ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3»

Руководство администратора безопасности. Приложение 4

Санкт-Петербург, 2019

1 Регламентное тестирование СЗИ «Блокхост-Сеть 3»

Программа проведения регламентного тестирования для автономного варианта использования СЗИ «Блокхост-Сеть 3» (используемого локально) и для варианта с удаленным управлением идентична и приведена в таблице П4.1.

Просмотр событий аудита, содержащихся в журнале СЗИ «Блокхост-Сеть 3», осуществляется администратором безопасности с помощью:

- программы просмотра событий операционной системы – консоли MMC (просмотр событий аудита с помощью средств консоли MMC подробно рассмотрен в подразделе 8.1 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности»);
- консоли «Системы развертывания и аудита».

Таблица П4.1 – Программа проведения регламентного тестирования СЗИ «Блокхост-Сеть 3»

№ п/п	Наименование испытаний (проверок)	Пункт методики
1	**Проверка реализации прав разграничения доступа (ПРД)**	1.1
	Проверка дискреционного принципа контроля доступа	1.1.1
	Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа	1.1.1.1
	Проверка применимости контроля доступа к каждому объекту и субъекту (индивиду или группе равноправных индивидов)	1.1.1.2
	Проверка возможности санкционированного изменения ПРД, в том числе изменения списка пользователей СВТ и списка защищаемых объектов	1.1.1.3
	Проверка предоставления прав изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.)	1.1.1.4
	Проверка наличия механизма, претворяющего в жизнь дискреционные ПРД, как для явных, так и для скрытых действий пользователя	1.1.1.5
	Проверка контроля запуска программ и файлов	1.1.1.6
	Проверка контроля запуска по маске имени файла	1.1.1.7
	Проверка контроля запуска процессов по модели разрешенных процессов	1.1.1.8
	Проверка мандатного принципа контроля доступа	1.1.2
	Проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта	1.1.2.1
	Проверка запроса и получения классификационных меток при вводе новых данных в систему	1.1.2.2

№ п/п	Наименование испытаний (проверок)	Пункт методики
	Проверка реализации мандатного принципа контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов	1.1.2.3
	Проверка возможности изменения классификационных уровней субъектов и объектов специально выделенными субъектами при реализации мандатных ПРД	1.1.2.4
	Проверка реализации диспетчера доступа	1.1.2.5
	Проверка сетевого мандатного принципа разграничения доступа	1.1.2.6
	Проверка сетевого мандатного доступа без использования MS Active Directory	1.1.2.7
2	**Проверка очистки памяти**	1.2
	Проверка очистки внешней памяти	1.2.1
	Проверка очистки оперативной памяти	1.2.2
3	**Проверка маркировки документов**	1.3
	Проверка наличия и заполнение штампа №1 при выводе на печать документа, содержащего защищаемую информацию	1.3.1
4	**Проверка защиты ввода и вывода информации на отчуждаемый физический носитель**	1.4
	Проверка возможности различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»)	1.4.1
	Проверка обеспечения соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства	1.4.2
	Проверка обеспечения соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой удаленного объекта при работе в «помеченном» канале связи	1.4.3
	Проверка возможности изменения в назначении и разметке устройств только под контролем СЗИ «Блокхост-Сеть 3»	1.4.4
5	**Проверка сопоставления пользователя с устройством**	1.5
	Проверка возможности обеспечить вывод информации на запрошенное пользователем устройство	1.5.1
	Проверка механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству	1.5.2
6	**Проверка механизма идентификации и аутентификации пользователей**	1.6
	Проверка требования от пользователей идентифицировать себя при запросах на доступ и проверка подлинности идентификатора субъекта (аутентификации)	1.6.1
	Проверка возможности надежно связывать полученную идентификацию со всеми действиями данного пользователя	1.6.2
7	**Проверка механизма регистрации событий**	1.7
	Проверка регистрации событий использования идентификационного и аутентификационного механизмов	1.7.1
	Проверка регистрации запроса на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)	1.7.2
	Проверка регистрации создания и уничтожения объекта	1.7.3

