УТВЕРЖДЕН

МБРЦ.468313.002-ЛУ

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

Функциональное тестирование

МБРЦ.468313.002 Д11

Листов 38

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

АННОТАЦИЯ

Настоящий документ функциональное тестирование МБРЦ.468313.002 Д11 является основным документом, описывающим порядок действий администратора при проведении тестов программного изделия “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС” МБРЦ.468313.002 (далее по тексту – изделие или ПИ “Горизонт-ВС”).

В документе приведены основные сведения, необходимые администратору для проведения тестов изделия, установленного на *терминалах* и *серверах виртуализации*, созданных на базе персональной электронной вычислительной машины (ПЭВМ).

При проведении тестов необходимо дополнительно руководствоваться следующей эксплуатационной документацией:

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

– МБРЦ.468313.002 Д10. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Руководство по КСЗ;

– 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” используется для организации защищенного исполнения виртуальных машин, а также соединения виртуальных машин и терминалов.

В состав ПИ “Горизонт-ВС” входит комплекс программ “Терминал-Сервер” RU.МБРЦ.501130.02-01 (далее по тексту – КП “Терминал-Сервер”).

Целью функционального тестирования является проверка соответствия изделия показателям защищенности, приведенным в руководящем документе ФСТЭК России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”, по 3 классу защищенности:

– идентификация и аутентификация пользователей;

– дискреционный и мандатный принципы контроля доступа;

– изоляция процессов и очистка памяти;

– регистрация событий защиты;

– контроль целостности программных файлов и данных, а также загрузочных секторов жестких магнитных дисков;

– защита ввода и вывода на отчуждаемый физический носитель информации;

– маркировка документов;

– тестирование;

– сопоставление пользователя с устройством;

– взаимодействие пользователя с комплексом средств защиты (КСЗ);

– надежное восстановление свойств КСЗ после сбоев и отказов оборудования.

Все тесты проводятся на изделии, настроенном согласно эксплуатационной документации.

2 ОПИСАНИЕ ИСПЫТАТЕЛЬНОГО СТЕНДА

2.1 Схема испытательного стенда

Тестирование изделия проводится на стенде, настроенном в соответствии с требованиями эксплуатационной документации. Схема испытательного стенда приведена на рисунке 1.

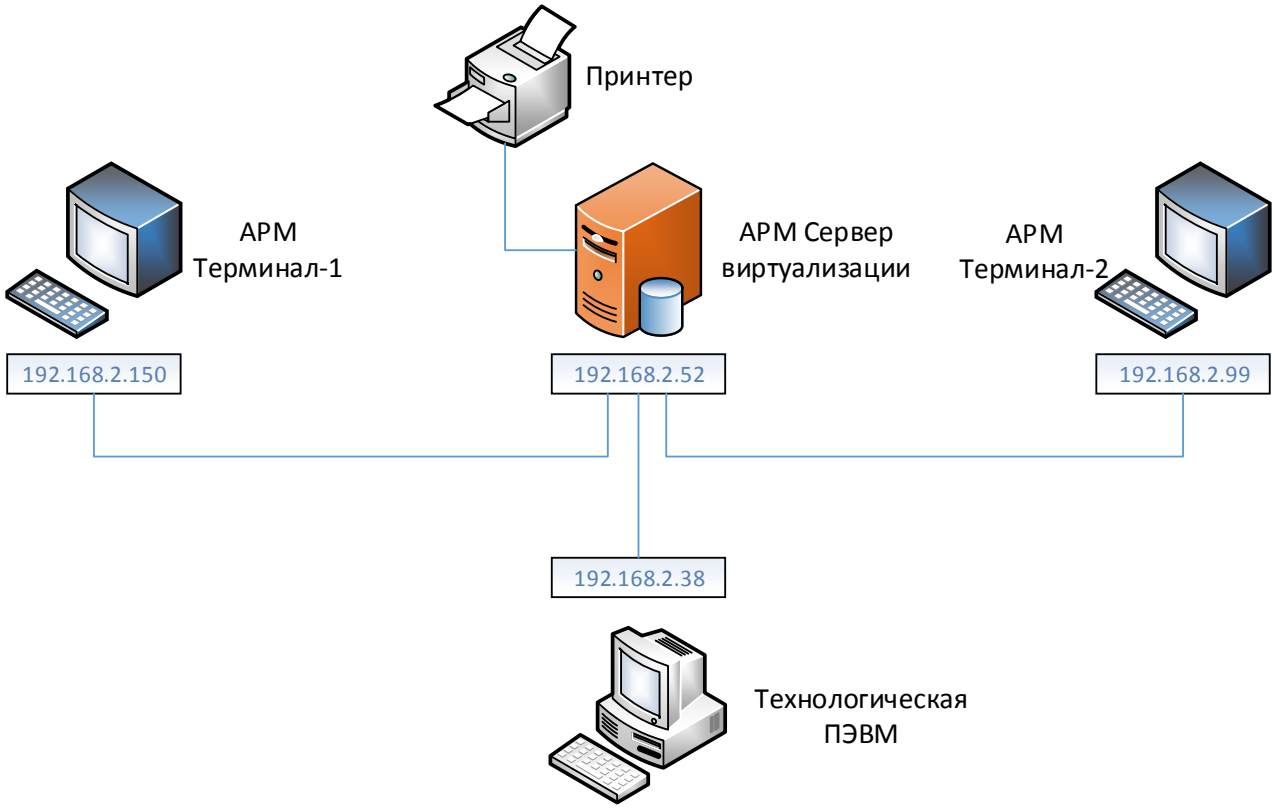


Рисунок 1 – Схема испытательного стенда

Конфигурация испытательного стенда приведена в таблице 1.

Таблица 1 – Конфигурация испытательного стенда

Обозначение	Аппаратная конфигурация	Программная конфигурация
АРМ-Терминал-1	Процессор Intel Celeron CPU G1820 2.7 ГГц; ОЗУ 4096 Мб; Flash Drive 8 Gb; Системная плата ASUS H81M-K Версия BIOS 1002 x64 Дата создания 08/12/2014 Версия ME FW 9.0.30.1482 Intel PCH Rev ID 05/C2 Адрес сетевой карты - 192.168.2.150.	Файлы комплекса программ «Терминал-Сервер» RU.МБРЦ.501130.01-03 (устанавливаются на ПЭВМ, выполняющую функции терминала). Формуляр МБРЦ.468313.002 ФО, Приложение А, Таблица А.1, Модуль 1.

Обозначение	Аппаратная конфигурация	Программная конфигурация
АРМ-Терминал-2	Процессор Intel Celeron CPU 1017U 1.6 ГГц; ОЗУ 4096 Мб; 8 Gb Flash Drive; Адрес сетевой карты - 192.168.2.99.	Файлы комплекса программ «Терминал-Сервер» RU.МБРЦ.501130.01-03 (устанавливаются на ПЭВМ, выполняющую функции терминала). Формуляр МБРЦ.468313.002 ФО, Приложение А, Таблица А.1, Модуль 1.
АРМ-Сервер виртуализации	Процессор: Intel Core i3-3220 3,3 ГГц; ОЗУ 4096 Мб; 8 Gb Flash Drive; 40Gb SSD; 1000 Gb HDD; Системная плата - ASUS P8B-C/4L; Адрес сетевой карты - 192.168.2.52.	Файлы комплекса программ «Терминал-Сервер» RU.МБРЦ.501130.01-03 (устанавливаются на ПЭВМ, выполняющую функции сервера). Формуляр МБРЦ.468313.002 ФО, Приложение А, Таблица А.2, Модуль 2.
Технологическая ПЭВМ	Процессор: Intel Core i5-7500 3,4 ГГц; ОЗУ 16 Gb; Тип системы: 64-разрядная ОС Адрес сетевой карты - 192.168.2.38.	Windows 7 (SP1) с установленным программным обеспечением “ФИКС 2.0.2”

2.2 Предварительная настройка испытательного стенда

Перед началом тестирования необходимо произвести следующие предварительные настройки *сервера виртуализации*:

- настроить параметры BIOS согласно таблице 2;

Таблица 2 – Настройки BIOS

Обозначение	Конфигурация
АРМ-Терминал-1	Подменю «Загрузка»: Сообщения Option ROM – Отображать; Перехват 19 прерывания – Отключено; CSM (Compability Support Module): Запуск CSM - Включено; Параметры загрузочных устройств - Только Legacy; Загрузка с сетевых устройств - Сначала Legacy; Загрузка с устройств хранения - Сначала Legacy; Загрузка с устройтв PCI-E/PCI - Сначала Legacy.
АРМ-Терминал-2	Настройки BIOS: Startup->Boot Mode - Legacy only; Настройки BIOS по умолчанию.

Обозначение	Конфигурация
АРМ-Сервер виртуализации	Подменю Boot: Option ROM Messages - Force BIOS; INT19 Trap Response – Immediate; CSM Parameters: Launch CSM – Always; Остальные параметры - Legacy Only; Other PCI device ROM priority – LegacyOpROM.

– произвести настройки *сервера виртуализации* согласно руководству администратора МБРЦ.468313.002 Д2 (п. 2.4);

– настроить правила регистрации событий, согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.14);

– произвести настройки *терминалов* на подключение к *серверу виртуализации* согласно руководству администратора МБРЦ.468313.002 Д2 (п. 4.1.2);

– на *сервере виртуализации* создать пользователей **user1, user2** согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.4);

– на *сервере виртуализации* создать ВМ с именем **vmtest1** (с ОС Astra Linux 1.5), **vmtest2** (с ОС Windows 7) согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.6);

– зарегистрировать пользователей на ВМ согласно таблице доступа (таблица 3) как описано в руководстве администратора МБРЦ.468313.002 Д2 (п. 3.7.1);

Таблица 3 – Доступ пользователей к ВМ

	vmtest1	vmtest2
user1	+	-
user2	-	+

– подключить к созданным ВМ хранилище SAMBA (руководство администратора МБРЦ.468313.002 Д2 (п. 2.12));

– подключить принтер к *серверу виртуализации* и настроить сервер печати (руководство администратора МБРЦ.468313.002 Д2 (п. 3.11));

– очистить журнал регистрации событий согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.14.2).

