Для служебного пользования
Экз. № ___

УТВЕРЖДЕН
МБРЦ.468313.002-ЛУ

ПРОГРАММНОЕ ИЗДЕЛИЕ “БАЗОВЫЕ СРЕДСТВА ВИРТУАЛИЗАЦИИ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ “ГОРИЗОНТ-ВС”

Руководство по КСЗ
МБРЦ.468313.002 Д10
Листов 39

Литера

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

АННОТАЦИЯ

Настоящий документ руководство по комплексу средств защиты (КСЗ) МБРЦ.468313.002 Д10 (далее по тексту – руководство по КСЗ) содержит сведения о КСЗ программного изделия “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС” МБРЦ.468313.002 (далее по тексту – ПИ “Горизонт-ВС”) 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, описание контролируемых функций, руководство по генерации КСЗ, описание старта ПИ “Горизонт-ВС”.

Для работы с руководством по КСЗ следует ознакомиться с документами:

– МБРЦ.468313.002 Д2. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Руководство администратора;

– МБРЦ.468313.002 РЭ. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Руководство по эксплуатации.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

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

В состав изделия входит комплекс программ “Терминал-Сервер” RU.МБРЦ.501130.01-03 (далее по тексту – КП “Терминал-Сервер”).

ПИ “Горизонт-ВС” должен соответствовать требованиям РД ФСТЭК России по 3 классу защищенности и реализовывать следующие показатели защищенности:

- дискреционный принцип контроля доступа;
- мандатный принцип контроля доступа;
- очистку памяти;
- изоляцию модулей;
- маркировку документов;
- защиту ввода и вывода на отчуждаемый физический носитель информации;
- сопоставление пользователя с устройством;
- идентификацию и аутентификацию;
- регистрацию событий;
- взаимодействие пользователя с КСЗ;
- надежное восстановление;
- целостность КСЗ;
- тестирование;
- руководство пользователя;
- руководство по КСЗ;
- тестовую документацию;
- конструкторскую и проектную документацию.

ПИ “Горизонт-ВС” может применяться для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, государственных информационных систем (ГИС) до 1 класса защищенности включительно согласно приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации не составляющей государственную тайну, содержащейся в государственных информационных системах» и

методическому документу от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах», в информационных системах персональных данных (ИСПДн) до 1 уровня защищенности включительно согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и при построении автоматизированных систем (АС) до 1 класса защищенности включительно согласно приказу 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».

Перечень мер и порядок их выполнения с использованием изделия приведен в таблице 1.1.

Таблица 1.1 – Соответствие показателей защищенности и мер защиты информации в ГИС

№ п/п	Условное обозначение и номер меры	Мера защиты информации в ГИС	Показатели защищенностии
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Идентификация и аутентификация
2	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Идентификация и аутентификация
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Идентификация и аутентификация
4	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Идентификация и аутентификация
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Идентификация и аутентификация
6	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Идентификация и аутентификация

№ п/п	Условное обозначение и номер меры	Мера защиты информации в ГИС	Показатели защищенностии
7	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Дискреционный принцип контроля доступа; Мандатный принцип контроля доступа
8	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Идентификация и аутентификация
9	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Идентификация и аутентификация
10	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Идентификация и аутентификация
11	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Целостность КСЗ
12	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Регистрация событий
13	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Регистрация событий
14	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	Регистрация событий
15	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	Регистрация событий
16	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Регистрация событий
17	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Регистрация событий
18	РСБ.7	Защита информации о событиях безопасности	Регистрация событий
19	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях	Регистрация событий

№ п/п	Условное обозначение и номер меры	Мера защиты информации в ГИС	Показатели защищенностии
		отдельных пользователей в информационной системе	
20	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Целостность КСЗ
21	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Дискреционный принцип контроля доступа; Мандатный принцип контроля доступа
22	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	
23	ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	
24	ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	Идентификация и аутентификация
25	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти	Изоляция модулей
26	ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы	Очистка памяти

2 МОДЕЛЬ ЗАЩИТЫ

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

– защищается информация, хранимая и обрабатываемая в ПИ “Горизонт-ВС”;

– **объектами** доступа являются файлы;

– **субъектами** доступа являются пользователи;

– изделие работает только с идентифицированными и аутентифицированными пользователями;

– механизм аутентификации построен на паре имя-пароль; доступ разрешается, если имя и пароль пользователя совпадают с зарегистрированными в изделии;

– доступ всех субъектов к объектам контролируется согласно **дискреционным и мандатным 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 2.1.