№ п/п	Наименование испытаний (проверок)	Пункт методики
	Проверка регистрации действий по изменению ПРД	1.7.4
	Проверка наличия средств выборочного ознакомления с регистрационной информацией	1.7.5
	Проверка регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.)	1.7.6
8	**Проверка взаимодействия пользователя с СЗИ «Блокхост-Сеть 3»**	1.8
	Проверка наличия модульной структуры СЗИ «Блокхост-Сеть 3» для обеспечения возможности изучения, анализа, верификации и модификации	1.8.1
	Проверка наличия стандартизированного интерфейса пользователя	1.8.2
	Проверка обеспечения надежности интерфейса	1.8.3
	Проверка логического изолирования интерфейса пользователя и СЗИ от других таких же интерфейсов	1.8.4
9	**Проверка надежного восстановления**	1.9
	Проверка полного восстановления свойств СЗИ «Блокхост-Сеть 3» после сбоев и отказов оборудования при использовании процедур восстановления	1.9.1
10	**Проверка целостности СЗИ «Блокхост-Сеть 3»**	1.10
	Проверка наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3»	1.10.1
	Проверка наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3» с блокировкой доступа пользователя при нарушении целостности	1.10.2
	Проверка регистрации событий, связанных с изменением целостности среды	1.10.3
	Проверка регистрации событий, связанных с изменением аппаратной среды	1.10.4
	Проверка выполнения программ в отдельной части оперативной памяти	1.10.5

1.1 Проверка реализации прав разграничения доступа

1.1.1 Проверка реализации дискреционного принципа контроля доступа

1.1.1.1 Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа

Описание функции

При разграничении доступа пользователей к объектам файловой системы для каждой пары субъект-объект в явном виде могут задаваться следующие типы доступа:

- чтение;
- запись;
- полный доступ (комбинация двух предыдущих типов доступа).

При определении прав доступа конкретного пользователя к объектам файловой структуры учитывается иерархия объектов (логический диск, каталог, подкаталог, файл), а также настройки доступа процессов к объектам файловой структуры,

реализованные средствами ОС.

При разрешении чтения файла доступно чтение содержимого файла. Запрещается изменение содержимого, переименование, перемещение, удаление файла. При этом нельзя изменить содержимое каталога.

При разрешении записи в файл возможно изменение содержимого и удаление файла. Остальные действия невозможны, например, нельзя прочитать содержимое каталога (подкаталоги и файлы), при этом все его содержимое также имеет запрет по чтению.

Комбинация этих двух разрешений дает полный доступ: чтение и изменение содержимого, запуск исполняемого файла, переименование, перемещение и удаление файла. Матрица доступа представлена в таблице (таблица П4.2).

Таблица П4.2 - Перечень разрешенных операций в зависимости от типа доступа

Разрешения на доступ для субъекта		**Перечень разрешенных операций по отношению к файлу (объекту)**					
Чтение	Запись	Чтение содержимого	Запись (изменение содержимого)	Запуск (для исполняемого файла)	Переимено-вание	Перемеще-ние	Удаление
+	-	+	-	+	-	-	-
-	+	-	+ (в каталоге)	-	-	-	+ (файл)
+	+	+	+	+	+	+	+
-	-	-	-	-	-	-	-

Действия

Для проведения тестов необходимо создание матрицы доступа, которая задаётся в явном виде средствами СЗИ, через консоль администрирования установкой соответствующих настроек.

Таблица П4.3 – Перечень действий при проверке контроля доступа наименованных субъектов

Каталог	**D:\D1**	**D:\D2**	**D:\D3**	**D:\D4**	**D:\D5**	**D:\D6**
User1	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).
User2	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).
User3	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).
User4	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)
Гость БхСети	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)
DefaultAccount	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)
Все пользователи	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)

БхСети						
UserTest1	Default	Default	Default	Default	Default	Default
UserTest2	Default	Default	Default	Default	Default	Default
Файлы	**D:\D1\ copyN.txt**	**D:\D2\ delN.txt**	**D:\D3\ modifyN.txt**	**D:\D4\ moveN.txt**	**D:\D5\ readN.txt**	**D:\D6\ renN.txt**
User1	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).	Чтение (R), Запись(W), Аудит (A).
User2	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).	Запись(W), Аудит (A).
User3	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).	Чтение (R), Аудит (A).
User4	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)
Гость БхСети	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)
DefaultAccount	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)	Аудит (A)

К защищаемым каталогам устанавливаются права доступа групп пользователей, которые выше установлены средствами СЗИ и предоставляют «Полный доступ» к каталогам. Соответственно «Полный доступ» включает в себя, такие права как «Чтение» и «Запись».