3 ПРОВЕРКА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Цель тестирования – проверка выполнения изделием функции идентификации и аутентификации пользователя.

Процедура тестирования 1:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. На *терминале* установить индивидуальный USB-носитель в разъем USB-порта и включить *терминал* кнопкой включения питания (**Power**).
3. После появления окна аутентификации изделия ввести произвольное имя пользователя с произвольным паролем и нажать клавишу **Enter**.

Процедура тестирования 2:

1. Включить *терминал* кнопкой **Power**.
2. После появления окна аутентификации изделия ввести имя пользователя **user1** с неверным паролем и нажать кнопку **Yes**.

Процедура тестирования 3:

1. Включить *терминал* кнопкой **Power**.
2. После появления окна аутентификации изделия необходимо ввести имя пользователя **user1**, верный пароль и нажать кнопку **Yes**.
3. Для перехода к загрузке ПО КП “Терминал-Сервер” необходимо выбрать виртуальную машину (ВМ) из списка доступных пользователю и нажать кнопку **Запустить**.
4. После смены состояния ВМ на “Работает” (ВМ запустится на *сервере виртуализации*) нажать кнопку **Подключить** и дождаться загрузки среды ВМ (вид рабочего стола пользователя показан в руководстве по эксплуатации МБРЦ.468313.002 РЭ).

Процедура тестирования 4:

1. Включить *сервер виртуализации* кнопкой **Power**.
2. В окне аутентификации ввести имя пользователя **user1**, пароль и нажать кнопку **Yes**.

Процедура тестирования 5:

1. Включить *сервер виртуализации* кнопкой **Power**.

2. В окне аутентификации выбрать пользователя **vss**, ввести пароль и нажать клавишу **Enter**.

Ожидаемый результат 1: невозможно войти в систему, вводя неверные данные пользователя.

Ожидаемый результат 2: невозможно войти в систему, вводя неверный пароль.

Ожидаемый результат 3: успешная авторизация пользователя.

Ожидаемый результат 4: невозможно войти на *сервер виртуализации* с именем и паролем пользователя.

Ожидаемый результат 5: успешная авторизация администратора.

Фактический результат 1: неуспешная авторизация пользователя и вывод сообщения об ошибке (рисунок 2).

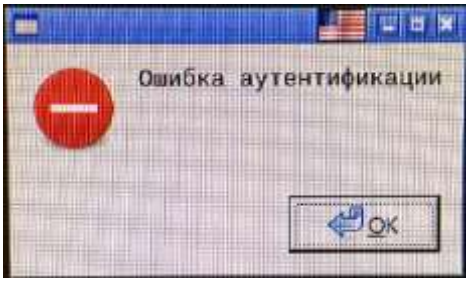


Рисунок 2 – Сообщение об ошибке

Фактический результат 2: неуспешная авторизация пользователя и вывод сообщения об ошибке (рисунок 2).

Фактический результат 3: успешная авторизация пользователя и загрузка рабочего стола КП “Терминал-Сервер”.

Фактический результат 4: неуспешная авторизация пользователя и повторный вывод окна аутентификации (рисунок 3).

Рисунок 3 – Окно аутентификации

Фактический результат 5: успешная авторизация администратора и загрузка рабочего стола ПИ “Горизонт-ВС” (рисунок 4).

Рисунок 4

Изделие считают выдержавшим проверку выполнения функции идентификации и аутентификации, если ПИ “Горизонт-ВС”:

- загружается в случае соответствия существующих учетных данных зарегистрированного пользователя введенным данным;
- не загружается в случае несоответствия существующих учетных данных зарегистрированного пользователя введенным данным.

4 ПРОВЕРКА ДИСКРЕЦИОННОГО ПРИНЦИПА КОНТРОЛЯ ДОСТУПА

Цель тестирования – проверка реализации в изделии механизма дискреционного разграничения доступа.

Процедура тестирования 1:

1. На *сервере виртуализации* установить для ВМ **vmtest1**, **vmtest2** одинаковые уровни доступа (Общедоступно – “ОД”) согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.7.1).
2. Зайти на *терминалы* под соответствующими учетными записями пользователей (таблица 3).
3. На общем хранилище SAMBA создать пользователем **user1** файл “example1.txt”, **user2** файл “example2.txt”.
4. На общем хранилище SAMBA совершить попытку чтения и изменения файлов для **user1** и **user2** согласно таблице 4.

Таблица 4 – Файлы пользователей

	“example1.txt”	“example2.txt”
user1	+	-
user2	-	+
администратор безопасности	+	+

***Примечание**: у администратора безопасности уровень допуска к сведениям, составляющим государственную тайну, вплоть до «совершенно секретно».*

Процедура тестирования 2:

1. На *сервере виртуализации* изменить права доступа к файлу “example1.txt” командой в консоли (разрешение чтения и запрет на изменение):

 # chmod 640 /srv/samba/example1.txt

2. В общем хранилище SAMBA пользователем **user2** совершить попытку чтения и изменения файла “example1.txt”.

Процедура тестирования 3:

1. Совершить попытку доступа к *серверу виртуализации* пользователем **user2** с целью полного доступа к хранилищу SAMBA.

Процедура тестирования 4:

1. Совершить попытку доступа к *терминалу* пользователем **vss** (администратором).

Процедура тестирования 5:

1. Зайти на *сервер виртуализации* с учетной записью администратора **vss**;
2. Перейти на общее хранилище SAMBA, находящееся в директории /srv/samba;
3. Совершить попытку чтения и изменения файлов “example1.txt” и “example2.txt”.

Ожидаемый результат 1: доступ к файлам “example1.txt”, “example2.txt”, предоставлен в соответствии с таблицей 4.

Ожидаемый результат 2: успешная попытка чтения и запрет на изменение файла “example1.txt”.

Ожидаемый результат 3: неуспешная попытка доступа.

Ожидаемый результат 4: неуспешная попытка доступа.

Ожидаемый результат 5: успешный доступ к файлам “example1.txt”, “example2.txt”.

Фактический результат 1:

1. Попытка доступа **user1** к файлу “example1.txt”, user2 к файлу “example2.txt” успешна.
2. Попытка доступа user1 к файлу “example2.txt”, **user2** к файлу “example1.txt” неуспешна – выдано сообщение об ошибке (рисунок 5).

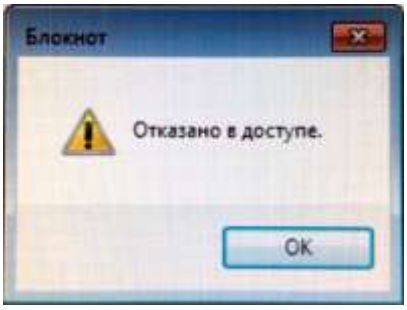


Рисунок 5

Фактический результат 2:

1. Попытка чтения файла “example1.txt” успешна (рисунок 6).

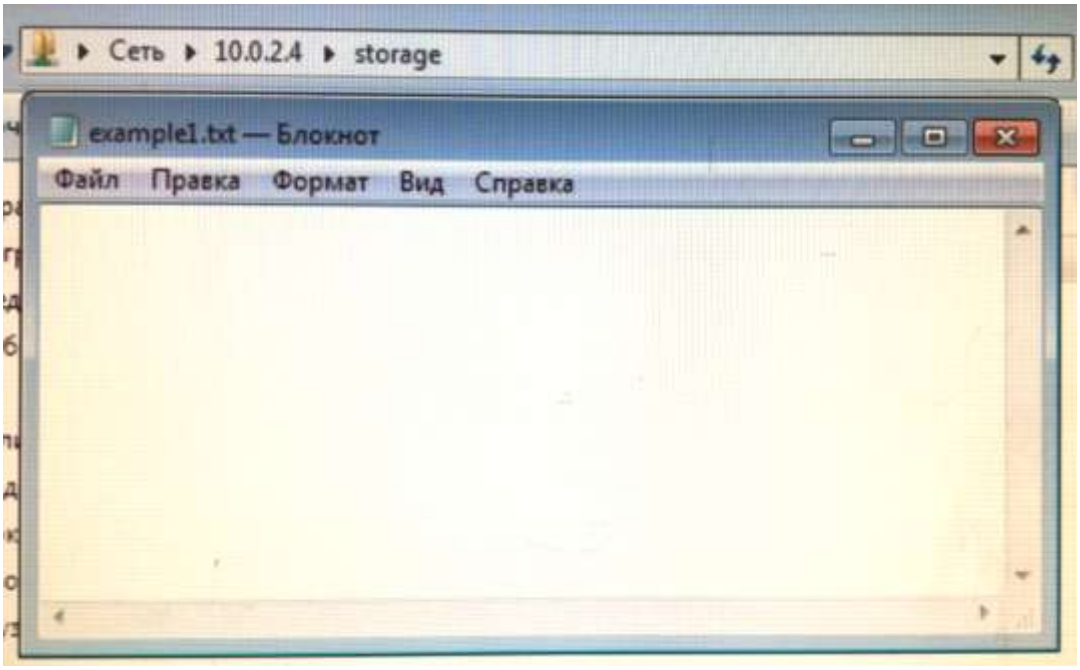


Рисунок 6

2. Попытка изменения файла “example1.txt” неуспешна – выдано сообщение об ошибке (рисунок 7).

