяемой части корневой файловой системы;
- создания замкнутой (изолированной) программной среды.

4.6.1 Средство подсчета контрольных сумм файлов на USB-носителе и контроля загрузочных секторов USB-носителя

Подсчет контрольных сумм файлов загружаемых USB-носителей, а также загрузочных секторов USB-носителей осуществляется платой МИиКДС «Шина». Список контролируемых файлов прошивается в энергонезависимой памяти (ЭНП) память платы МИиКДС «Шина» на этапе изготовления.

Контроль целостности осуществляется в файловом режиме, при котором контролируются пять системных файлов:

- KERNEL – ядро КП «Терминал-Сервер»;
- LDLINUX.C32 – расширение пакета syslinux;
- LDLINUX.SYS – файл загрузчика syslinux КП «Терминал-Сервер»;

- SYSLINUX.CFG – файл конфигурации загрузчика syslinux КП «Терминал-Сервер»;
- ROOTFS – неизменяемый образ файловой системы КП «Терминал-Сервер», содержащий эталонные копии исполняемых файлов, инсталлируемых на жёсткий диск *сервера виртуализации*.

Поскольку в файлах KERNEL, LDLINUX.C32, LDLINUX.SYS, SYSLINUX.CFG, ROOTFS содержится ядро и корневая файловая система в виде сжатого образа SQUASHFS, совпадение контрольных сумм данных файлов с эталонными обеспечивает гарантированный контроль целостности образа ядра и файловой системы. Процедура контроля целостности запускается автоматически при каждом входе в систему перед загрузкой КП «Терминал-Сервер».

При инсталляции изделия администратор СДЗ должен запустить на выполнение процедуру «Установка векторов», которая последовательно выбирает из списка контролируемые файлы, находит их и вычисляет для каждого объекта значение контрольного вектора его содержимого. Полученные контрольные вектора запоминаются в ЭНП изделия. В конце процедуры «Установка векторов» формируется контрольный вектор списка контролируемых файлов**,** который также записывается в ЭНП изделия.

При выполнении процедуры контроля целостности плата МИиКДС «Шина» загружает список контролируемых файлов, проверяет его целостность, а затем последовательно вычисляет для каждого объекта значение контрольного вектора и сравнивает полученное значения со значением, которое хранится в ЭНП изделия. Целостность программной среды считается не нарушенной, если все значения вычисленных контрольных векторов совпадают с эталонными, хранящимися в ЭНП изделия. Для вычисления контрольного вектора файла (объекта) используется операция выработки контрольной суммы на содержимое файла (объекта) в соответствии с алгоритмом CRC32.

Подсистема контроля целостности работает в жестком режиме, т.е. при нарушении целостности информации на носителе пользователя запрещается загрузка КП «Терминал-Сервер». Сообщения о нарушении целостности носителя заносятся в журнал регистрации событий.

4.6.2 Средства контроля целостности неизменяемой части корневой файловой системы

На *сервере виртуализации* системные файлы копируются на жесткий диск, поэтому после успешного выполнения контроля целостности USB-носителей платой МИиКДС «Шина» производится контроль целостности неизменяемой части корневой файловой системы, установленной на жесткий диск *сервера виртуализации*. Для каждого файла, находящегося в директории ***/usr***, вычисляется MD5-hash функция, которая сравнивается с аналогичной суммой, вычисленной для данного файла на этапе сборки. В случае полного соответствия вычисленных контрольных сумм эталонным система продолжает загрузку. В противном случае загрузочный скрипт полностью очищает директорию ***/usr*** и осуществляет безусловное копирование неизменяемой корневой части файловой системы с USB-носителя.

Периодический контроль целостности обеспечивается периодической перезагрузкой *сервера виртуализации*, *АРМ администратора* и *терминалов*.

4.6.3 Средства создания замкнутой (изолированной) программной среды

В ПАК «Горизонт-ВС» реализован механизм изоляции программной среды. Данный механизм запускается после завершения установки изделия на жесткий диск сервера виртуализации. Дальнейшие настройки, кроме тех, которые возможно выполнить из графического интерфейса согласно руководству администратора МБРЦ.468313.001 Д2.1 будет выполнить невозможно, так как будет отключена командная строка.

Список требований для обеспечения изолированной программной среды, методы их проверки и ожидаемые результаты проверок приведены в таблице ниже (Таблица 4).

Таблица 4 – Требования для обеспечения изолированной программной среды

Требования для обеспечения изолированной программной среды	**Проверка выполнения требований**	**Ожидаемые результаты**
Монтирование файловой системы выполнено с опцией *iversion*.	Ввод команды в консоли: *mount | grep ' / '*	Наличие опции *i_version* у примонтированной файловой системы.
В ядре системы реализованы механизмы IMA (Integrity Measurement Architecture) для слежения за целостностью системы.	Ввод команды в консоли: *ls /sys/kernel/security*	Наличие каталога */sys/kernel/security/ima*.
При запуске в ядро загружается политика подсистемы IMA на запрет исполнения *appraise*.	Ввод команды в консоли: *ls /sys/kernel/security/ima/*	Отсутствие файла *policy*, так как политики загружены.
Закрытый ключ, которым на начальном этапе инсталляции производится подпись хеш-сумм файлов, по окончании процедуры автоматически уничтожается.	Проверить невозможно, т.к. ключ создается при запуске скрипта *initialize* и удаляется после завершения его выполнения.	-
Цепочка ключей _ima содержит открытый ключ, которым проверяется подпись хеш-сумм.	Ввод команды в консоли: *keyctl show*	Вывод списка цепочек ключей.

Механизм создания изолированной программной среды основан на следующих положениях.