Таблица П4.4 – Матрица разграничения доступа, к файловой системе NTFS

Каталог	**D:\D1**	**D:\D2**	**D:\D3**	**D:\D4**	**D:\D5**	**D:\D6**
Прошедшие проверку	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ
Администраторы	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ
Пользователи	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ

Перечень действий для проверки выполнения контроля доступа и ожидаемый результат после выполнения каждого действия представлен в таблице П4.5.

Таблица П4.5 – Перечень действий при проверке контроля доступа наименованных субъектов

№ п/п	**Действия**	**Результат**
1	**Создание матрицы доступа и тестовых объектов файловой системы**	
	Создать матрицу разграничения доступа	Таблица П4.4
	На ЭВМ2 создать объекты файловой системы для проверки ПРД к каталогам: D:\D1, D:\D2, D:\D3,	Успешное создание указанных директорий и файлов

№ п/п	Действия	Результат
	D:\D4, D:\D5, D:\D6, каждый из которых содержит следующие файлы: copyN.txt, delN.txt, modifyN.txt, moveN.txt, readN.txt renameN.txt, где N – порядковый номер каталога из диапазона 1 – 6 и для проверки ПРД к файлам: D:\copy.txt, D:\del.txt, D:\modify.txt, D:\move.txt, D:\read.txt D:\rename.txt	
2	**Задание дискреционных ПРД**	
2.1	Запустить консоль администрирования СЗИ «Блокхост-Сеть 3»	Появление консоли администрирования
	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт **Список пользователей**. Выбрать пункт главного меню **Управление пользователями → Добавить пользователей**.	Появление окна **«Добавление пользователей»**
	Создать пользователей **User1**, **User2**, **User3**, **User4**	Пользователи **User1**, **User2**, **User3**, **User4** появились в **Основной панели настроек клиентов** в списке пользователей рабочей станции
	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → User1**. Выбрать параметр «**Дискреционный»**	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User1**
	Задать дискреционные ПРД для пользователя **User1** в соответствии с матрицей разграничения доступа, включить для всех объектов аудит	Отображение произведенных настроек в **Основной панели настроек клиента**
2.2	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → User2**. Выбрать параметр **Дискреционный**»	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User2**
	Задать дискреционные ПРД для пользователя **User2** в соответствии с матрицей разграничения доступа, включить для всех объектов аудит	Отображение произведенных настроек в **Основной панели настроек клиента**
2.3	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → User3**. Выбрать параметр «**Дискреционный**»	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User3**

№ п/п	Действия	Результат
	Задать дискреционные ПРД для пользователя **User3** в соответствии с матрицей разграничения доступа, включить для всех объектов аудит	Отображение произведенных настроек в **Основной панели настроек клиента**
2.4	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User4**. Выбрать параметр «**Дискреционный**»	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User4**
	Задать дискреционные ПРД для **User4, Гость БхСети, DefaultAccount, Все пользователи БхСети** в соответствии с матрицей РД, включив для всех объектов аудит	Отображение произведенных настроек в **Основной панели настроек клиента**
2.5	Создать средствами СЗИ пользователя UserTest1	Пользователь создан. Права дискреционного доступа в явном виде **не установлены**
2.6.	Создать средствами ОС пользователя UserTest2	Пользователь создан. Права дискреционного доступа в явном виде **не установлены**
2.7.	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Настройки сохранены
3	**Просмотр событий**	
	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2, Нажать кнопку «**Выполнить запрос»**.	Появление сообщений, фиксирующих произведенное изменение настроек на выбранной рабочей станции
	Завершить работу с консолью Системы развертывания и аудита	Закрытие окна Системы развертывания и аудита
4	**Проверка и установка политик разграничения доступа к файловой системе NTFS**	
	Открыть вкладку **Безопасность** свойств диска D:\, выбрать строку **Администраторы**	Отображаются права доступа файловой системы различных групп пользователей, после выбора строки **Администраторы** отображаются права группы **Администраторы**
	Выбрать из списка групп и пользователей строчку **Пользователи (…\Пользователи**)	Отображение прав доступа файловой системы группы **Пользователи**, которые не препятствуют полному доступу субъектов к объектам
4.1.	Установить права для группы «Пользователи» D:\D1 D:\D2 D:\D3 D:\D4 D:\D5 D:\D6	Полный доступ к каталогам группе «Пользователи» предоставлен (таблица П4.4)
5	**Проверка дискреционного механизма разграничения доступа для заданных пользователям ПРД**	
5.1	Осуществить вход в систему от имени и с правами пользователя **User1** и выполнить следующие действия	
	Чтение — D:\D1	Успешно
	Чтение — D:\read.txt	Успешно