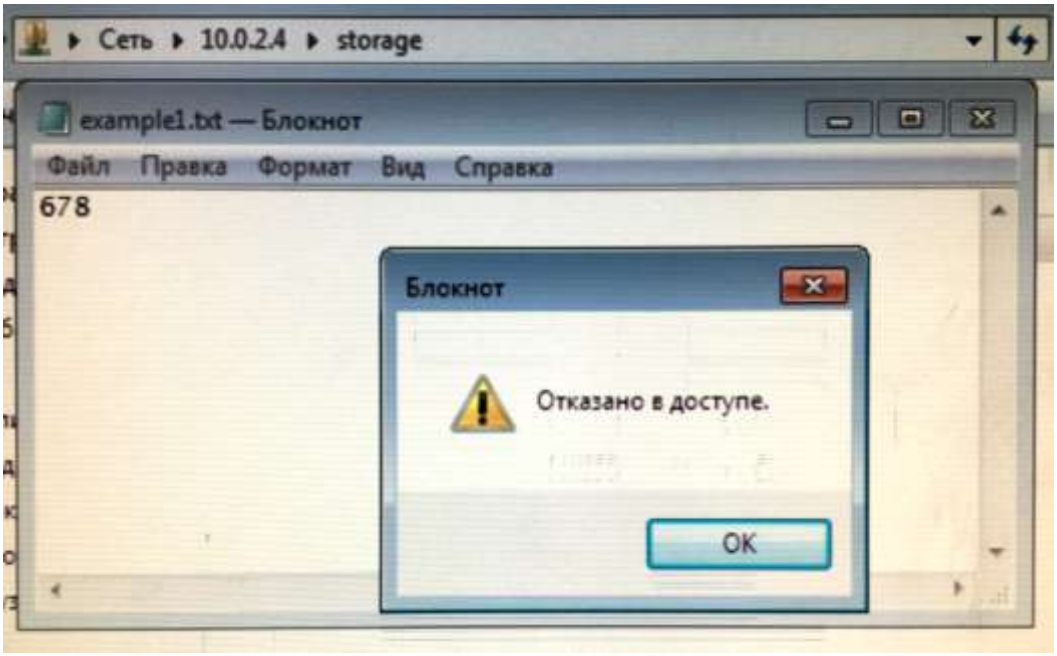


Рисунок 7

Фактический результат 3: неуспешная попытка доступа пользователем **user2** к *серверу виртуализации* (рисунок 8).

Рисунок 8

Фактический результат 4: неуспешная попытка доступа администратора **vss** к *терминалу* (рисунок 9).

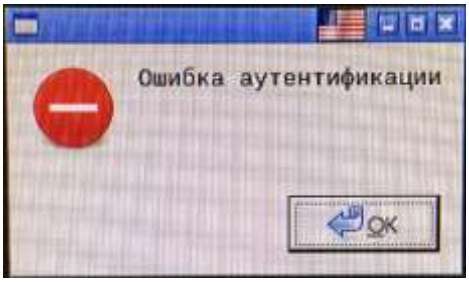


Рисунок 9

Фактический результат 5: успешная попытка доступа администратора к файлам “example1.txt”, “example2.txt” (рисунок 10).

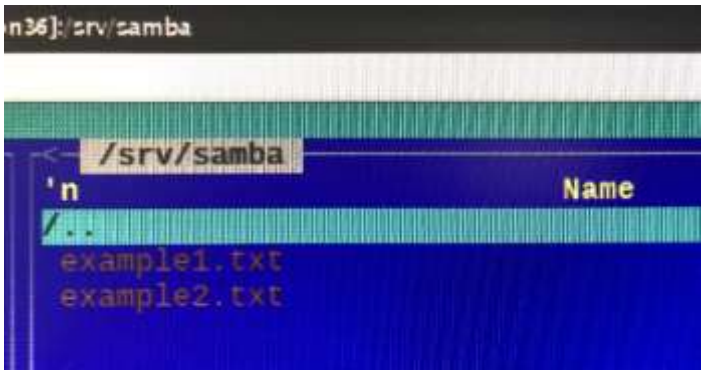


Рисунок 10

5 ПРОВЕРКА МАНДАТНОГО ПРИНЦИПА КОНТРОЛЯ ДОСТУПА

Цель тестирования – проверка реализации в изделии механизма мандатного разграничения доступа к объектам файловой системы (ФС), включая создание файлов с мандатной меткой, чтение файлов с установленным мандатным уровнем, запись в файлы с установленным мандатным уровнем, запись и чтение файлов с установленной мандатной категорией.

***Примечание**: перед проведением данной проверки необходимо произвести проверку дискреционного принципа контроля доступа (п. 4).*

Процедура тестирования 1:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. На *сервере виртуализации* установить для ВМ **vmtest1** уровень доступа “Д1”, **vmtest2** уровень доступа “Д2” согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.7.1).
3. Зайти на *терминалы* под соответствующими учетными записями пользователей (таблица 4).
4. На общем хранилище SAMBA создать пользователем **user1** файл “example3.txt”, **user2** файл “example4.txt”.
5. Разрешить все виды доступа для файлов “example3.txt”, “example4.txt” командами в консоли *сервера виртуализации*:

```
# chmod 777 /srv/samba/example3.txt
# chmod 777 /srv/samba/example4.txt
```

6. На общем хранилище SAMBA совершить попытку доступа к файлам согласно таблице 5.

Таблица 5 – Файлы пользователей

	“example3.txt”	“example4.txt”
user1 (“Д1”)	+	-
user2 (“Д2”)	+	+

Процедура тестирования 2:

1. Выключить ВМ на *терминалах*.
2. Для **vmtest1** установить уровень доступа “Д4”, запустить ВМ на *терминале*.

3. На общем хранилище SAMBA с ВМ **vmtest1** совершить попытку доступа к файлам “example3.txt”, “example4.txt”.

Процедура тестирования 3:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. Разрешить только доступ на чтение для файла “example3.txt” командой в консоли *сервера виртуализации*:

 # *chmod 444 /srv/samba/example3.txt*

3. Зайти на *терминал* под учетной записью пользователя **user2**;
4. На общем хранилище SAMBA совершить попытку редактирования файла “example3.txt”.

Процедура тестирования 4:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. На *сервере виртуализации* установить для ВМ **vmtest1** уровень доступа “Д3” согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.7.1).
3. На общем хранилище SAMBA с ВМ **vmtest1** совершить попытку доступа к файлам “example3.txt”, “example4.txt”.

Процедура тестирования 5:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. На *сервере виртуализации* установить для ВМ **vmtest1** уровень доступа “ОД” согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.7.1).
3. На общем хранилище SAMBA с ВМ **vmtest1** совершить попытку доступа к файлам “example3.txt”, “example4.txt”.

Процедура тестирования 6:

1. Зайти *на сервер виртуализации* с учетной записью администратора;
2. Перейти на общее хранилище SAMBA, находящееся в директории /srv/samba;
3. Совершить попытку чтения и изменения файлов “example3.txt” и “example4.txt”.

Ожидаемый результат 1: доступ к файлам предоставлен в соответствии с таблицей 5.

Ожидаемый результат 2: успешная попытка доступа к файлам “example3.txt”, “example4.txt”.

Ожидаемый результат 3: успешная попытка чтения и запрет на изменение файла “example3.txt”.

Ожидаемый результат 4: успешная попытка доступа к файлам “example3.txt”, “example4.txt”.

Ожидаемый результат 5: успешная попытка доступа к файлам “example3.txt”, “example4.txt”.

Ожидаемый результат 6: успешная попытка доступа к файлам “example3.txt”, “example4.txt”.

Фактический результат 1:

1. Попытка доступа **user1** к файлу “example3.txt” успешна, файл “example4.txt” не виден на хранилище (рисунок 11).

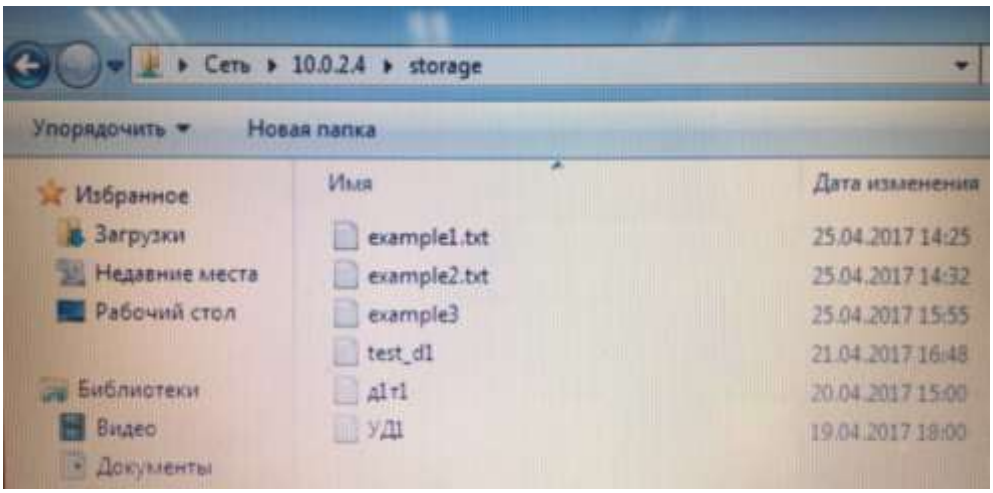


Рисунок 11

2. Попытка доступа **user2** к файлам “example3.txt”, “example4.txt” успешна (рисунок 12).

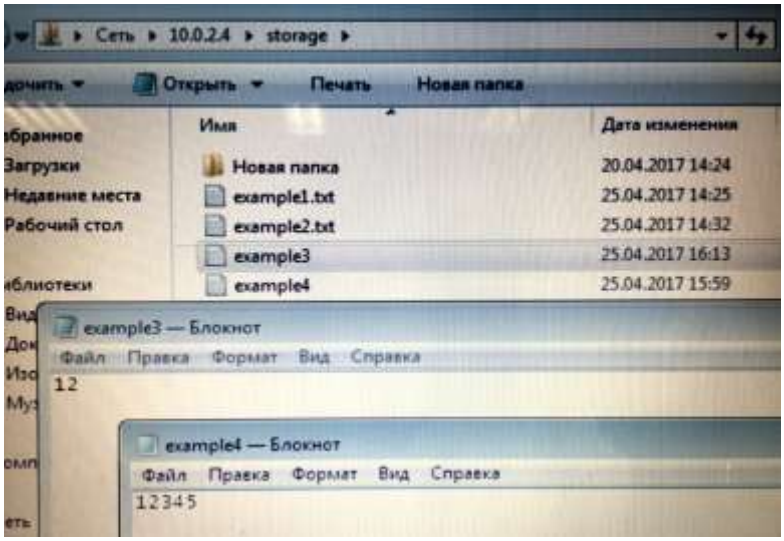


Рисунок 12

Фактический результат 2: попытка доступа **user1** к файлам “example3.txt”, “example4.txt” успешна (рисунок 12).