Таблица 2.1 – Пример матрицы доступа

Субъекты (пользователи)	Объекты (файлы)			
	O_1	O_2	…	O_n
S_1	rwxat	rwx		rwxa
S_2	r	rwx		x
…				-
S_n	rwxa	rx		rw

Элементами матрицы могут быть любые комбинации из четырех прав: r – чтение, w – запись, x – исполнение, a – дополнение, t – удалить файл может только владелец этого файла. 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, тогда соответствующий доступ разрешается, в

противном случае запрос на доступ отклоняется. Поскольку во время функционирования системы изменяется количество субъектов и объектов, а также меняются права доступа субъектов к объектам, изменяется и матрица доступа.

Основным положением модели мандатного доступа является назначение всем участникам процесса документооборота и всем документам специальной метки, например, «секретно», «сов. секретно» и т.д., получившей название уровня безопасности. Уровни представляют собой множество, на котором определено отношение порядка, например, уровень «сов. секретно» считается более высоким чем уровень «секретно», или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании следующих правил:

1. уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило защищает информацию, обрабатываемую более доверенными субъектами, от доступа со стороны менее доверенных. Второе правило предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса к низкоуровневым.

Таким образом, если в дискреционной модели управление доступом происходит путем наделения пользователей полномочиями выполнять определенные операции над определенными объектами, то в мандатной модели управляют доступом неявным образом – с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними.

Права доступа могут быть изменены только администратором.

Правила изменения ПРД:

Для формализации правил изменения ПРД введем ряд обозначений.

1) Множество зарегистрированных в системе пользователей U, включающее привилегированного пользователя (суперпользователя) {U0} с нулевым идентификатором и администратора {Ua}. Пользователи U представлены в системе посредством множества субъектов S.

2) Множество объектов доступа O включает: системные файлы и процессы Oc,

файлы и процессы КСЗ Оксз, файлы и процессы непривилегированных пользователей Оп. При этом Ос ∪ Оксз ∪ Оп = О.

3) Атрибут владения объектом доступа Ao=<Au0, Au1, Au2, …, AuM>, где Aui – атрибут принадлежности объекта пользователю Ui.

4) Множество меток доступа I включает следующие метки:

а) множество зарегистрированных в системе администратором меток доступа к объектам Io;

б) множество зарегистрированных в системе администратором меток доверия к субъектам Is.

Определим ПРД.

1) Субъекты множества Sксз имеют неограниченный доступ к множеству объектов доступа Оксз для эффективного управления ПРД.

2) Субъекты множества Sп не имеют доступа к объектам множества Оксз.

3) Субъекты, принадлежащие множеству Sксз, имеют доступ к объектам из множества Оп.

Правила изменения ПРД.

1) Регистрацию пользователя Ua в системе выполняет пользователь U0.

2) Asi назначается для пользователя Ui пользователем Ua.

3) {Aoj} назначается автоматически в соответствии с {Is} субъекта, создавшего объект.

4) Модификации {Ao} могут выполняться пользователем {Ua} произвольно.

5) Пользователь {Ui} может повышать {Ioi}, но не выше {Lui}.

Такие правила изменения ПРД определяют, что гриф информации, передаваемой между любой парой непривилегированных пользователей системы, не может быть произвольно или непроизвольно снижен, а 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.

– для контроля действий пользователей, особенно имеющих административные полномочия, используется **система аудита** с функцией протоколирования фактов несанкционированного доступа / нарушений модели безопасности в реальном времени. В изделии регистрируются:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу;
- создание и уничтожение объекта;
- действия по изменению ПРД;
- все действия оператора и выделенных пользователей.

– **контроль целостности** на *сервере виртуализации,* системные файлы которого копируются на жесткий диск, производится для неизменяемой части корневой файловой системы на жестком диске. Для каждого файла, находящегося в директории ***/etc***, вычисляется MD5-hash функция, которая сравнивается с аналогичной суммой, вычисленной для данного файла на этапе сборки. Контроль целостности USB-накопителей с ПИ “Горизонт-ВС” производится путем вычисления контрольных сумм файлов согласно процедуре, описанной в формуляре МБРЦ.468313.002 ФО (Приложение А) и сверки полученных значений с указанными в формуляре. Данную процедуру необходимо проводить перед каждым запуском *сервера виртуализации* и *терминалов*.

– в ПИ “Горизонт-ВС” реализована **изолированная программная среда**. Процесс закрытия программной среды основан на следующих положениях. В процессе инициализации системы автоматически генерируется пара закрытый и открытый ключ, и для всех без исключения инсталлируемых на жёсткий диск файлов ПИ “Горизонт-ВС” 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 автоматически уничтожается. В системе остаётся только открытый ключ, в случае удаления или подмены которого, загрузка и функционирование ПИ “Горизонт-ВС” будет невозможно.