№ п/п	Действия		Результат
	Копирование	D:\D2, копирование на D:\	Успешно
		D:\copy.txt, копирование на D:\	Успешно
	Переименование	D:\D3, новое имя D:\D3-rename	Успешно
		D:\rename.txt, новое имя D:\rename-rename.txt	Успешно
	Изменение	D:\D4\modify4.txt	Успешно
		D:\modify.txt	Успешно
	Перемещение	D:\D5\ в директорию D:\D2	Успешно
		D:\move.txt, в директорию D:\D1	Успешно
	Удаление	D:\D6\	Успешно
		D:\del.txt	Успешно
5.2	Восстановить объекты файловой системы. Завершить сеанс работы пользователя User1		Появление приглашения для входа в систему
5.3	Осуществить вход в систему от имени и с правами пользователя **User2** и выполнить следующие действия		
	Чтение	D:\D1	Неудачно
		D:\read.txt	Неудачно
	Копирование	D:\D2, копирование на D:\	Неудачно
		D:\copy.txt, копирование на D:\	Неудачно
	Переименование	D:\D3, новое имя D:\D3-rename	Неудачно
		D:\rename.txt, новое имя D:\rename-rename.txt	Неудачно
	Изменение	D:\D4\modify4.txt	Неудачно
		D:\modify.txt	Неудачно
	Перемещение	D:\D5\ в директорию D:\D2	Неудачно
		D:\move.txt, в директорию D:\D1	Неудачно
	Удаление	D:\D6	Неудачно
		D:\del.txt	Неудачно
	Восстановить объекты файловой системы. Завершить сеанс работы пользователя User2		Появление приглашения для входа в систему
5.4	Осуществить вход в систему от имени и с правами пользователя **User3** и выполнить следующие действия		
	Чтение	D:\D1	Успешно
		D:\read.txt	Успешно
	Копирование	D:\D2, копирование на D:\	Успешно
		D:\copy.txt, копирование на D:\	Успешно
	Переименование	D:\D3, новое имя D:\D3-rename	Неудачно
		D:\rename.txt, новое имя D:\rename-rename.txt	Неудачно

№ п/п	Действия		Результат
	Изменение	D:\D4\modify4.txt	Неудачно
		D:\modify.txt	Неудачно
	Перемещение	D:\D5\ в директорию D:\D2	Неудачно
		D:\move.txt, в директорию D:\D1	Неудачно
	Удаление	D:\D6	Неудачно
		D:\del.txt	Неудачно
	Восстановить объекты файловой системы. Завершить сеанс пользователя User3. Перезагрузить ОС		Появление приглашения для входа в систему
5.5	Осуществить вход в систему от имени и с правами пользователя **User4** и выполнить следующие действия		
	Чтение	D:\D1	Неудачно:
		D:\read.txt	Неудачно:
	Копирование	D:\D2, копирование на D:\	Неудачно:
		D:\copy.txt, копирование на D:\	Неудачно:
	Переименование	D:\D3, новое имя D:\D3-rename	Неудачно:
		D:\rename.txt, новое имя D:\rename-rename.txt	Неудачно:
	Изменение	D:\D4\modify4.txt	Неудачно:
		D:\modify.txt	Неудачно:
	Перемещение	D:\D5\ в директорию D:\D2	Неудачно:
		D:\move.txt, в директорию D:\D1	Неудачно:
	Удаление	D:\D6	Неудачно:
		D:\del.txt	Неудачно:
5.6.	Осуществить вход в систему от имени и с правами пользователя **UserTest1** и выполнить следующие действия		
	Чтение	D:\D1	Отказ в доступе к папке
	Чтение	D:\D2	Отказ в доступе к папке
	Чтение	D:\D3	Отказ в доступе к папке
	Чтение	D:\D4	Отказ в доступе к папке
	Чтение	D:\D5	Отказ в доступе к папке
	Чтение	D:\D6	Отказ в доступе к папке
5.7.	Осуществить вход в систему от имени и с правами пользователя **UserTest2** и выполнить следующие действия		
	Чтение	D:\D1	Отказ в доступе к папке
	Чтение	D:\D2	Отказ в доступе к папке
	Чтение	D:\D3	Отказ в доступе к папке
	Чтение	D:\D4	Отказ в доступе к папке
	Чтение	D:\D5	Отказ в доступе к папке
	Чтение	D:\D6	Отказ в доступе к папке
6	**Просмотр событий**		

№ п/п	Действия	Результат
	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1, Нажать кнопку **Выполнить запрос**.	Появление сообщений, фиксирующих успешные и неуспешные попытки доступа пользователей к файловым объектам

Результаты тестирования

Проверка контроля доступа наименованных субъектов к наименованным объектам считается успешной, если результатами проверок подтверждено, что:

- средства СЗИ позволяют задавать явные и недвусмысленные типы доступа (чтение, запись) для каждой пары «пользователь - объект доступа» (формировать матрицу доступа);
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым объектам.