Фактический результат 3: попытка изменения файла “example3.txt” неуспешна – выдано сообщение об ошибке (рисунок 13).

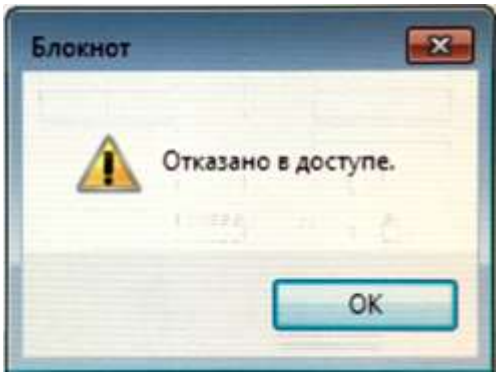


Рисунок 13

Фактический результат 4: попытка доступа **user1** к файлам “example3.txt”, “example4.txt” успешна (рисунок 14).

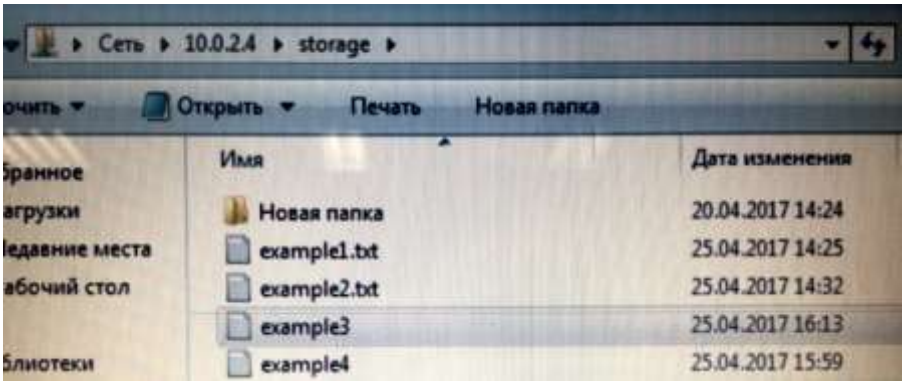


Рисунок 14

Фактический результат 5: попытка доступа **user1** к файлам “example3.txt”, “example4.txt” неуспешна, файлы не видны на хранилище (рисунок 15).

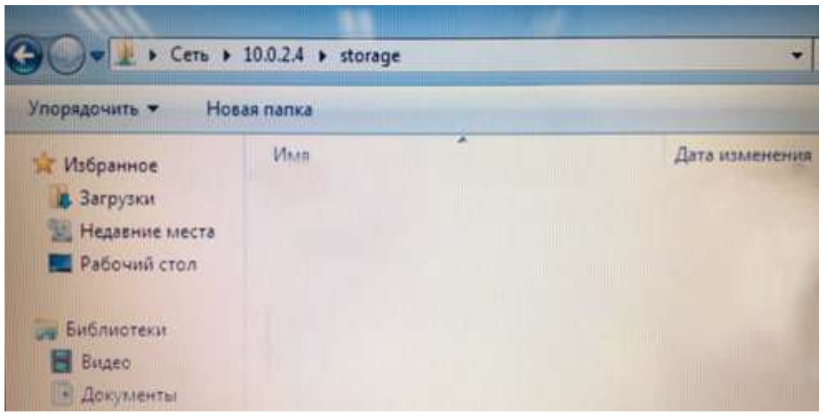


Рисунок 15

Фактический результат 6: попытка доступа **user1** к файлам “example3.txt”, “example4.txt” успешна (рисунок 16).

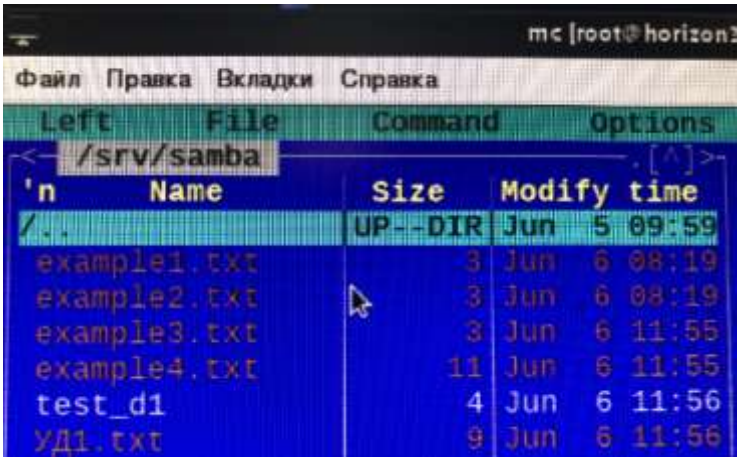


Рисунок 16

6 ПРОВЕРКА ОЧИСТКИ ПАМЯТИ

Цель тестирования – проверка выполнения изделием функции очистки внешней и оперативной памяти.

Процедура тестирования 1:

1. Зайти на *терминал* под учетной записью пользователя **user1**.
2. На хранилище SAMBA создать текстовые файлы “test_memory1” “test_memory2” диска, заполнив первый файл сигнатурой 456783216584, а второй – 789561231574.
3. К *серверу виртуализации* подключить USB-накопитель, отформатированный в файловую систему ext4 и скопировать на него файлы “test_memory1” и “test_memory2” из хранилища.
4. Удалить файл “test_memory1”, а из файла “test_memory2” удалить сигнатуру.
5. Установить USB-накопитель в технологическую ПЭВМ с установленным сертифицированным ПО, например, “Сканер-ВС”, и произвести поиск сигнатур.

Процедура тестирования 2:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. Запустить утилиту очистки оперативной памяти командой в консоли:

 # *clrmem*

Примечание: *Очистка оперативной памяти в ПИ «Горизонт-ВС» реализована на основе опции M_PERTURB функции mallopt. Данная функция вызывается в строке 3212 файла vl.c пакета QEMU. Это приводит к тому, что оперативная память перед каждым выделением (вызов malloc()) заполняется заданным байтом, а перед каждым освобождением (вызов free()) – заполняется его инвертированным значением.*

Очистка внешней памяти в ПИ «Горизонт-ВС» основана на снимках ВМ. После окончательной настройки гостевой ОС Администратор в программе virt-manager должен включить опцию «Fix VM». При этом средствами библиотеки libvirt происходит создание снимка ВМ с именем снимка «default». Далее, когда в программе start-spice пользователь нажимает кнопку «Запустить», в программе start-spice (файл start-spice.c, строка 1011) происходит поиск снимка с именем

«default» посредством функции virDomainSnapshotLookupByName. Если данный снимок был найден, происходит восстановление ВМ с использованием этого снимка. В этом случае все изменения, внесенные пользователем в предыдущем сеансе, перестают существовать.

Ожидаемый результат 1: после удаления сигнатуры на USB-накопителе не найдены.

Ожидаемый результат 2: после запуска утилиты оперативная память очистится.

Фактический результат 1: ни одной сигнатуры в созданном образе диска ВМ не найдено.

Фактический результат 2: оперативная память очистилась (рисунок 17).

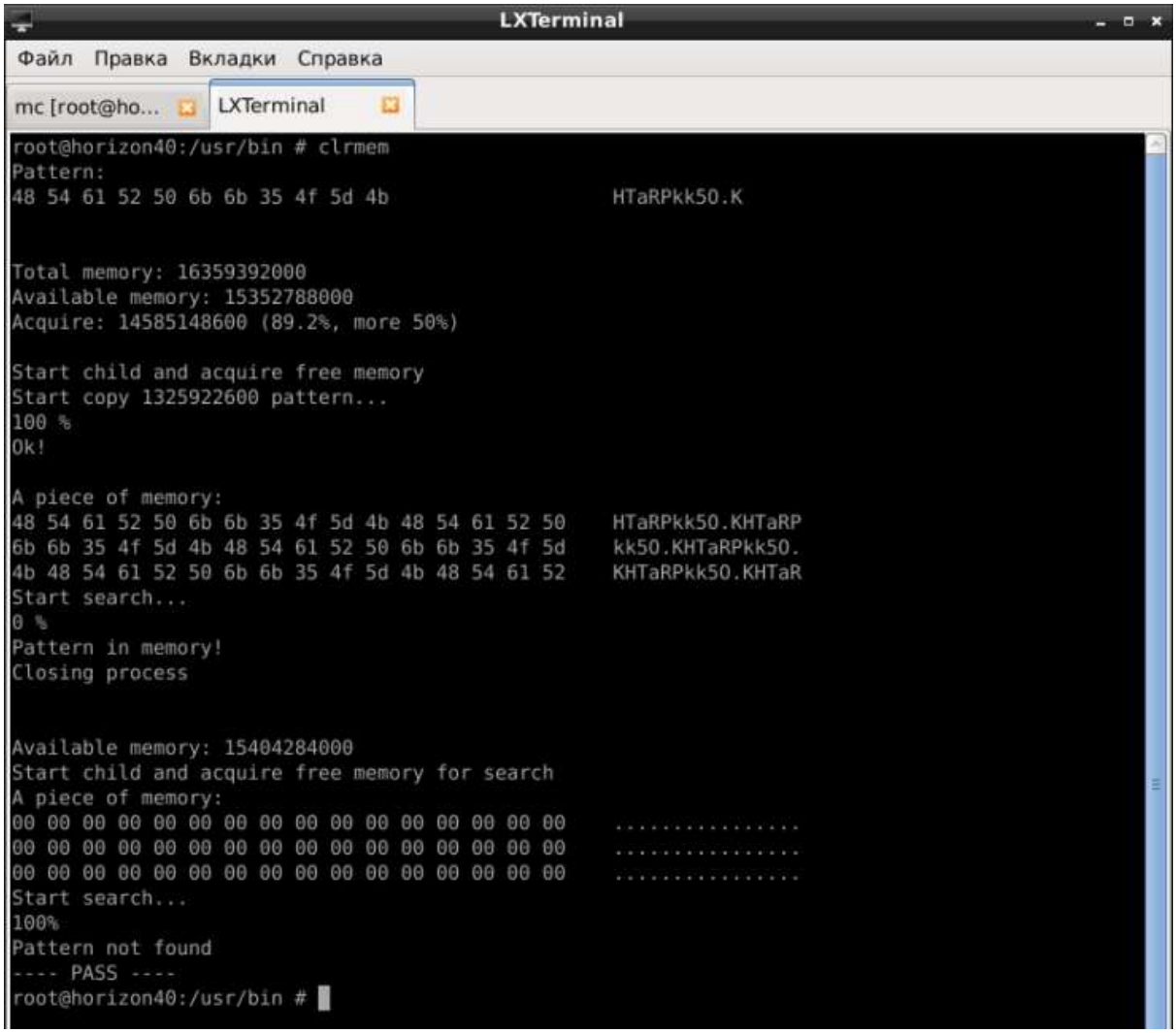


Рисунок 17

7 ПРОВЕРКА ИЗОЛЯЦИИ МОДУЛЕЙ

Цель тестирования – проверка наличия для каждого процесса в системе собственного изолированного адресного пространства.