На ПЭВМ с проверенной BIOS устанавливается ПАК «Горизонт-ВС». Проверка BIOS осуществляется согласно методике оценки отсутствия угроз обеспечения безопасного функционирования ПАК «Горизонт-ВС» в среде функционирования системы базового ввода-вывода (BIOS) вычислителя, приведенной в функциональном тестировании МБРЦ.468313.001 Д11 (п. 6).

Инсталляция и дальнейшая загрузка ПАК «Горизонт-ВС» производится с USB-накопителя, целостность содержимого которого контролируется при загрузке аппаратными средствами – МИиКДС «Шина». При инсталляции системы запускается скрипт *initialize*, которым автоматически генерируется

пара закрытый и открытый ключ и инициализируется механизм защиты. В процессе инициализации, для всех без исключения инсталлируемых на жёсткий диск файлов ПАК «Горизонт-ВС» системой автоматически подсчитывается с использованием алгоритма sha-1 контрольная хеш-сумма, которая подписывается сгенерированным закрытым ключом. После этого подписанная хеш-сумма сохраняется в расширенных атрибутах файловой системы, для каждого файла в отдельности. Поскольку хеш-сумма с электронной подписью сохраняются в атрибутах каждого файла, при копировании и переносе файлов в другие директории подписанная хеш-сумма копируется совместно с файлами, таким образом, изменение пути файла на возможность проверки перемещённых или скопированных файлов не влияет.

Сразу же по завершении процесса инсталляции закрытый ключ и инсталляционный скрипт *initialize* автоматически уничтожаются. В системе остаётся только открытый ключ, который сохраняется на жёстком диске в директории ***/*etc**. В случае удаления или подмены этого ключа, загрузка и функционирование системы будет невозможна. Схема реализации механизма создания изолированной программной среды приведена на рисунке ниже (Рисунок 1).

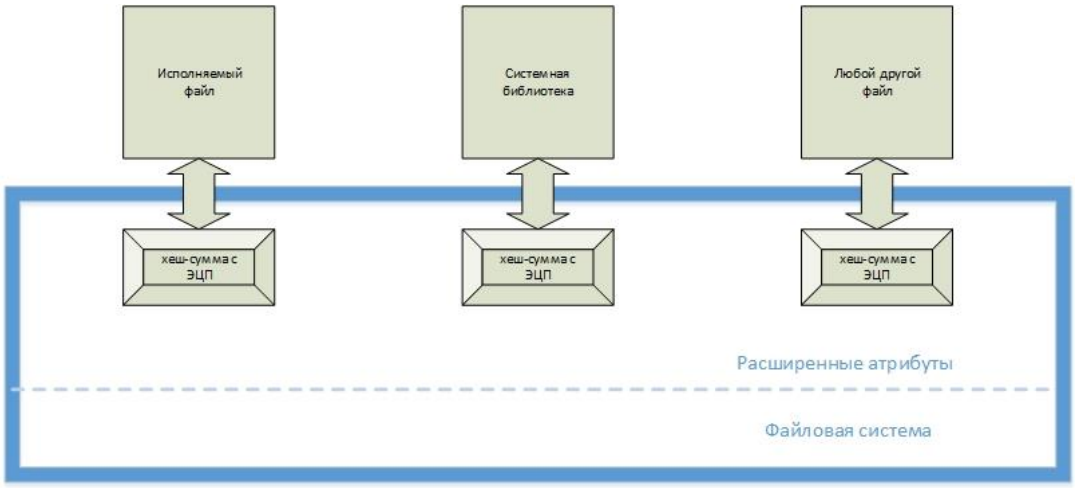

Рисунок 1 – Изолированная программная среда

В ходе функционирования системы осуществляется проверка исполнения файла, согласно алгоритму, приведенному на рисунке ниже (Рисунок 2).

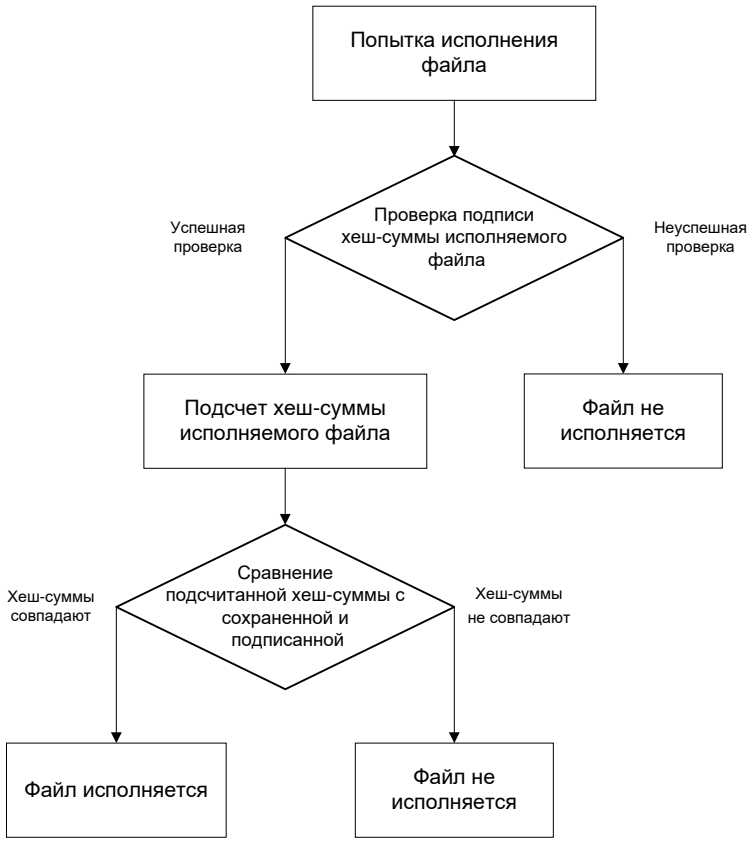

Рисунок 2 – Алгоритм проверки файлов

Перед загрузкой любого файла в оперативную память для исполнения, ядром системы проверяется целостность этого файла, т.е. подсчитывается хеш-сумма файла и сравнивается с сохранённой в процессе инсталляции в расширенных атрибутах файловой системы. Перед процедурой сравнения проверяется электронная подпись сохранённой суммы при помощи открытого ключа, действующего в системе.