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 ПИ “Горизонт-ВС”, невозможно выполнить какой-либо файл, не инсталлированный в ходе процедуры начальной установки, либо изменённый в процессе эксплуатации.

– **очистка оперативной памяти** осуществляется при её перераспределении посредством перезаписи каждого байта нулями. Очистка **внешней памяти** на хранилище SAMBA осуществляется при её освобождении и перераспределении путем записи случайной последовательности.

– любые **носители информации**, предназначенные для использования в ПИ “Горизонт-ВС”, предварительно должны быть учтены в *сервере виртуализации* как описано в руководстве администратора МБРЦ.468313.002 Д2 (п. 2.8.11). Очистка памяти на внешних USB-носителях реализуется средствами гостевых ОС;

– установка пароля для графического сервера Spice обязательна согласно руководству администратора МБРЦ.468313.002 Д.2 (п. 2.8.9);

– гостевые ОС, устанавливаемые в ВМ, должны иметь сертификат соответствия не ниже 3 класса защищенности от НСД и не ниже 2 уровня контроля отсутствия недекларированных возможностей (НДВ).

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Функция идентификации и аутентификации пользователей в ПИ “Горизонт-ВС” основывается на паре имя-пароль.

В изделии поддерживаются два типа пользователей: администраторы и пользователи, также существует суперпользователь root.

При регистрации в изделии каждому пользователю присваивается пароль и системное имя. Системное имя связывается в КП “Терминал-Сервер” с идентификатором пользователя — UID (User ID).

Функция идентификации и аутентификации пользователей решается следующим методом. На *сервере виртуализации* пользователи создаются при помощи утилиты Менеджер пользователей ВМ (*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* с использованием SASL-аутентификации и передает ей имя и пароль пользователя. 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.

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 ***var/log/messages***.

Если в системе предполагается работа с сервером, поддерживающим Astra Linux Directory (ALD), то процедура аутентификации выполняется следующим образом. В качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов LDAP. Вся служебная информация располагается на выделенном сервере ALD. Сервер виртуализации совершает LDAP-запрос к серверу ALD. Если получен ответ, то переданные данные используются в

качестве списка имен пользователей. Выбрав из списка нужного пользователя, можно назначить его на ВМ, и она запустится с его мандатными и дискреционными атрибутами.

Если ответа от сервера ALD получено не было, то он считается недоступным, и работа ведется с локальной базой пользователей (***/etc/shadow***) как описано выше.

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 к вводу имени и 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: имя пользователя и пароль, – что позволяет изделию заносить информацию об идентификации и аутентификации, а также дальнейших действиях пользователя в журнал регистрации событий.

4 ДИСКРЕЦИОННЫЙ ПРИНЦИП КОНТРОЛЯ ДОСТУПА

В ПИ “Горизонт-ВС” реализована функция безопасности дискреционного контроля доступа субъектов (пользователей) к объектам (файлам). 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 ВМ доступ предоставляется по результатам процедуры авторизации, то есть обработки запроса на основе дискреционных правил разграничения доступа. Матрица доступа пользователей к ВМ приведена в таблице 4.1.

Таблица 4.1 – Матрица доступа пользователей к ВМ

Объект / Субъект	ВМ 1	ВМ 2	…	ВМ N
Администратор	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление	Создание Доступ Модификация Удаление
Пользователь 1	Доступ	—	—	—
Пользователь 1	—	Доступ	—	—
…	…	…	…	…
Пользователь N	—	—	—	Доступ

Для каждой ВМ можно добавить устройство SAMBA, которое подключается к гостевой ОС по протоколу CIFS и отображается как сетевое хранилище (далее по тексту – “хранилище”). К документам, находящимся на “хранилище”, применяется дискреционный контроль доступа. Матрица доступа ВМ к файлам приведена в таблице 4.2.

Таблица 4.2 – Матрица доступа ВМ к файлам

Объект / Субъект	Файл 1	Файл 2	…	Файл N
ВМ1	rwxat	rwxat	rwxat	rwxat
ВМ2	rw	—	r	—

ВМ3	—	rwx	—	—
…	…	…	…	…
ВМN	r	—	—	at

Таким образом, доступ субъекта к объекту рассматривается как доступ ВМ, назначенной пользователю, к файлам на “хранилище”.

Таким образом, 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 (r – чтение, w – запись, x – исполнение, a – дополнение, t – удалить файл может только владелец этого файла). Матрица доступа для ПИ “Горизонт-ВС” приведена в таблице 4.1.