Процедура тестирования:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. На *сервере виртуализации* создать пользователя **user3** и ВМ с именем **vmtest3** (с ОС Windows 7) согласно руководству администратора МБРЦ.468313.002 Д2.
3. Запустить 3, созданные ранее, ВМ.
4. Ввести команду:

 # ps ax | grep qemu

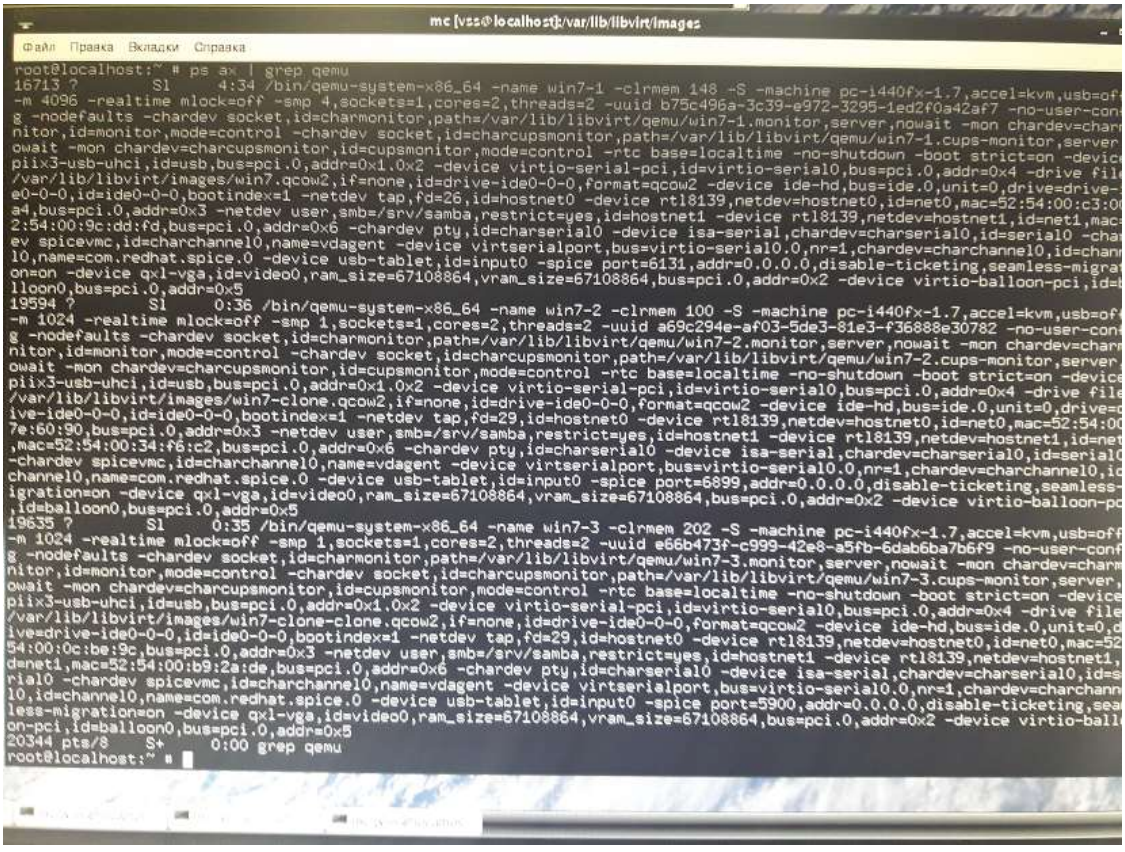


Рисунок 18

5. Ввести 3 команды, в соответствии с номерами процессов (рисунок 18):

 # cat /proc/16713/maps > 16713.txt
 # cat /proc/19594/maps > 19594.txt
 # cat /proc/19635/maps > 19635.txt

6. Сравнить адресные пространства процессов при помощи команды:

 # cat 16713.txt / grep qemu
 # cat 19594.txt / grep qemu
 # cat 19635.txt / grep qemu

Ожидаемый результат: адресные пространства процессов не должны пересекаться.

Фактический результат: адресные пространства процессов не пересекаются (рисунок 19).