Таким образом контролируются все файлы, имеющие, либо приобретающие атрибуты исполнения, – скрипты и бинарные elf-файлы, а также системные библиотеки.

Если рассчитанная хеш-сумма запускаемого файла не совпадает с подписанной хеш-суммой, сохранённой в расширенных атрибутах этого файла, запуск файла блокируется ядром системы на начальном этапе загрузки. Также заблокирован запуск для всех файлов, которые не имеют подписанной контрольной суммы в расширенных атрибутах. Вследствие того, что закрытый ключ, которым были подписаны файлы при инсталляции, при её завершении уничтожается, подписать контрольную сумму какого-либо файла после

процедуры инсталляции, в ходе эксплуатации изделия, не представляется возможным. В связи с этим, после инсталляции изделия, в среде ПАК «Горизонт-ВС», невозможно выполнить какой-либо файл, не инсталлированный в ходе процедуры начальной установки, либо изменённый в процессе эксплуатации.

Таким образом, в функционирующей изолированной среде ПАК «Горизонт-ВС» возможен запуск только тех файлов, скриптов и библиотек, которые были установлены в процессе начальной инсталляции и целостность которых подтверждается всякий раз при их запуске.

4.7 Разграничение доступа к управлению изделием

ПАК «Горизонт-ВС» поддерживает роли администратора СДЗ и пользователя и ассоциирует пользователей с ролями.

Данная функция безопасности реализуется средствами МИиКДС «Шина». В административной группе может быть зарегистрировано не более трех администраторов и не более 125-ти пользователей. Создание и регистрация первого администратора СДЗ (**ADMIN_1**) выполняется при инсталляции платы изделия на *АРМ Администратора*.

Создание и регистрация нового администратора СДЗ или пользователя осуществляется на *АРМ Администратора* и доступно только администратору СДЗ.

Администратор СДЗ реализует функции управления административной группой, регистрацией пользователей, управления сетевыми настройками, реакцией на события информационной безопасности и др. Пользователю доступна только функция прохождения процедуры идентификации и аутентификации, доступа к настройкам пользователь не имеет, поскольку ему не доступно *АРМ Администратора*.

4.8 Управление работой изделия

ПАК «Горизонт-ВС» способен к выполнению следующих функций управления работой изделия:

- управление режимом выполнения функций безопасности,
- управление данными функций безопасности.

ПАК «Горизонт-ВС» может функционировать в режиме АРМ администратора, терминала и сервера виртуализации. Общая схема функционирования представлена на рисунке ниже (3).

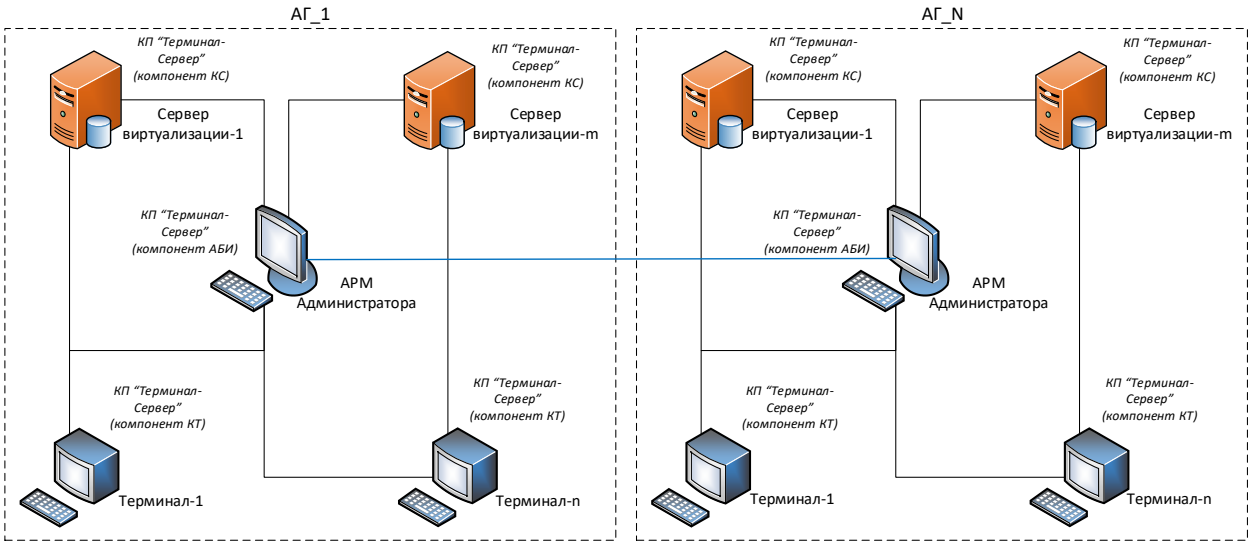

Рисунок 3 – Схема функционирования

На АРМ администратора имеют право работать только администраторы СДЗ, пользователям доступ на АРМ администратора запрещён, т.к. с данного АРМ реализуется управление всеми функциями безопасности административной группы. Сервер виртуализации позволяет принимать входящие соединения для подключения к виртуальным машинам. Терминал позволяет осуществлять работу пользователей с виртуальными машинами, исполняющимися на сервере виртуализации

ПАК «Горизонт-ВС» ограничивает возможность удаления, модификации, добавления следующих пользователей только администратору СДЗ, так как эти функции осуществляются только с *АРМ администратора*.