Таблица 4.1 – Матрица доступа

Объект / Субъект	Файл 1	Файл 2	…	Файл N
Администратор	rwxat	rwxat	rwxat	rwxat
Пользователь 1	rw	—	r	—
Пользователь 1	—	rwx	—	—
…	…	…	…	…
Пользователь N	r	—	—	at

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 на доступ к объекту этот вид доступа предоставляется ему вне зависимости от правил. Доступ к объекту явно запрещается субъектам с несоответствующими именем или паролем, 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.

Процедура изменения списка пользователей и назначения правил доступа к объектам описана в руководстве администратора МБРЦ.468313.002 Д2 (п.п. 2.5, 2.6).

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

Таким образом, реализованный в ПИ “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 (файлу);
- создание и уничтожение объекта (файлов);
- действия по изменению ПРД.

5 МАНДАТНЫЙ ПРИНЦИП КОНТРОЛЯ ДОСТУПА

Мандатный принцип контроля доступа обеспечивает управление доступом путем сопоставления мандатных меток безопасности (иерархических (грифы секретности)) каждого субъекта и каждого объекта.

Субъектам и объектам доступа присваиваются мандатные метки, на основании сравнения которых по определенным правилам диспетчер доступа предоставляет либо отклоняет доступ субъекта к объекту. На сервере виртуализации существуют специальные механизмы, позволяющие назначить на каждую из ВМ метку доступа, причём на каждую ВМ можно назначить только один уровень доступа. Все документы, записанные на “хранилище”, получают метку конфиденциальности, соответствующую метке конфиденциальности ВМ, из которой был осуществлен доступ к “хранилищу”.

Иерархические уровни мандатных меток задаются суперпользователем в файле *translate* как описано в руководстве администратора МБРЦ.468313.002 (п. 2.6).

Реализация диспетчера доступа требует от субъекта наличия прав доступа по обоим механизмам – по мандатному и по дискреционному, в противном случае доступ запрещен.

При создании объекта на “хранилище ведется аудит данного события (информация сохраняется в файл ***/var/log/libvirt/libvirtd.log***).

При попытке открыть уже созданный объект в “хранилище доступ осуществляется по следующим правилам:

1. Если владелец объекта или субъект доступа есть суперпользователь (UID=0), предоставляется доступ на выполнение любого открытия;

2. Если требуется открыть объект в режиме только чтение или исполнение, осуществляется проверка прав субъекта доступа; операция разрешается при выполнении следующего условия: не превышение численного значения иерархической метки объекта доступа численного значения иерархической субъекта доступа;

3. Если требуется открыть объект в режиме запись, осуществляется проверка прав субъекта доступа; операция разрешается при выполнении следующего условия: не превышение численного значения иерархической метки субъекта доступа численного значения иерархической объекта доступа.

4. Если требуется открыть объект в режиме чтение и запись, осуществляется проверка прав субъекта доступа; операция разрешается при

выполнении следующего условия: равенство численных значений иерархических меток субъекта и объекта доступа.

Аудит при открытии объекта на устройстве SAMBA осуществляется как при успешном завершении операции, так и в ином (информация сохраняется в файл ***/var/log/libvirt/libvirtd.log***).

При попытке удаления объекта осуществляется следующая методика мандатного контроля доступа:

1. Если владелец объекта или субъект доступа есть суперпользователь (UID=0), доступ предоставляется;

2. Доступ предоставляется, если выполняется условие: равенство численных значений иерархических меток субъекта и объекта доступа.

Аудит при удалении объекта в разделяемой памяти осуществляется как при успешном завершении операции, так и в ином случае (информация сохраняется в файл ***/var/log/libvirt/libvirtd.log***).

Как при открытии, так и при удалении объектов в разделяемой памяти осуществляется дискреционный контроль доступа к объекту.

После удаления каждого пользователя утилита *vm-users* осуществляет поиск файлов в директории ***/srv/samba***, принадлежащих удаляемому пользователю, и изменяет их владельца на пользователя root.

6 ИЗОЛЯЦИЯ МОДУЛЕЙ

ПИ “Горизонт-ВС” гарантирует, что непривилегированный процесс не получит данные чужого процесса, если это не разрешено ПРД. Это означает, что процессы не могут получить неочищенную память (как оперативную, так и дисковую).

Каждая ВМ, исполняемая на сервере, является процессом, т.е. каждая машина — это отдельно взятый процесс. Этот процесс изолирован и исполняется в своем контексте. Контекстную изоляцию на аппаратном уровне обеспечивает процессор. В административном режиме можно включить (отключить) механизм для очистки высвобождаемой оперативной памяти. Если процесс освобождает определенный сегмент памяти, то этот сегмент принудительно зачищается.