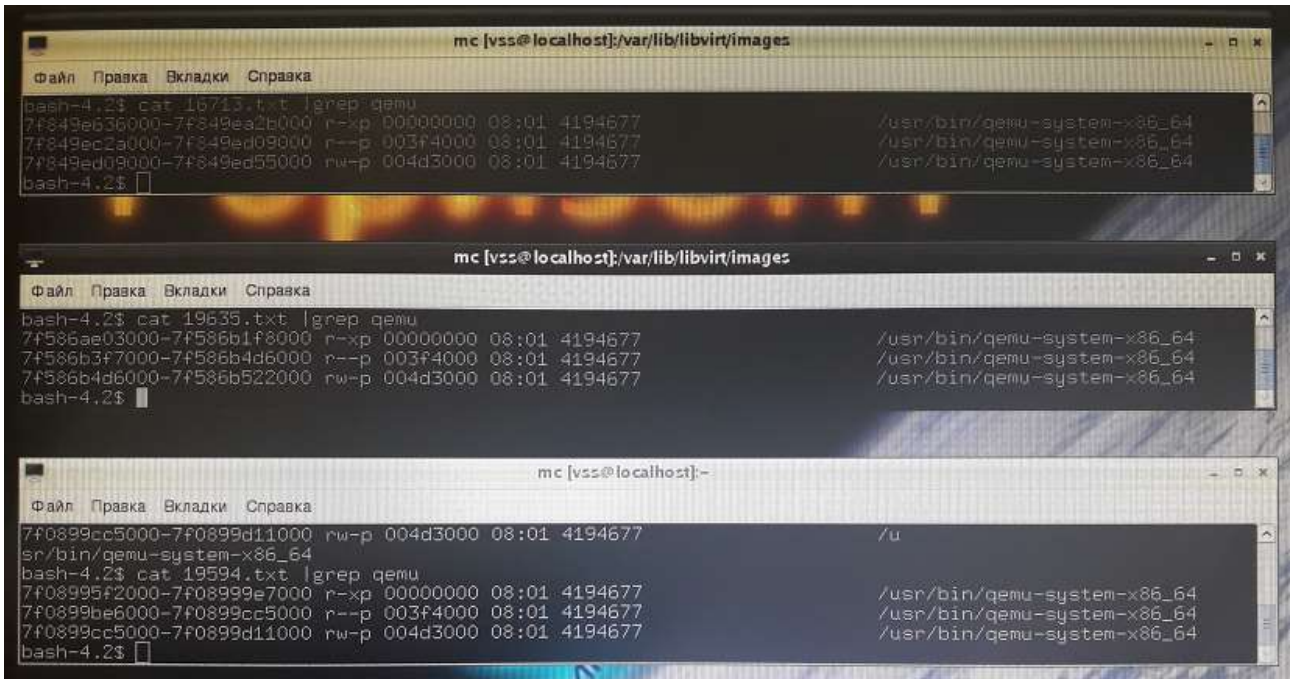


Рисунок 19

8 ПРОВЕРКА МАРКИРОВКИ ДОКУМЕНТОВ

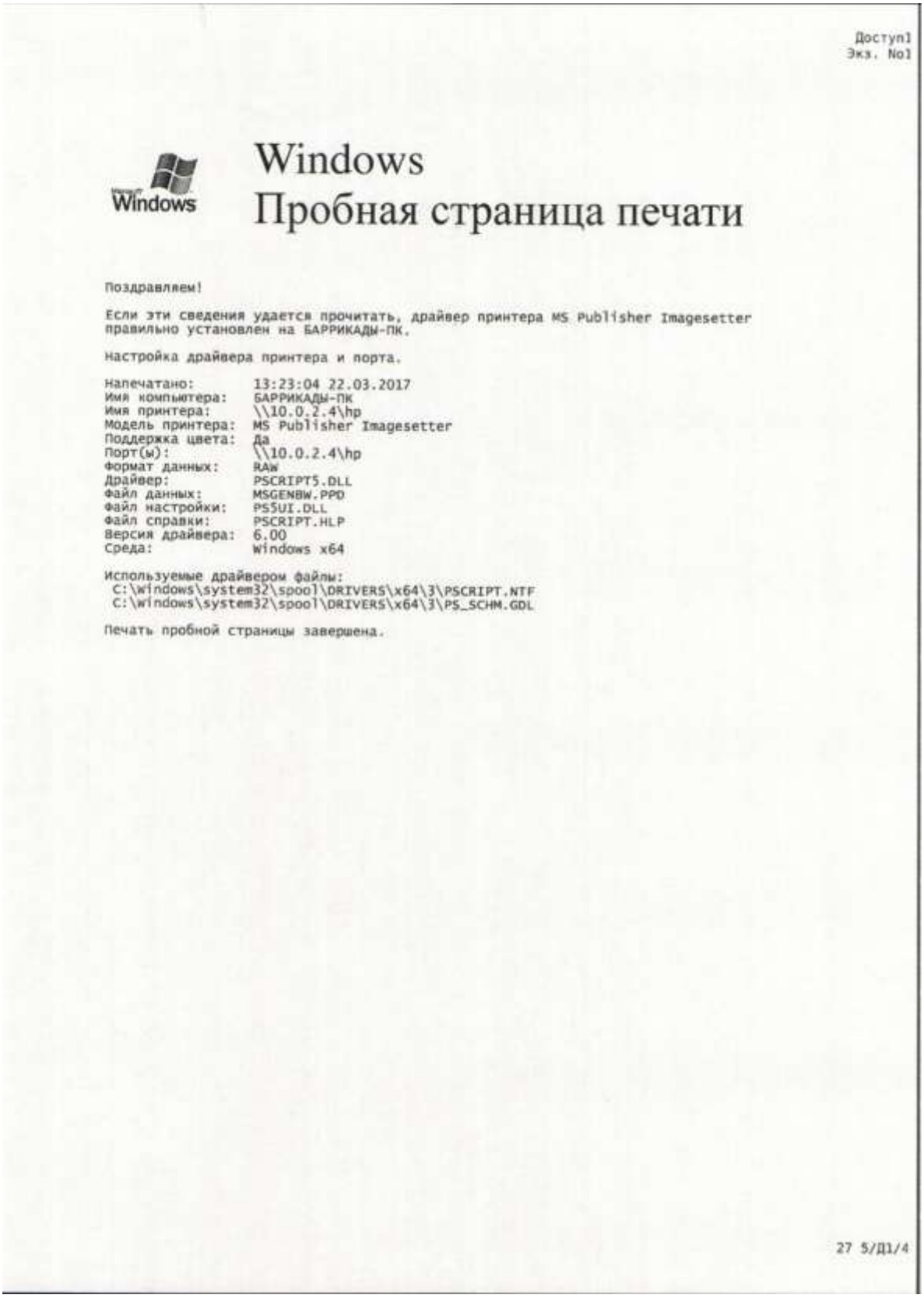
Цель тестирования – проверка выполнения изделием функции маркировки документов.

Процедура тестирования:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. Настроить сервер печати и принтер для печати документов с мандатными атрибутами согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.11).
3. Выполнить вход на *терминале* пользователем **user1** на **vmtest1**.
4. Создать текстовый документ и отправить его на печать.

Ожидаемый результат: наличие маркировки листов документа, предусматривающей печать грифа документа, номера листа и учетного номера документа.

Фактический результат: на печать выведены страницы с соответствующими атрибутами (рисунки 20, 21).



Доступ1
Экз. No1

Windows

Windows
Пробная страница печати

Поздравляем!

Если эти сведения удается прочитать, драйвер принтера MS Publisher Imagesetter правильно установлен на БАРРИКАДЫ-ПК.

Настройка драйвера принтера и порта.

Напечатано:	13:23:04 22.03.2017
Имя компьютера:	БАРРИКАДЫ-ПК
Имя принтера:	\\10.0.2.4\hp
Модель принтера:	MS Publisher Imagesetter
Поддержка цвета:	Да
Порт(ы):	\\10.0.2.4\hp
Формат данных:	RAW
Драйвер:	PSCRIPT5.DLL
Файл данных:	MSGENBW.PPD
Файл настройки:	PS5UI.DLL
Файл справки:	PSCRIPT.HLP
Версия драйвера:	6.00
Среда:	Windows x64

Используемые драйвером файлы:
C:\windows\system32\spool\DRIVERS\x64\3\PSCRIPT.NTF
C:\windows\system32\spool\DRIVERS\x64\3\PS_SCHM.GDL

Печать пробной страницы завершена.

27 5/Д1/4

Рисунок 20

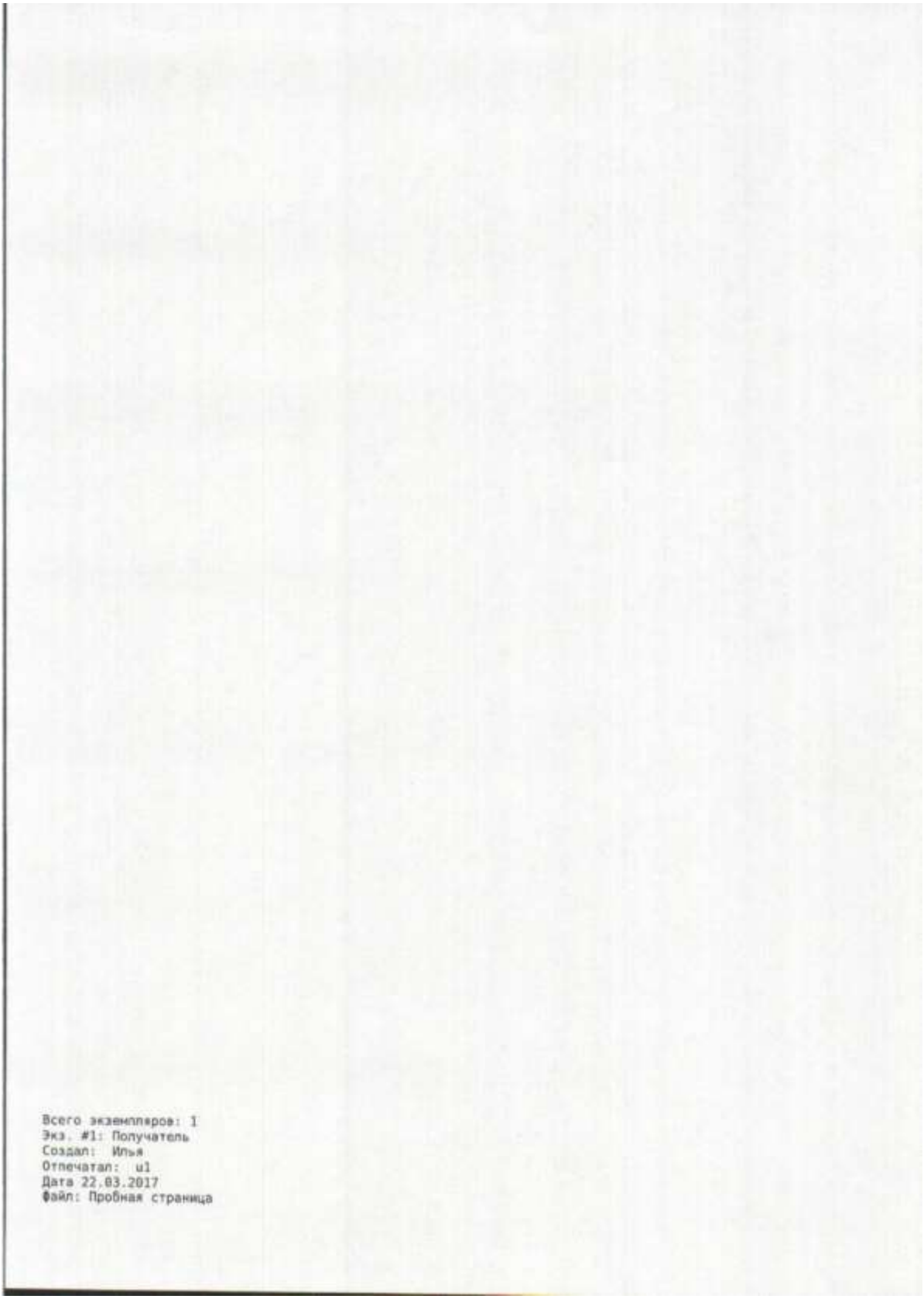

Всего экземпляров: 1
Экз. #1: Получатель
Создал: Илья
Отпечатал: u1
Дата 22.03.2017
Файл: Пробная страница

Рисунок 21

9 ПРОВЕРКА ЗАЩИТЫ ВВОДА-ВЫВОДА ИНФОРМАЦИИ НА ОТЧУЖДАЕМЫЙ ФИЗИЧЕСКИЙ НОСИТЕЛЬ И СОПОСТАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ С УСТРОЙСТВОМ

Цель тестирования – проверка выполнения изделием функций защиты ввода-вывода информации на отчуждаемый физический носитель и сопоставления пользователя с устройством.

Процедура тестирования 1:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. В “Менеджере виртуальных машин” для **vmtest1** зарегистрировать USB-носитель согласно руководству администратора МБРЦ.468313.002 Д2 (п. 3.7.11).

***Примечание**. перед регистрацией USB-носитель отформатировать.*

3. Выполнить вход на *терминале* пользователем **user1** на **vmtest1**.
4. Установить зарегистрированный USB-носитель в свободный разъем *терминала*.
5. Подключить USB-носитель так, как это описано в руководстве по эксплуатации МБРЦ.468313.002 РЭ.
6. Открыть USB-носитель с помощью программы “Проводник” и убедиться, что на нем можно создать файл, например, “example.txt“.

Процедура тестирования 2:

1. Установить незарегистрированный USB-носитель в свободный разъем *терминала*.

Процедура тестирования 3:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. Настроить сервер печати и принтер для печати документов с согласно руководству администратора МБРЦ.468313.002 Д2 (п.3.11).
3. Подключить принтер в **vmtest1** так, как это описано в руководстве администратора МБРЦ.468313.002 Д2 (п. 4.2).
4. Выполнить вход на *терминале* пользователем **user1** на **vmtest1**.
5. Создать текстовый документ и отправить его на печать.

Процедура тестирования 4:

1. Подключить к *серверу виртуализации* видеокарту в свободный PCI-разъем на материнской плате.

2. Зайти на *сервер виртуализации* с учетной записью администратора.

3. Зайти в меню Приложения → Системные → Менеджер виртуальных машин.

4. Кликнуть два раза левой клавишей “мыши” по иконке **vmtest1**, в открывшемся окне нажать кнопку **Показать параметры виртуального оборудования**.

5. В окне параметров виртуального оборудования ВМ нажать кнопку **Добавить оборудование** и в левой части окна добавления нового виртуального устройства необходимо выбрать **PCI устройство хоста**.

6. В окне параметров необходимо выбрать модель устройства для подключения к ВМ и нажать кнопку **Завершить**.

Ожидаемый результат 1: успешный доступ к USB-носителю и создание файла “example.txt“.