4.9 Управление параметрами изделия

ПАК «Горизонт-ВС» ограничивает возможность определения режима назначения ролей безопасности, предоставляя данное право только администратору СДЗ. Управление ограничениями данных функций безопасности доступно только на АРМ администратора, так как программа «Администратор МИиКДС» функционирует только на данном АРМ.

В административной группе может быть зарегистрировано не более трех администраторов и не более 125-ти пользователей.

При достижении или превышении установленных выше ограничений выдается сообщения об ошибке. Данные записи администратор СДЗ получает при прочтении журнала модуля «Шина». Администратор СДЗ может читать не только записи журнала своего АРМ, но и запрашивать журналы безопасности терминалов и серверов виртуализации, входящих в административную группу.

4.10 Контроль компонентов СВТ

ПАК «Горизонт-ВС» способен защищать хранимые записи аудита от несанкционированного удаления.

ПАК «Горизонт-ВС» способен к предотвращению модификации хранимых записей аудита в журнале аудита. Доступ к журналу безопасности доступен только администратору СДЗ на АРМ администратора.

ПАК «Горизонт-ВС» выполняет перезапись самой старой записи журнала аудита, если журнал аудита превышает размер в 1024 записи для платы и размер записи для сервера виртуализации 6 Мб.

Более подробное описание работы подсистемы аудита приведено в разделе 4.5.

4.11 Блокирование загрузки операционной системы СДЗ

ПАК «Горизонт-ВС» обеспечивает блокирование загрузки операционной системы при следующих случаях:

- выявлении попыток загрузки нештатной операционной системы.
- превышении числа неудачных попыток аутентификации пользователя.
- нарушении целостности средства доверенной загрузки.
- нарушении целостности загружаемой программной среды.
- при критичных типах сбоев и ошибок.

Под операционной системой в данном случае понимается программное обеспечение комплекса программ «Терминал-Сервер» RU.МБРЦ.501130.01-01.

Механизм блокировки загрузки альтернативной ОС

Так как штатная загрузка выполняется с носителя, который определяется в BIOS системы как диск с номером **0x80**, для предотвращения возможности загрузки с других дисков в изделии реализована принудительная загрузка ОС с диска **0x80** (по адресу **0000:0C00** считывается MBR диска **0x80** и командой ***jmp far*** передается управление первичному загрузчику ОС).

Проверка «легитимности» тома, подключенного в качестве диска **0x80**, выполняется средствами подсистемы контроля целостности МИиКДС «Шина».

Механизм блокировки загрузки ОС при превышении числа неудачных попыток входа

В каждом изделии для каждого пользователя во флэш-памяти хранится структура ***USER_INFO*** (файл ***...\data_struct.h***). В структуре ***USER_INFO*** в поле ***failed_entries*** хранится общее число неудачных попыток входа для данного пользователя. Как только значение ***failed_entries*** превысит значение «Максимальное количество неудачных попыток входа» (MAX_FAILED_ENTRIES=10), пользователь блокируется.

Снять блокировку пользователя может любой из администраторов. При этом значение поля ***failed_entries*** обнуляется.

Механизм блокировки загрузки ОС при нарушении целостности встроенного ПО

Проверку целостности встроенного ПО выполняет процедура ***check_IV_code()***. Если вычисленная контрольная сумма не совпадает с эталоном, который хранится в секторе ***TECH_SECT***, работа изделия блокируется (процедура ***PC_STOP()*** (файл ***…\main.c***))***.***

Механизм блокировки загрузки ОС при появлении критичных сбоев и ошибок

Блокировку изделия выполняет процедура ***PC_STOP(),*** которая передает сигнал аппаратного останова работы ПЭВМ **avr_lock_device()** и переходит к бесконечному циклу «while(1)».

В таблице ниже (Таблица 5) дан перечень ситуаций, когда работа изделия блокируется процедурой ***PC_STOP()*** при выявлении критических ошибок.

Таблица 5 – Перечень ситуаций при выявлении критических ошибок

Номер	Файл	Процедура	Описание ситуации
1	***...\main.c***	***check_IV_code()***	Нарушение целостности кода встроенного ПО
2	***...\main.c***	***Init_Start()***	Сбой при инициализации периферии процессора Microblaze
3	***…\main.c***	***avr_test_presence()***	Сбой при инициализации системы аппаратного контроля
4	***...\main.c***	***SPI_WRITE_SECTOR_WITH_IV***	Сбой при записи сектора ***TECH_SECT***
5	***...\main.c***	***Main()***	Сбой при определении режима работы платы MODE_CARD > 3
6	***...\main.c***	***LOAD_FROM_SPI_S0()***	Сбой при чтении сектора S0
7	***...\main.c***	***SAVE_TO_SPI_S0***	Сбой при записи сектора S0
8	***...\main.c***	***HOST_ADMIN()***	Сбой протокола обмена при выполнении процедуры ***HOST_ADMIN***
9	***...\bios.c***	***Test_HRAND()***	Сбой при тестировании ФДСЧ

ОО обеспечивает перезагрузку средства вычислительной техники, блокировку учётной записи пользователя, блокировку загрузки операционной системы средства вычислительной техники, регистрацию события в журнале аудита при выявлении попыток обхода средства доверенной загрузки.

4.12 Сигнализация СДЗ

ПАК «Горизонт-ВС» информирует администратора СДЗ при обнаружении возможного нарушения безопасности с использованием сообщений об ошибках, которые отображаются на дисплее СВТ. Для некоторых типов нарушений безопасности предусмотрена блокировка работы серверов виртуализации, АРМ администратора и терминалов (см. раздел 12).