Виртуальное аппаратное окружение для гостевых операционных систем (ОС) ВМ обеспечивается модулем QEMU. Гостевые виртуальные процессоры представляются в ядре системы как POSIX потоки, то есть процессоры гостевой системы представлены для ядра хостовой системы как изолированные друг от друга и в рамках основного потока процессы.

Реализация модели памяти обеспечивает поддержку:

- отслеживания изменений памяти гостевой ВМ;
- инициализацию памяти для KVM;
- инициализацию ioeventfd-регионов для KVM.

Память моделируется как ацикличный граф объектов MemoryRegion, которые будут описаны ниже. RAM и MMIO области являются конечными узлами или листьями графа, тогда как другие узлы представляют собой шины, контроллеры памяти и перенаправляемые области памяти.

Область памяти не уничтожается до тех пор, пока она используется устройством или процессором. В QEMU действует общее правило не создавать и не уничтожать области памяти динамически в течение времени жизни устройства. Возможен только вызов функции ***object_unparent()*** в callback вызове instance_finalize владельца области памяти. Динамически зарезервированная структура данных, которая содержит область памяти, потом должна быть явно освобождена в обратном вызове instance_finalize.

Таким образом, ВМ функционирует как изолированный процесс в пространстве пользователя. Диапазоны областей памяти различных виртуальных машин относятся к разным процессам и не перекрываются. Память для гостевой ВМ выделяется функцией *glib g_malloc0*, которая при выделении памяти заполняет выделяемую

область значением “0”. Выделяемая гостевой ВМ память в QEMU разделяется на виртуальные регионы, часть из которых относится к отображаемым диапазонам памяти устройств ввода-вывода. При обращении к областям памяти устройств ввода-вывода осуществляется вызов callback функций, программно эмулирующих поведение соответствующих устройств ввода-вывода.

7 ОЧИСТКА ПАМЯТИ

Требование показателя защищенности “Очистка памяти” при освобождении (перераспределении) внешней и оперативной памяти предотвращать доступ субъекту к остаточной информации решается следующим методом.

7.1 Очистка внешней памяти на общем хранилище

В ПИ “Горизонт-ВС” реализован механизм очистки неиспользуемых блоков файловой системы при их освобождении. Данные любых удаляемых или уменьшаемых файлов в пределах заданной файловой системы перезаписываются случайными байтами, полученными из функции rand() из библиотеки glibc.

Работа данного механизма снижает скорость выполнения операций удаления и уменьшения размера файла.

Очистка внешней памяти на USB-накопителях осуществляется средствами гостевой ОС, установленной на ВМ.

7.2 Очистка памяти на дисках гостевых ОС

Каждая виртуальная машина, исполняемая на сервере виртуализации, является процессом в оперативной памяти. После всех настроек ВМ с помощью библиотеки libvirt осуществляется создание «снимка» исходного состояния ВМ под названием default и сохранение его в директории, где сохранен виртуальный диск ВМ. При работе пользователей с данной ВМ, она будет восстанавливаться из данного «снимка», таким образом, производится очистка памяти.

Примечание: Работа в таком режиме возможна только с виртуальными дисками формата qqow2.

Также при уничтожении ВМ можно установить флаг “Очистить связанные хранилища перед удалением”. При этом происходит заполнение дискового пространства, занимаемого хранилищем, случайным числом, генерируемым функцией rand() из библиотеки glibc.

7.4 Очистка оперативной памяти

Очистка оперативной памяти в ПИ “Горизонт-ВС” производится при её перераспределении. Оперативная память перед каждым выделением заполняется заданным случайным байтом, а перед каждым освобождением — заполняется его инвертированным значением.

8 РЕГИСТРАЦИЯ СОБЫТИЙ

На сервере виртуализации с установленным ПИ “Горизонт-ВС” 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 ПИ “Горизонт-ВС”.

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

- *log_file* — файл, в котором будут храниться логи подсистемы аудита (***var/log/audit/audit.log***);
- *log_format* — формат, в котором будет сохранены логи (***raw***);
- *freq* — максимальное число записей протокола, которые могут храниться в буфере (***20***);
- *flush* — режим синхронизации буфера с диском (***incremental*** — переносить данные из буфера на диск с частотой, указанной в значении параметра *freq*);
- *max_log_file* — максимальный размер файла лога в мегабайтах (**6**);
- *max_log_file_action* — действие при превышении максимального размера файла лога (***rotate*** – осуществлять перезапись журнала).