1.1.1.2 Проверка применимости контроля доступа к каждому объекту и субъекту (индивиду или группе равноправных индивидов)

Описание функции

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Проверка данного требования осуществляется с использованием механизма копирования настроек СЗИ пользователей (индивидов). Механизм копирования настроек СЗИ «Блокхост-Сеть 3» позволяет применить созданные правила к разным пользователям, что существенно упрощает процесс настройки ПРД пользователей. Копирование настроек СЗИ позволяет выполнить полностью однотипные настройки для пользователей или группы равноправных пользователей.

Действия

Проверка применимости контроля доступа к каждому объекту и каждому субъекту выполняется на основе действий, выполняемых в п. 1.1.1.1.

Для настройки группового применения контроля доступа выполнить действия, указанные в таблице П4.6.

Таблица П4.6 – Проверка применимости контроля доступа к каждому объекту и субъекту

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Создать каталог TEST_DIR на диске D:\	Папка создана

№ п/п	Действия	Ожидаемый результат
3	Загрузить консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ1	Запуск консоли администрирования
4	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User1**. Выбрать параметр «**Дискреционный»**	Появление в **Основной панели настроек клиента** настроек дискреционного механизма СЗИ
5	Выполнить настройку дискреционного механизма: добавить каталог D:\TEST_DIR, отметить пункт **Аудит**	Изменения внесены
6	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
7	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **«User1»**. Выбрать параметр «**Дискреционный».**	Появление в **Основной панели настроек клиента** настроек дискреционного механизма СЗИ
8	Выбрать пункт меню «**Главная»** → **«Копировать настройки»**	Настройки дискреционного механизма пользователя **User1** скопированы в буфер обмена
9	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»**. Выбрать пользователя **User2**	Появление в **Основной панели настроек клиента** индивидуальных настроек разграничения доступа пользователя **User2**
10	Выбрать пункт меню «**Главная»** → **«Вставить»**	Настройки дискреционного механизма пользователя **User2** обновлены
11	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
12	Обновить отображение настроек механизмов СЗИ ЭВМ1, для чего выбрать пункт контекстного меню «**Обновить».**	Обновлено отображение настроек СЗИ рабочей станции
13	Убедиться в правильности применения настроек пользователя **User1** к пользователю **User2**	Правильное применение настроек пользователя **User1** к пользователю **User2**
14	Повторить действия пунктов 1-13 для всех поддерживаемых ОС на ЭВМ 1 – ЭВМ 5 для всех остальных операционных систем	Совпадение полученных результатов с приведенными выше

Результаты тестирования

Проверка считается успешной, если контроль доступа применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

1.1.1.3 Проверка возможности санкционированного изменения ПРД, в том числе изменения списка пользователей СВТ и списка защищаемых объектов

Описание функции

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

По умолчанию, право изменять ПРД предоставлено только встроенному локальному администратору СВТ, которому в СЗИ предоставлены полномочия «Администратор». Остальные пользователи СВТ не имеют прав на запуск консоли администрирования, что позволяет исключить возможность редактирования правил разграничения доступа пользователями.

Действия

Действия проверки выполняются последовательно, на основании проведенных проверок, изменяя установленные и фиксируя новые значения ПРД и списка пользователей:

1 проверка выполняется после выполнения действий п. 1.1.1.1.

Изменяются разрешения к файлу ***copyN.txt*** согласно матрице доступа, приведенной в таблице П4.7.