4.13 Управление компонентами виртуальной инфраструктуры

ПАК «Горизонт-ВС» обеспечивает управление перемещением виртуальных машин (миграцию и копирование виртуальных машин между серверами виртуализации), включающее в себя:

- управление размещением и перемещением файлов-образов виртуальных машин между носителями (системами хранения данных);
- управление размещением и перемещением исполняемых виртуальных машин между серверами виртуализации;
- управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных);
- очистку освобождаемых областей памяти на серверах виртуализации, носителях, при перемещении виртуальных машин и обрабатываемых на них данных.

Управление перемещением виртуальных машин предусматривает полный запрет перемещения виртуальных машин и ограничение перемещения виртуальных машин в пределах информационной системы.

Управление перемещением виртуальных машин реализуется модулем Open Nebula, описание работы которого приведено в документе Описание программы RU.МБРЦ.501130.01-01 13 01 (раздел 3.2.2.2).

ПАК «Горизонт-ВС» обеспечивает резервное копирование данных виртуальной инфраструктуры, включая:

- определение мест хранения резервных копий виртуальных машин и данных, обрабатываемых в виртуальной инфраструктуре;
- резервное копирование виртуальных машин;
- резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;
- резервирование программного обеспечения серверов виртуализации, автоматизированного рабочего места администратора;

- периодическую проверку резервных копий и возможности восстановления виртуальных машин и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий;
- резервное копирование конфигурации виртуальной инфраструктуры;
- резервирование дистрибутивов средств построения виртуальной инфраструктуры (в том числе средств управления виртуальной инфраструктурой).

Резервное копирование виртуальных машин и конфигураций виртуальной инфраструктуры реализуется модулем ***backup***, описание работы которого приведено в документе Описание программы RU.МБРЦ.501130.01-01 13 01 (раздел 3.2.1.5).

При контроле доступа к компонентам виртуальной инфраструктуры ПАК «Горизонт-ВС» обеспечивает только для администратора СДЗ:

- доступ к средствам управления компонентами виртуальной инфраструктуры;
- доступ к файлам-образам виртуальных машин, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;
- доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин;
- доступ к виртуальному аппаратному обеспечению информационной системы;
- контроль запуска виртуальных машин на основе заданных режимов запуска;
- определение состава устройств виртуальных машин, объёма используемой оперативной памяти, подключаемых виртуальных и физических носителей информации.

Контроль доступа к компонентам виртуальной инфраструктуры реализуется модулем Open Nebula, описание работы которого приведено в документе Описание программы RU.МБРЦ.501130.01-01 13 01 (раздел 3.2.2.2).

4.14 Список сообщений журнала регистрации событий

Таблица 6– Перечень событий, подлежащих аудиту

№, п/п	Событие	Тип события	Пояснения и рекомендации
1	Аутентификация	И	Выполнена успешная аутентификация пользователя/администратора на данном узле
2	Блокировка пользователя	И	Выполнена блокировка пользователя/администратора на данном узле
3	Ошибка аутентификации	О	Произошла ошибка при выполнении аутентификации пользователя (неверный ЭК или пароль) на данном узле
4	Разблокировка пользователя	И	На данном узле выполнено снятие блокировки пользователя
5	Запрос на доступ к защищаемому ресурсу (виртуальной машине)	И	Пользователем выполнен запрос на запуск виртуальной машины.
6	Создание объекта	И	Выполнено создание новой виртуальной машины администратором.
7	Уничтожение объекта	И	Выполнено удаление виртуальной машины администратором.
8	Изменение правил разграничения доступа	И	Администратором выполнено изменение правил разграничения доступа к виртуальной машине
9	Ввод сменного ключа KEY_1	И	Выполнена запись сменного ключа KEY_1 с ЭК в плату изделия на данном узле
10	Ввод сменного ключа KEY_2	И	Выполнена запись сменного ключа KEY_2 с ЭК в плату изделия на данном узле
11	Генерация сменных ключей KEY_1	И	На АРМ Администратора выполнена генерация сменных ключей KEY_1
12	Генерация сменных ключей KEY_2	И	На АРМ Администратора выполнена генерация сменных ключей KEY_2

13	Загрузка ОС	И	Переход к загрузке ОС
14	Ошибка при контроле векторов	О	Нарушена целостность носителя данных (СПО) на данном узле
15	Прием команды смены ключей маскирования	И	На данном узле принята команда смены ключей маскирования
16	Регистрация пользователя	И	На АРМ Администратора – выполнено создание нового пользователя. На терминале/сервере – выполнена регистрация существующего пользователя, созданного ранее на АРМ Администратора
17	Смена ключей маскирования	И	На терминале/сервере выполнена смена ключей маскирования
18	Смена пароля пользователя	И	Выполнена смена пароля пользователя/администратора на данном узле
19	Старт сессии	И	Начало работы очередной сессии
20	Удаление пользователя	И	Выполнено удаление пользователя из списка
21	Установка векторов	И	Успешно выполнена установка векторов
22	Очистка журнала	И	Успешно выполнена очистка ЖРС

Примечание - *События в ЖРС могут быть двух типов:*

1) информационные события (И);

2) события, связанные с ошибками администратора/пользователя (О).

5 Описание операций

5.1 Генерация ИБ

После установки ПАК «Горизонт-ВС» на *серверы виртуализации*, *АРМ администратора* и *терминалы* необходимо произвести развертывание административной группы согласно руководству администратора МБРЦ.468313.001 ИЗ.02-01 и первоначальную настройку изделия согласно руководству администратора МБРЦ.468313.001 ИЗ.02-02.