Ожидаемый результат 2: убедиться в невозможности доступа к носителю.

Ожидаемый результат 3: успешное подключение принтера и доступность печати.

Ожидаемый результат 4: успешное подключение физической видеокарты к ВМ.

Фактический результат 1: создание файла “example.txt“.

Фактический результат 2: невозможность доступа к носителю.

Фактический результат 3: на печать выведены страницы с соответствующими атрибутами (рисунки 20, 21).

Фактический результат 4: видеокарта была подключена в ВМ и в диспетчере устройств гостевой ОС отобразился тип видеокарты (рисунок 22).

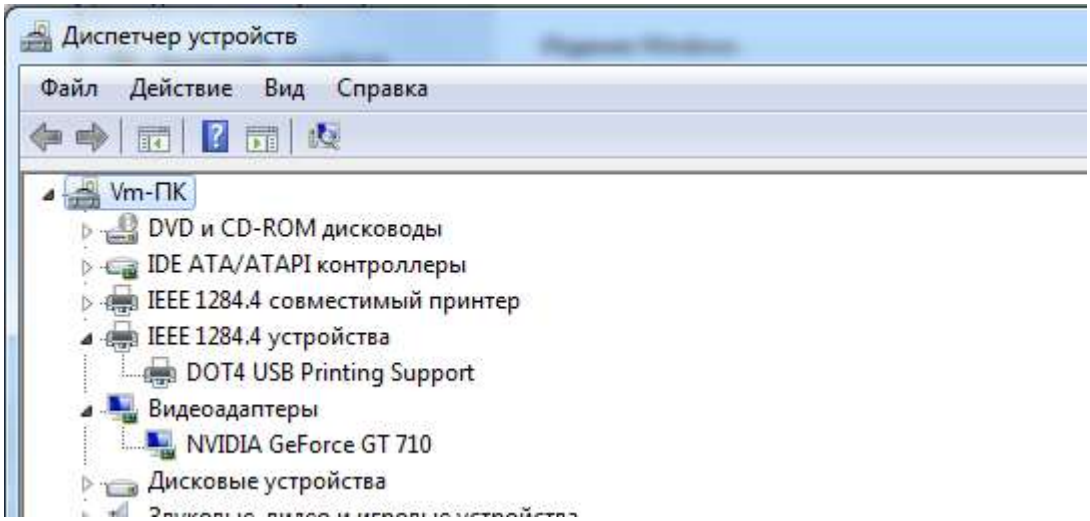


Рисунок 22

Изделие считают выдержавшим проверку тестирования ввода и вывода информации на отчуждаемый физический носитель, если успешен доступ к зарегистрированному USB-носителю и невозможен доступ к незарегистрированному USB-носителю, а также санкционированный пользователь надёжно сопоставляется выделенному устройству.

10 ПРОВЕРКА РЕГИСТРАЦИИ СОБЫТИЙ

Цель тестирования – проверка выполнения изделием функции генерации данных аудита.

***Примечание**: перед тестированием данного компонента необходимо выполнить проверку функций идентификации и аутентификации (п. 3), дискреционного и мандатного разграничения доступа (п.п. 4, 5).*

Процедура тестирования 1:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. Получить доступ к данным журнала аудита, находящемся в директории ***/var/log/messages*** путем набора в консоли команды

cat /var/log/messages | grep vmacd

Процедура тестирования 2:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. В консоли получить значение UID пользователя, используя команду:

***id** <имя пользователя в системе>*

3. Получить доступ к данным журнала аудита путем набора в консоли команды

ausearch –ua <**UID пользователя**> --interpret | grep CREATE

отображает все созданные файлы пользователем с заданным UID в контролируемых директориях.

ausearch –a <**номер события**> --interpret

отображает подробную информацию по выбранному событию:

- дата и время (msg=audit),
- название файла (name),
- пользователь (ouid) и группа (ogid),
- успешность выполнения (success=no/yes).

Процедура тестирования 3:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. Изменить правила разграничения доступа (ПРД) командой chown или chmod в консоли:

chown u1.vmusers /srv/samba/test

или ***chmod 777 /srv/samba/test***

3. Получить доступ к данным журнала аудита путем набора в консоли команды

ausearch -ua 0 --interpret | grep chown

ausearch -ua 0 --interpret | grep chmod

отображает изменение в ПРД.

Ожидаемый результат 1: в файле аудита представлены сведения об идентификации и аутентификации пользователей.

Ожидаемый результат 2: в файле аудита представлены сведения о работе пользователей с файлами.

Ожидаемый результат 3: в файле аудита представлены сведения об изменении ПРД.

Фактический результат 1: убедиться в наличии сообщений (рисунки 23, 24):

- успешная аутентификация – ***User <****имя пользователя****> request connect***;
- неуспешная аутентификация – ***SASL: performing SASL negotiation: authentication failure***;
- попытка аутентификации незарегистрированного пользователя – ***SASL: performing SASL negotiation: user not found***.

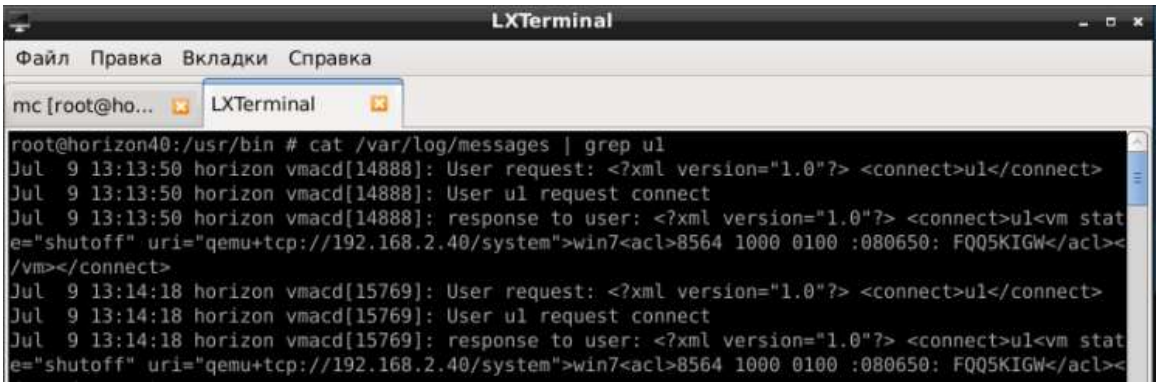


Рисунок 23

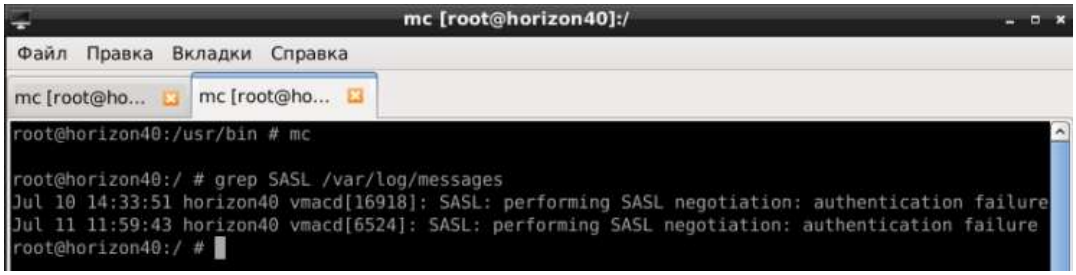


Рисунок 24

Фактический результат 2: убедиться в наличии сообщений (рисунок 25):

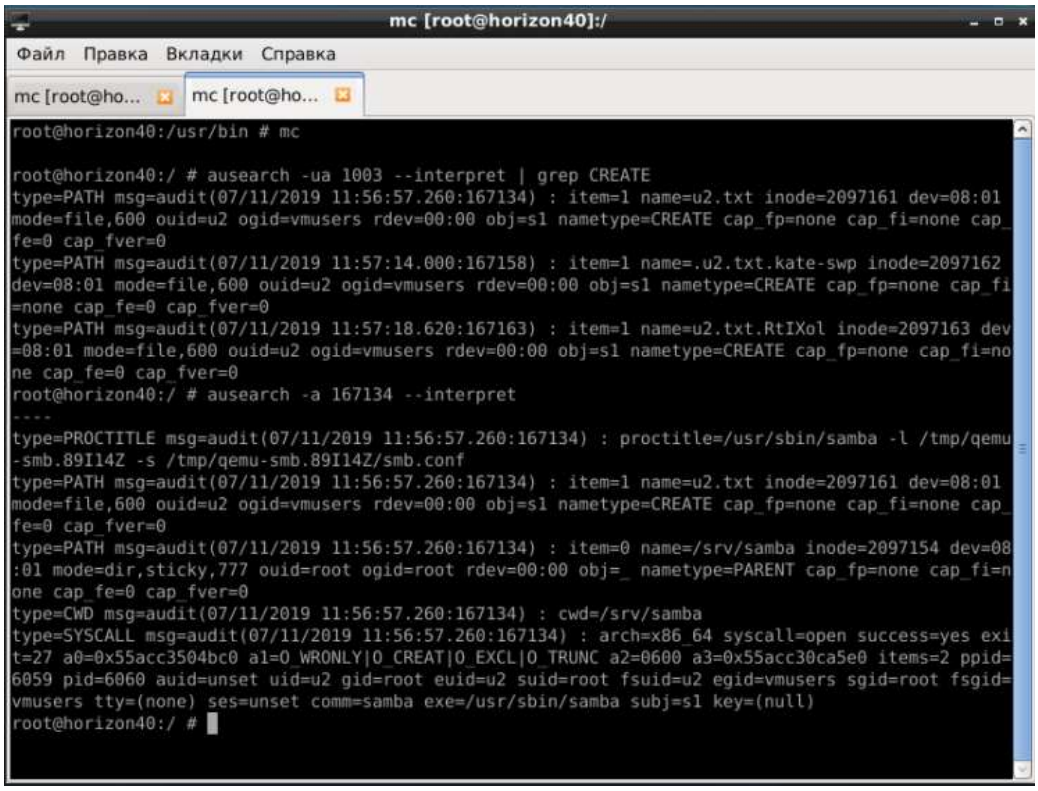


Рисунок 25

Фактический результат 3: убедиться в наличии сообщений (рисунок 26):