Таблица П4.7 – Матрица доступа к файлу ***copyN.txt***

	Действующие разрешения	**Устанавливаемые разрешения**
Каталог	**D:\D1**	**D:\D1**
Файлы	**D:\D1\copyN.txt**	**D:\D1\copyN.txt**
User1	Чтение (R)	Чтение (R)
	Запись(W)	-
	Аудит (A)	Аудит (A)

Таблица П4.8 – Проверка возможности санкционированного изменения ПРД

№ п/п	**Действия**		**Ожидаемый результат**
1	**Проверка изменения ПРД к файловым объектам**		
1.1	Войти в систему ЭВМ1 от имени и с правами пользователя Admin и запустить консоль администрирования СЗИ «Блокхост-Сеть 3»		Появление консоли администрирования
1.1.1	В окне **«Список машин»** выбрать ЭВМ2, и выполнить следующие действия: - в окне **«Настройки машины»** выбрать пункт «**Список пользователей»;** - выбрать пользователя **User1;** - выбрать параметр «**Дискреционный»;** - задать дискреционные ПРД для пользователя **User1** в соответствии с матрицей разграничения доступа приведенной в таблице П4.7; - сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**		Отображение произведенных настроек в **Основной панели настроек клиента**
1.2	Осуществить вход в систему от имени и с правами пользователя **User1** и выполнить следующие действия		
1.2.1	Изменение	D:\D1\copyN.txt	Неудачно

№ п/п	Действия	Ожидаемый результат
2	**Проверка изменения политики доступа к МНИ**	
2.1.	Войти в ОС ЭВМ14 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
2.1.1	Выполнить следующие действия: 1) В окне «Список машин» выбрать «Все_машины»; 2) Перейти в окно «Настройка группы Все_машины»; 3) Установить курсор на меню «Список пользователей»; 4) В группе «Все пользователи БхСети» выбрать опцию «Контроль портов и CD»; 5) Установить параметры «Разрешено» для USB, USB устройства, Запоминающие устройства, неизвестные устройства; 6) Нажать кнопку «Сохранить все»	Политика доступа создана и сохранена
2.2.	Войти в ОС ЭВМ6 от имени и справами пользователя User4	Загрузка рабочего стола
2.2.1	Подключить к USB портам:	В списке «Устройства и диски»
	- Flash drive 1,	Отражается
	- Flash drive 2,	Отражается
	- Flash drive 3,	Отражается
	- Flash drive 4,	Отражается
3	**Проверка санкционированного изменения списка пользователей**	
3.1	Войти на ОС **ЭВМ3** от имени и с правами локального пользователя **PC3\UserTest2 стандартным способом аутентификации**	**Отказ в доступе** (Пользователю запрещен интерактивный вход в систему)
3.2.	Войти в ОС **ЭВМ5** от имени и с правами пользователя Admin и загрузить серверную консоль администрирования СЗИ	Консоль запущена
3.2.1	Выбрать **ЭВМ3** и выполнить следующие действия: • в окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. • выбрать пункт главного меню «**Управление пользователями»** нажать кнопку **«Добавление пользователей»** • выбрать пользователя **UserTest2** и добавить в список пользователей.	Пользователь **UserTest2** добавлен в список пользователей СЗИ ЭВМ3
3.2.2	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
3.3.	Войти на ОС **ЭВМ3** от имени и с правами локального пользователя **PC3\UserTest2 стандартным способом аутентификации**	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
3.4.	Войти на ОС **ЭВМ3** от имени и с правами доменного пользователя **GIS\UserTest1**	Загрузка рабочего стола
3.5.	Войти в ОС **ЭВМ5** от имени и с правами пользователя Admin и загрузить серверную консоль администрирования СЗИ	Консоль запущена
3.5.1.	Выбрать **ЭВМ3** и выполнить следующие действия: • в окне **«Настройки машины»** выбрать пункт «**Список пользователей»**; • выбрать в списке доменного пользователя пункт главного **GIS\UserTest1** меню «**Управление пользователями»;** • через контекстное меню выбрать команду «Удаление из настроек».	Пользователь **GIS\UserTest1 удалён из** списка пользователей СЗИ ЭВМ3
3.5.2.	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
3.6.	Войти на ОС **ЭВМ3** от имени и с правами доменного пользователя **GIS\UserTest1**	**Отказ в доступе** (Пользователю запрещен интерактивный вход в систему)

Результаты тестирования

Проверка считается успешной, если администратор СЗИ успешно:

- создал и изменил ПРД пользователей (субъектов доступа) к объектам доступа (файлам, устройствам);
- создал и изменил список пользователей средствами СЗИ.

1.1.1.4 Проверка предоставления прав изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.)

Описание функции

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможность предоставления прав изменения ПРД выделенным субъектам.