5.2 Описание старта ПАК «Горизонт-ВС»

Перед включением *АРМ администратора* и *сервера виртуализации* необходимо подключить съемный USB-носитель с установленным программным обеспечением КП «Терминал-Сервер» в один из свободных USB-разъемов на сервере. После этого следует включить питание сервера кнопкой **Power**. Далее необходимо зайти в BIOS и установить в качестве основного загрузочного устройства подключенный USB-накопитель.

После сохранения настроек и перезагрузки сервера виртуализации администратору необходимо пройти процедуру аутентификации: установить ЭК в считыватель и ввести пароль. После успешной аутентификации и прохождения процедуры контроля целостности на мониторе будет отображаться процесс загрузки ПАК «Горизонт-ВС».

Правильность старта ПАК «Горизонт-ВС» подтверждается успешной загрузкой КП «Терминал-Сервер», вид которого приведен на рисунке ниже (**Рисунок 4**).

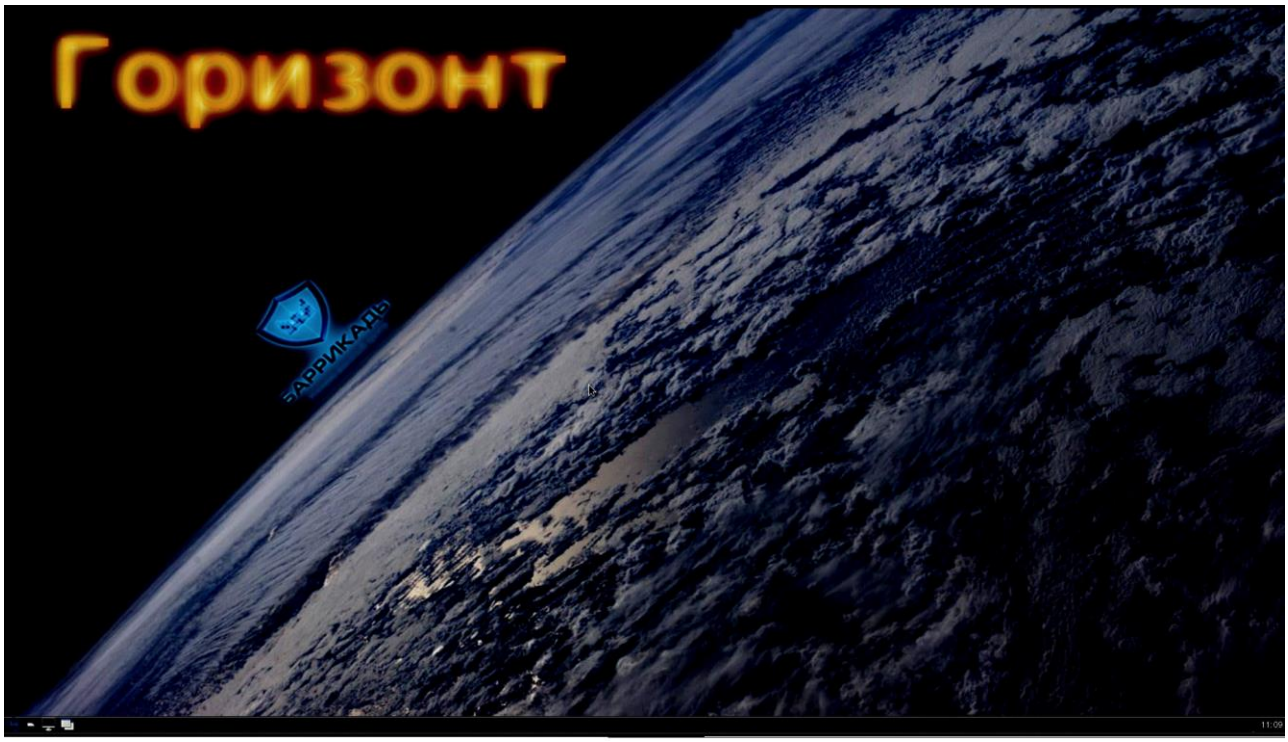

Рисунок 4 – Вид рабочего стола сервера виртуализации

В случае *терминалов* в начале работы пользователь должен установить индивидуальный USB-носитель в свободный разъем USB-порта и включить терминал кнопкой включения питания (**Power**). После этого пользователю необходимо пройти процедуру идентификации и аутентификации: установить ЭК в считыватель и ввести пароль. После успешной процедуры контроля целостности произойдет автоматическая загрузка КП «Терминал-Сервер» с USB-носителя, и пользователь осуществляет доступ в среду операционной системы (ОС), установленной на виртуальной машине, исполняемой на *сервере виртуализации*.

5.3 Представление реализации для политики дискретного доступа

В таблице ниже (Таблица 7) приведено соответствие показателей защищенности, функций безопасности и компонентов ПАК «Горизонт-ВС», реализующих политику дискреционного управления доступом.

Таблица 7 – Соответствие показателей защищенности, функций безопасности и компонентов ПАК «Горизонт-ВС»

Наименование показателя защищённости	Функция безопасности изделия	Функциональные требования безопасности изделия	Модули, реализующие функциональные возможности
Дискреционный принцип контроля доступа	Дискреционный контроль доступа	FDP_ACC.2 полное управление доступом FDP_ACF.1 управление доступом, основанное на атрибутах безопасности FMT_MTD.1 Управление данными ФБО	Libvirt Kernel Start-spice OpenNebula Vmacd

В библиотеке libvirt реализована функция безопасности дискреционного контроля доступа, которой обеспечивает наличие для каждой пары субъект-объект явное и недвусмысленное перечисление допустимых типов доступа. Субъектами являются пользователи ПАК «Горизонт-ВС», объектами – виртуальные машины. Каждая ВМ в системе запускается с UID запустившего её пользователя.