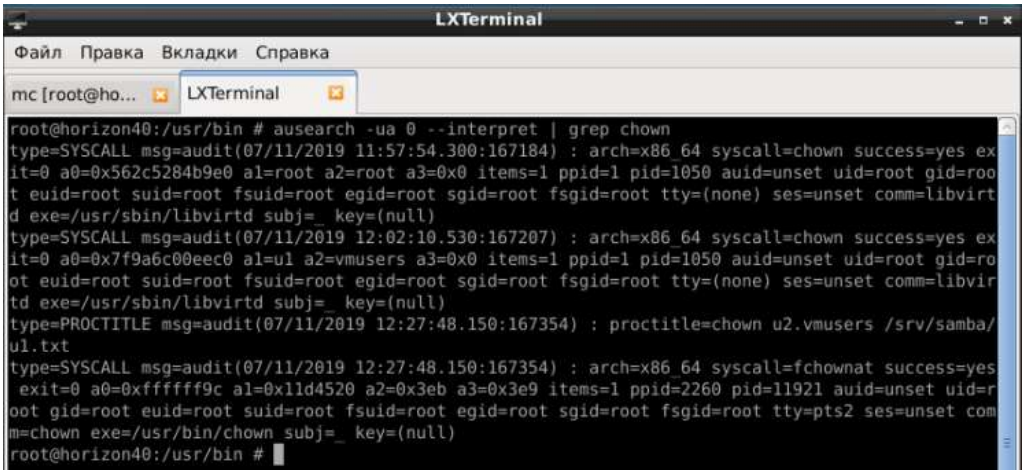


Рисунок 26

11 ПРОВЕРКА КОНТРОЛЯ ЦЕЛОСТНОСТИ КСЗ

Цель тестирования – проверка выполнения изделием функции контроля целостности.

Процедура тестирования 1:

1. На *технологической ПЭВМ* с установленным программным обеспечением “ФИКС 2.0.2” установить индивидуальный USB-носитель для *сервера виртуализации* и *терминала* в разъем USB-порта.
2. Произвести расчет контрольных сумм файлов на USB-носителе согласно процедуре, описанной в формуляре МБРЦ.468313.002 ФО (Приложение А).

Процедура тестирования 2:

3. На *сервере виртуализации* установить индивидуальный USB-носитель в разъем USB-порта и включить *сервер виртуализации* кнопкой включения питания (**Power**).

Процедура тестирования 3:

1. Зайти на *сервер виртуализации* с учетной записью администратора.
2. В консоли запустить файловый менеджер *Midnight Commander* командой **mc**.
3. Перейти в директорию ***/usr/bin*** и запустить приложение **Менеджер виртуальных машин** командой в консоли ***./virt-manager***.

Процедура тестирования 4:

1. В файловом менеджере *Midnight Commander* скопировать приложение ***virt-manager*** – в списке приложений появится ***virt-manager_new***.
2. В консоли попытаться запустить скопированное приложение командой ***./virt-manager_new***.

Процедура тестирования 5:

1. В файловом менеджере *Midnight Commander* открыть приложение ***virt-manager*** для редактирования и изменить его содержимое.
2. Перезапустить *сервер виртуализации*.

Ожидаемый результат 1: рассчитанные контрольные суммы неизменяемых файлов дистрибутива совпадают с указанными в формуляре на изделие.

Ожидаемый результат 2: сообщение об успешной проверке контроля целостности.

Ожидаемый результат 3: успешный запуск программы **Менеджер виртуальных машин**.

Ожидаемый результат 4: неуспешная попытка запуска скопированного приложения, так как при копировании не наследуются расширенные атрибуты файла, содержащие контрольную сумму.

Ожидаемый результат 5: сообщение об ошибке при подсчете контрольных сумм, переустановка неизменяемой части ПИ “Горизонт-ВС” с USB-носителя.

Фактический результат 1: рассчитанные контрольные суммы совпадают с указанными в формуляре (таблицы А.1, А.2).

Фактический результат 2: при загрузке показано сообщение “**verify checksum OK**”.

Фактический результат 3: запуск приложения **Менеджер виртуальных машин** (рисунок 27).

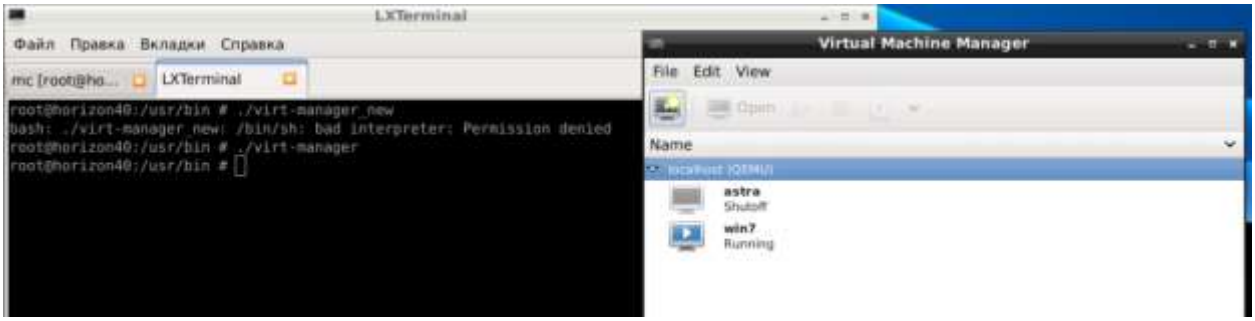


Рисунок 27

Фактический результат 4: неуспешная попытка запуска скопированного приложения – сообщение “Permission denied” (рисунок 28).

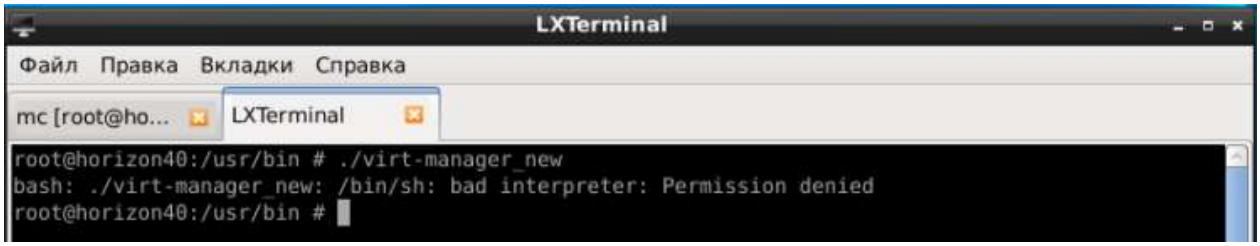


Рисунок 28

Фактический результат 5: на экран выдано сообщение об ошибке при подсчете контрольных сумм (рисунок 29).

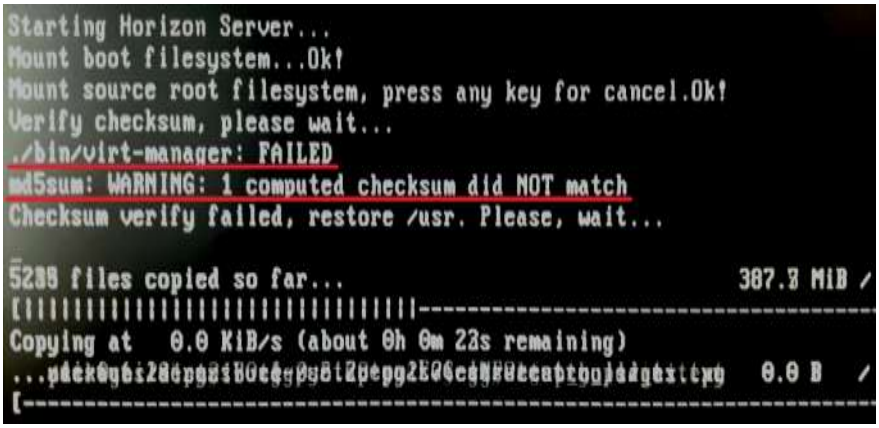


Рисунок 29

и произведена переустановка неизменяемой части ПИ “Горизонт-ВС” с USB-носителя (рисунок 30).

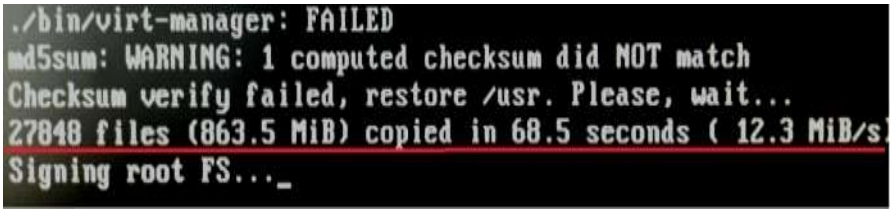


Рисунок 30

12 ПРОВЕРКА НАДЕЖНОГО ВОССТАНОВЛЕНИЯ

Цель тестирования – проверка выполнения изделием функции надежного восстановления.

Процедура тестирования:

1. Зайти на *сервер виртуализации* под учетной записью администратора.
2. Перейти в директорию ***/etc*** и удалить файл **installed**.
3. Перезагрузить *сервер виртуализации*.
4. Убедиться, что происходит копирование данных и переустановка ПИ “Горизонт-ВС” с USB-носителя.
5. После окончания установки ПИ “Горизонт-ВС” повторить проверки функций безопасности по п.п. 3-11 настоящего документа.

Ожидаемый результат: ПИ “Горизонт-ВС” переустановлено, и все функции безопасности работают.

Фактические результат: ПИ “Горизонт-ВС” переустановлено, ожидаемые результаты проверок по п.п. 3-11 данного функционального тестирования совпадают с фактическими.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

ВМ	- виртуальная машина
КП	- комплекс программ
КСЗ	- комплекс средств защиты
НСД	- несанкционированный доступ
ПИ	- программное изделие
ПО	- программное обеспечение
ПРД	- правила разграничения доступа
ПЭВМ	- персональная электронная вычислительная машина

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводи-тельного документа и дата	Подпись	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					