Действия

Для выполнения проверки пользователю **User1** необходимо присвоить права администратора локальной рабочей станции. Выполняемые при проверке действия указаны в таблице П4.9.

Таблица П4.9 – Проверка предоставления прав изменения ПРД выделенным субъектам

№ п/п	Действия	Ожидаемый результат
1	**Создание субъектов доступа для администрирования СЗИ**	
	Загрузить серверную консоль администрирования СЗИ,	Запуск консоли администрирования

№ п/п	Действия	Ожидаемый результат
	в окне **«Список машин»** выбрать ЭВМ1	
	При отсутствии в списке пользователей СЗИ, добавить пользователей с именами **User1, User2 и User3** в соответствии с п. 6.5.1.1 настоящей методики	Добавление пользователей в базу СЗИ
2	Создание ПРД к администрированию СЗИ	
2.1	Выбрать **User1** и перейти в **Полномочия**. Для **User1** установить полномочия **Администратор**	Для **User1** полномочия Администратора установлены
2.2	Выбрать **User2** и перейти в **Полномочия**. Для **User2** установить полномочия Аудитор	Для **User2** полномочия Аудитора установлены
2.3	Для **User3** не настраивать **Полномочия** и оставить без изменения	
3	**Осуществление санкционированных и несанкционированных попыток доступа к администрированию СЗИ**	
3.1	Выполнить вход в систему от имени и с правами пользователя **User1**	
	Запустить серверную консоль администрирования СЗИ	Консоль запущена
	Изменить настройки СЗИ и произвести сохранение настроек	Измененные настройки сохранены
3.2	Выполнить вход в систему от имени и с правами пользователя **User2**	
	Запустить серверную консоль администрирования СЗИ	Консоль запущена
	Изменить настройки СЗИ и произвести сохранение настроек	Измененные настройки не сохранены, кнопка сохранить не активна
3.3	Выполнить вход в систему от имени и с правами пользователя **User3**	
	Запустить серверную консоль администрирования СЗИ	Консоль не запущена, Ошибка доступа: У Вас недостаточно прав для запуска консоли управления политиками.
4	Выполнить указанные в пунктах 1–3 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
5	Выполнить указанные в пунктах 1–3 действия для остальных поддерживаемых ОС на рабочих станциях в виртуальной сети	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки

Проверка считается успешной, если выделенному субъекту успешно предоставлены права на изменения ПРД и после входа в систему под учетной записью выделенного субъекта имеется возможность изменить правила разграничения доступа.

1.1.1.5 Проверка наличия механизма, претворяющего в жизнь дискреционные ПРД, как для явных, так и для скрытых действий пользователя

Описание функции

СЗИ «Блокхост-Сеть 3» должен содержать механизм, реализующий дискреционные ПРД как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, недопустимого с точки зрения заданных ПРД).

Под «явными» действиями подразумеваются действия, осуществляемые с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т.д.; а под «скрытыми» действиями – иные действия, в том числе с использованием собственных программ работы с устройствами.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.1.1 и основные ее этапы приведены в таблице П4.10.

Таблица П4.10 – Этапы проверки механизма ПРД

№ п/п	Действия	Ожидаемый результат
1	Войти в систему ЭВМ 2 от имени и справами пользователя Admin	Загрузка рабочего стола
2	Открыть файл *D:\D1\read1.txt*	Успешно
3	Изменить файл *D:\D1\read1.txt* и попытаться сохранить	Неудачно
4	Открыть файл *D:\read.txt*	Успешно
5	Изменить файл *D:\read.txt* и попытаться сохранить	Неудачно
6	Запустить файловый менеджер **Far**	Появление интерфейса программы
7	С помощью менеджера **Far** открыть файл *D:\D1\read1.txt*	Успешно
8	С помощью менеджера **Far** изменить файл *D:\D1\read1.txt* и попытаться сохранить	Неудачно
9	С помощью менеджера **Far** открыть файл *D:\read.txt*	Успешно
10	С помощью менеджера **Far** изменить файл *D:\read.txt* и попытаться сохранить	Неудачно
11	Выполнить вход в систему ЭВМ 1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
12	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку ***Выполнить запрос***.	Появление сообщений о попытках доступа к контролируемым объектам
13	Выполнить указанные в пунктах 1 – 12 действия на рабочих станциях ЭВМ 1 –ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

№ п/п	Действия	Ожидаемый результат
14	Выполнить указанные в пунктах 1–12 действия для остальных поддерживаемых ОС на рабочих станциях в виртуальной сети	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если средства СЗИ обеспечивают надежный контроль доступа субъектов к защищаемым ресурсам (объектам) в соответствии с принятой матрицей доступа как для явных действий, так и для скрытых действий пользователя.