Имя пользователя задаётся администратором в параметрах ВМ в графическом интерфейсе **virt-manager** или в системе группового управления на базе **OpenNebula**. Установка дискреционных прав на процесс **QEMU**, непосредственно исполняющий ВМ, реализована в файле исходных текстов: *src/security/security_dac.c*, входящем в пакет libvirt, в функции ***virSecurityDACSetProcessLabel (virSecurityManagerPtr mgr, virDomainDefPtr def ATTRIBUTE_UNUSED)*** и функции ***int virSetUIDGID (uid_t uid, gid_t gid, gid_t *groups ATTRIBUTE_UNUSED, int ngroups ATTRIBUTE_UNUSED)***.

Модуль **vmacd** прослушивает порт 5910 *сервера виртуализации* в ожидании запроса на подключение от терминала. Ожидание сессионного маскировочного ключа МИиКДС «Шина» на стороне *сервера виртуализации* производится в функции ***int apmdz_wait_for_key (u_char *client_ipaddr)*** файла исходных текстов *apmdz.c* пакета vmacd.

Размаскирование запроса от *терминала* реализовано в функции ***int apmdz_decrypt (u_char *ipaddr, u_char *encrypted_data, int encrypted_data_size, u_char **decrypted_data, int *decrypted_data_size)*** файла исходных текстов *apmdz.c* пакета vmacd.

Подключение к библиотеке libvirt, выполняющей функции управления виртуальными машинами, происходит с помощью функции ***virDomainGetInfo*** модуля libvirt (функция ***u_char *update_domain (const char *vm_name, bool run_domain)*** в файле исходных текстов *vmacd.c* пакета vmacd).

Генерация сеансового порта и пароля для подключения *терминала* реализована в функции ***void update_secret (xmlDocPtr doc, xmlNodePtr *node_answer, bool read_only)*** в файле исходных текстов *vmacd.c* пакета vmacd.

XML-ответ на запрос *терминала* маскируется средствами МИиКДС «Шина» в функции ***int apmdz_encrypt (u_char *ipaddr, u_char *raw_data, int data_size, u_char **encrypted_data, int *encrypted_data_size)*** файла исходных текстов *apmdz.c* пакета vmacd.

Сеанс подключения терминала к серверу виртуализации начинается с SASL-аутентификации подключающегося пользователя на утилите vmacd, работающей на сервере виртуализации, что реализовано в функции ***int vmacd_sasl_negotiate(FILE *in, FILE *out, sasl_conn_t *conn, char *server)*** (строки 1682-1766) файла исходных текстов *start-spice.c* пакета start-spice.

В случае успешной аутентификации происходит попытка получения у модуля vmacd списка ВМ, принадлежащих аутентифицированному пользователю, и их состояний. В случае неуспешной аутентификации, соединение разрывается.

5.4 Управление доступом пользователей

Внимание!

1. На одном терминале разрешается регистрировать только одного пользователя согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО, п. 6.4).

2. На сервере виртуализации согласно условиям по безопасности разрешается регистрировать только администраторов СДЗ.

Для регистрации пользователя на узле:

1. В **Таблице регистрации пользователя** в выпадающем меню в колонке **Отметка о регистрации** выбрать пункт **Зарегистрирован** для соответствующего узла (Рисунок 5).