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

На серверах резервирования информация о сделанных резервных копиях и ошибках резервирования заносится в файлы ***/var/log/audit/audit.log*** и ***var/log/messages***. Данные о файлах, выгруженных при резервном копировании, заносятся в файлы ***/var/log/audit/audit.log*** и ***var/log/messages*** на сервере виртуализации.

Требования РД ФСТЭК России для 3 класса защищенности в части регистрации событий и способ их реализации в ПИ “Горизонт-ВС” приводятся в таблице 6.1.

Таблица 6.1 - Регистрация событий

Требования РД ФСТЭК России	Способ реализации ПИ “Горизонт-ВС” требований РД ФСТЭК России в части регистрации событий
ПИ “Горизонт-ВС” должен быть в состоянии осуществлять регистрацию следующих событий: – использование идентификационного и аутентификационного механизма; – запрос на доступ к защищаемому ресурсу (файлы, программы); – создание и уничтожение объекта; – действия по изменению ПРД.	Регистрация событий использования идентификационного и аутентификационного механизма осуществляется КП “Терминал-Сервер”. События сохраняются в файл ***var/log/messages***. Регистрация запросов на доступ к защищаемому ресурсу осуществляется КП “Терминал-Сервер”. События сохраняются в файл ***/var/log/libvirt/libvirtd.log***. Регистрация создания и уничтожения объектов осуществляется КП “Терминал-Сервер”. События сохраняются в файл ***/var/log/libvirt/libvirtd.log***. Регистрация действий по изменению ПРД осуществляется КП “Терминал-Сервер”. События сохраняются в файл ***/var/log/audit/audit.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 подсистеме регистрации событий КП “Терминал-Сервер” регистрируется дата, время, пользователь, осуществляющий действия, тип события и результат (успешное выполнение или ошибка).
ПИ “Горизонт-ВС” должен содержать средства выборочного ознакомления с регистрационной информацией.	Выборочное ознакомление с событиями подсистемы регистрации событий КП “Терминал-Сервер” осуществляется путем применения ряда команд в консоли *сервера виртуализациии*. Подробнее команды описаны в руководстве администратора МБРЦ.468313.001 Д2 (п. 2.14).

9 КОНТРОЛЬ ЦЕЛОСТНОСТИ

Для обеспечения контроля целостности в ПИ “Горизонт-ВС” реализованы:

- средство контроля целостности неизменяемой части корневой файловой системы;
- средства создания замкнутой (изолированной) программной среды.

7.2 Средства контроля целостности неизменяемой части корневой файловой системы

На *сервере виртуализации* системные файлы копируются на жесткий диск, поэтому 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* и *терминалов*.

7.3 Средства создания замкнутой (изолированной) программной среды

В ПИ “Горизонт-ВС” реализован механизм изоляции программной среды.

Список требований для обеспечения изолированной программной среды, методы их проверки и ожидаемые результаты проверок приведены в таблице 7.1

Таблица 7.1 – 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 инициализации системы и удаляется после её завершения.	-
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.

Инсталляция и дальнейшая загрузка ПИ “Горизонт-ВС” производится с USB-накопителя. После инсталляции и настройки системы автоматически генерируется пара закрытый и открытый ключ, и инициализируется механизм защиты. В процессе инициализации, для всех без исключения инсталлируемых на жёсткий диск файлов ПИ “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 автоматически уничтожается. 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 1.