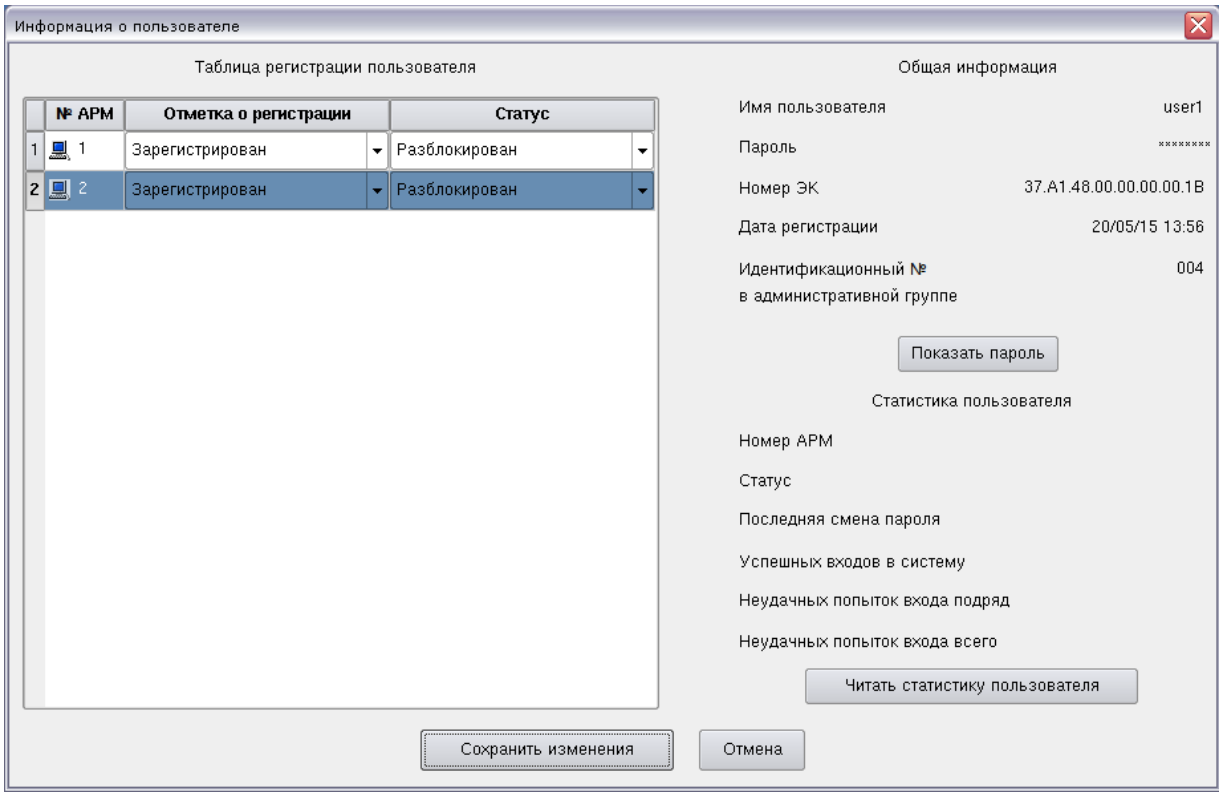

Рисунок 5 – Регистрация пользователя на узле

2. Нажать кнопку **Сохранить изменения** в нижней части окна.
3. Для блокировки/разблокировки пользователя на узле АГ, в строке узла (2) в колонке **Статус** выбрать **Заблокирован/Разблокирован**.
4. Нажать кнопку **Сохранить изменения**.

При успешном сохранении изменений на экране появится сообщение (Рисунок 6).

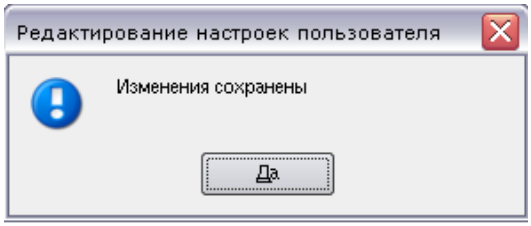

Рисунок 6 – Информационное сообщение

Внимание! *На АРМ администратора (узел №001) необходимо заблокировать пользователя после его создания (регистрации), изменив в таблице регистрации пользователей его статус на узле* ***№001****.*

Для предоставления доступа к ВМ пользователю системы:

1. На сервере виртуализации зайти в СГУ.
2. Зайти в раздел **Машины** → **ВМ**.
3. Выделить флагом ВМ и выбрать в верхнем меню пункт **Сменить владельца** (Рисунок 7).

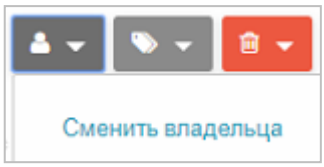

Рисунок 7 – Пункт меню «Сменить владельца»

4. В открывшемся окне необходимо выбрать пользователя, которому будет предоставлен доступ к ВМ и нажать кнопку **ОК** (8).

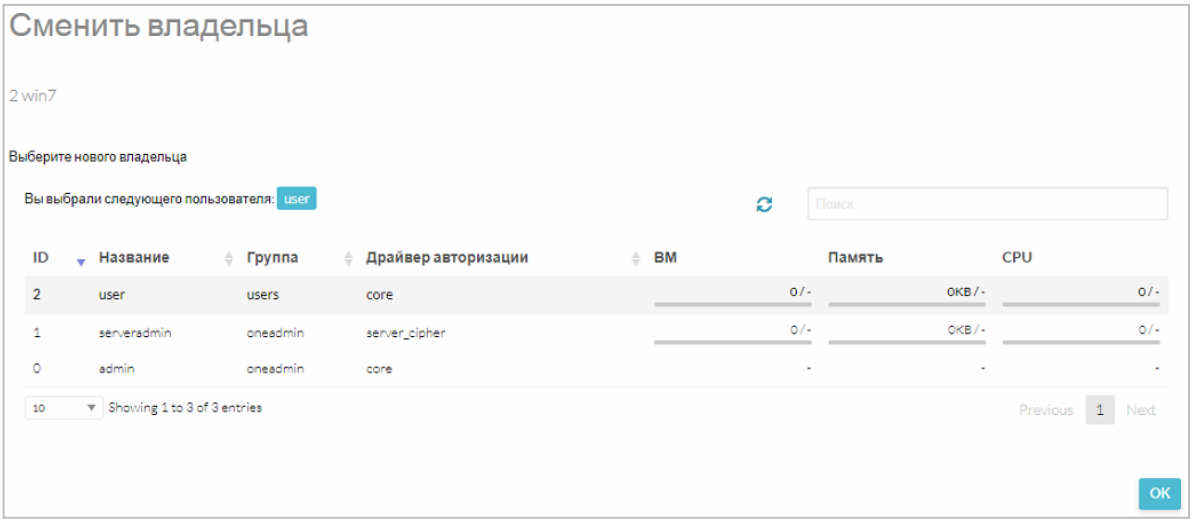

Рисунок 8 – Назначение пользователя ВМ

После назначения прав ВМ будет запускаться от имени указанного пользователя.

***Внимание**! Одному пользователю назначается только одна виртуальная машина согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО).*

Перечень принятых сокращений

Сокращение	Расшифровка
АГ	Административная группа
АРМ	Автоматизированное рабочее место
ВМ	Виртуальная машина
ГИС	Государственная информационная система
ЖРС	Журнал регистрации событий
КСЗ	Комплекс средств защиты
КП	Комплекс программ
МИиКДС	Модуль идентификации и контроля доверенной среды
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПРД	Правила разграничения доступа
РД	Руководящий документ
СВТ	Средство вычислительной техники
СДЗ	Средство доверенной загрузки
ИБ	Функции безопасности
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЭК	Электронный ключ
ЭНП	Энергонезависимая память
UID	User ID

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подпись	Дата
	Измен ен-ных	Заменен ных	Нов ых	Аннулирова нных					