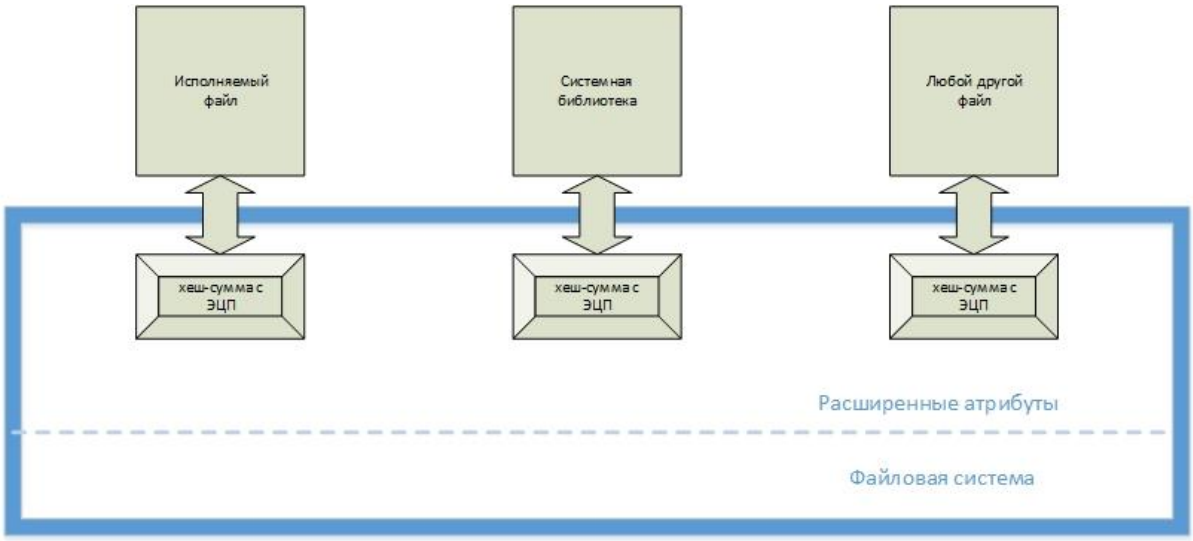

Рисунок 1 – Изолированная программная среда

В ходе функционирования системы осуществляется проверка исполнения файла, согласно алгоритму, приведенному на рисунке 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 ПИ “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 ПИ “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.

10 ЗАЩИТА ВВОДА И ВЫВОДА НА ОТЧУЖДАЕМЫЙ НОСИТЕЛЬ

Любые носители информации, предназначенные для использования в ПИ “Горизонт-ВС”, предварительно должны быть учтены (занесены) в БД сервера виртуализации. Для этого в программе “Менеджер виртуальных машин” предусмотрен пункт меню, через который вызываются окна, осуществляющие считывание модели и уникального ID съемного носителя.

Отчуждаемые физические носители могут рассматриваться относительно ПИ “Горизонт-ВС” с двух точек зрения:

– как блочные или символьные устройства ввода-вывода;

– как блочное устройство, которое может быть смонтировано.

В первом случае устройство представляет собой специальный файловый объект, доступ к которому контролируется мандатными и дискреционными ПРД обычным образом и, следовательно, ввод-вывод остается в рамках контроля этих правил.

Во втором случае отчуждаемый носитель информации содержит в себе образ файловой системы (ФС), которая и хранит данные. Данный носитель может быть смонтирован в заданный каталог, и при этом ФС носителя становится частью (представленной в виде поддерева) корневой ФС. Доступ к объектам данной ФС подчиняется мандатным и дискреционным ПРД обычным образом и, следовательно, ввод-вывод на отчуждаемый носитель остается в рамках контроля этих правил.

Для ПИ “Горизонт-ВС” возможность санкционированного монтирования конкретным пользователем конкретных носителей с конкретными ФС определяется администратором системы. В ПИ “Горизонт-ВС” реализованы средства разграничения доступа к подключаемым устройствам на основе генерации правил.

При подключении носителя фиксируется факт монтирования тома с определенной меткой, после чего блокируются все операции чтения/записи на данном томе. Если метка тома носителя в БД учтенных отсутствует, то доступ к устройству блокируется.

11 МАРКИРОВКА ДОКУМЕНТОВ

Подзадача маркировки документов решается следующим методом. В менеджере виртуальных машин на сервере виртуализации, при создании и редактировании виртуальных машин, каждой виртуальной машине назначается мандатный уровень доступа.

Среди прочих устройств виртуального аппаратного окружения виртуальной машины, можно добавить устройство SAMBA. Это устройство обеспечивает подключение гостевой операционной системы, исполняемой на виртуальной машине, к внешнему или внутреннему файловому хранилищу сервера виртуализации. В окружении гостевой операционной системы, устройство SAMBA возможно подключить по протоколу CIFS. Документ, записанный на это устройство, получает метку конфиденциальности, соответствующую уровню доступа родительской виртуальной машины.

В зависимости от метки конфиденциальности и в соответствии с описанными правилами (правила создаются и описываются администратором на сервере виртуализации), виртуальные машины с разными метками конфиденциальности могут иметь разный уровень доступа к документам, на носителе SAMBA, созданным пользователями машин с иной меткой конфиденциальности.

При печати документа из гостевой операционной системы, определяется метка конфиденциальности виртуального окружения, и в соответствии с этой меткой, средствами сервера виртуализации в документ добавляются дополнительные специальные атрибуты («фонарик», атрибуты пользователя и т.д.). При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1.

В общем случае, если пользователь имеет доступ на чтение документа, он может отправить данный документ на печать.

Каждый запрос на печать документа регистрируется в журнале аудита с указанием результата завершения (успешный / неуспешный / несанкционированный).

Маркировка документов опциональна и может настраиваться администратором в менеджере принтеров в разделе «Свойства принтера».

Информация, выдаваемая в полях штампов при маркировке (угловой штамп, нижний штамп, штамп на последнем листе), содержит следующие данные:

- уровень конфиденциальности документа;
- номер экземпляра;

- учетный номер документа;
- уровень конфиденциальности документа;
- номер листа;
- дата;
- количество отпечатанных экземпляров;
- номер экземпляра;
- адрес для каждого экземпляра;
- учетный номер документа;
- уровень конфиденциальности документа;
- ФИО исполнителя;
- ФИО отправившего на печать;
- дата выдачи документа.

12 СОПОСТАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ С УСТРОЙСТВОМ

ПИ “Горизонт-ВС” обеспечивает ввод-вывод информации на запрошенное пользователем устройство как для произвольно используемых им устройств, так и для идентифицированных (при совпадении маркировки).

ПИ “Горизонт-ВС” включает в себя механизм, обеспечивающий надежное сопоставление мандатного контекста пользователя с мандатным уровнем и категориями, установленными для устройства. Кроме того, механизм сопоставления пользователя с устройством, реализованный в ПИ “Горизонт-ВС”, обеспечивает при проверке совпадения маркировок носителя и пользователя применение дискреционных ПРД.

13 ВОССТАНОВЛЕНИЕ СВОЙСТВ КСЗ ПОСЛЕ СБОЕВ И ОТКАЗОВ

Основными причинами нарушения процесса функционирования КСЗ являются сбои оборудования, приведшие к различным повреждениям ФС. К таковым относятся: сбои электропитания, повреждения носителей информации (жестких дисков), повреждения соединительных кабелей.

В случае повреждения дисков на сервере виртуализации, следует заменить вышедшее из строя оборудование и заново установить ПИ “Горизонт-ВС” с USB-носителя (процедура установки описана в руководстве администратора МБРЦ.468313.002).

В случае повреждения ФС на сервере виртуализации следует проверить целостность файлов. В случае полного соответствия вычисленных контрольных сумм эталонным можно продолжать работу. В противном случае скрипт полностью очистит директорию ***/usr*** и осуществит безусловное копирование неизменяемой корневой части файловой системы.

14 ТЕСТИРОВАНИЕ

Описание тестов функций безопасности приведено в документе функциональное тестирование МБРЦ.468313.001 Д11 (далее по тексту – функциональное тестирование). Для каждой функции безопасности представлены планы и описания процедур тестирования, а также ожидаемые и фактические результаты тестирования.

Согласно требованиям РД ФСТЭК России в части тестирования в средствах вычислительной техники (СВТ) 3 класса защищенности должны тестироваться:

- реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- невозможность присвоения субъектом себе новых прав;
- очистка памяти;
- работа механизма изоляции процессов в оперативной памяти;
- маркировка документов;
- защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
- идентификация и аутентификация, а также их средства защиты;
- запрет на доступ несанкционированного пользователя;
- работа механизма, осуществляющего контроль за целостностью СВТ;
- регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией;
- работа механизма надежного восстановления.

После каждого выпуска обновлений изделия администратор должен проводить тестирование всех функций безопасности согласно документу функциональное тестирование МБРЦ.468313.001 Д11. Плановый выпуск очередного обновления изделия осуществляется один раз в год.

15 ГЕНЕРАЦИЯ КСЗ

После установки ПИ “Горизонт-ВС” на *серверы виртуализации* и *терминалы* необходимо произвести первоначальную настройку изделия согласно руководству администратора МБРЦ.468313.001 Д2 (п. 2.3).

16 ОПИСАНИЕ СТАРТА ПИ “ГОРИЗОНТ-ВС”

14.1 Перед включением *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: ввести имя и пароль. После успешной аутентификации на мониторе будет отображаться процесс загрузки ПИ “Горизонт-ВС”.

Правильность старта ПИ “Горизонт-ВС” подтверждается успешной загрузкой КП “Терминал-Сервер”, вид которого приведен на рисунке 3.

Рисунок 3 – Вид рабочего стола сервера виртуализации

14.2 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: ввести имя и 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*.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	- автоматизированное рабочее место
ВМ	- виртуальная машина
КСЗ	- комплекс средств защиты
КП	- комплекс программ
НДВ	- недекларированные возможности
НСД	- несанкционированный доступ
ОС	- операционная система
ПИ	- программное изделие
ПРД	- правила разграничения доступа
РД	- руководящий документ
СВТ	- средство вычислительной техники
СЗИ	- средство защиты информации
ФСТЭК России	- Федеральная служба по техническому и экспортному контролю
UID	- User ID

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					