1.1.1.6 Проверка контроля запуска программ и файлов

Описание функции

СЗИ «Блокхост-Сеть 3» должно иметь возможность производить контроль запуска программ и файлов, а также сообщать, какого типа файл был запущен (аудио\видео\изображение).

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.1.1 и основные ее этапы приведены в таблице П4.11.

Таблица П4.11 – Контроль запуска по типу файлов СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
1	Запустить консоль администрирования СЗИ «Блокхост-Сеть 3» на ЭВМ1 под учетной записью Admin	Появление консоли администрирования
2	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать «**Контроль запуска»**	В основной панели настроек отображаются настройки **Контроля запуска**
3	Установить «**Аудит»** на Аудио; Видео и Изображении	Настройки Контроля запуска по типу файла для ЭВМ2 установлены
4	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
5	Войти в систему ЭВМ2 пользователем **User1**	Загрузка рабочего стола
6	Запустить любое аудио, видео и изображение	Запуск успешен
7	Закрыть приложения с аудио, видео и изображениями	Закрытие процессов
8	Запустить консоль «Системы развертывания и аудита» на ЭВМ1. В окне выбрать **«Мониторинг»** выбрать ЭВМ1, под учетной записью Admin. Нажать кнопку «**Выполнить запрос»**.	Появление сообщений о запуске аудио, видео и изображения.
9	Выполнить указанные в пунктах 1 – 8 действия на рабочих станциях ЭВМ 1 –ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
10	Выполнить указанные в пунктах 1–8 действия для	Совпадение полученных

№ п/п	Действия	Ожидаемый результат
	остальных поддерживаемых ОС на рабочих станциях в виртуальной сети	результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если:

- средства СЗИ обеспечивают регистрацию событий запуска аудио и видео файлов, а также изображений;
- средства СЗИ обеспечивают регистрацию запуска аудио и видео файлов, а также изображений в виртуальной сети.

1.1.1.7 Проверка контроля запуска по маске имени файла

Описание функции

СЗИ «Блокхост-Сеть 3» должно иметь возможность производить контроль запуска программ и файлов по маске имени.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.1.1 и основные ее этапы приведены в таблице П4.12.

Таблица П4.12 – Контроль запуска по маске СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
1	Запустить консоль администрирования СЗИ «Блокхост-Сеть 3» на ЭВМ1 под учетной записью Admin	Появление консоли администрирования
2	В окне **«Список машин»** выбрать ЭВМ1, в окне **«Настройки машины»** выбрать «**Контроль запуска».**	В основной панели настроек отображаются настройки **Контроля запуска**
3	Нажать кнопку «**Добавить»** и в появившемся окне «**Маска имени файла»** добавить маску notepad и любое описание	Настройки Контроля запуска по маске имени файла для ЭВМ1 установлены
4	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
5	Войти в систему пользователем **User1**	Загрузка рабочего стола
6	Запустить word.exe	Запуск успешен
7	Запустить notepad.exe	Запуск успешен
8	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос»**.	Появление сообщений о запуске notepad.exe
9	Выполнить указанные в пунктах 1 – 8 действия на рабочих станциях ЭВМ 1 –ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
10	Выполнить указанные в пунктах 1–8 действия для	Совпадение полученных

№ п/п	Действия	Ожидаемый результат
	остальных поддерживаемых ОС на рабочих станциях в виртуальной сети	результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если средства СЗИ обеспечивают регистрацию событий запуска процессов по маске.

1.1.1.8 Проверка контроля запуска процессов по модели разрешенных процессов

СЗИ «Блокхост-Сеть 3» должно иметь возможность производить контроль запуска процессов по модели разрешённых процессов (модель замкнутой программной среды).

СЗИ должно обеспечивать регистрацию событий, связанных с контролем состояния запускаемых компонентов.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.1.1 и основные ее этапы приведены в таблице П4.13.

Таблица П4.13 – Контроль запуска процессов СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
1	Запустить консоль клиента СЗИ «Блокхост-Сеть 3» на ЭВМ1 под учетной записью Admin	Появление консоли администрирования
2	**Настройка списка разрешённых процессов на ЭВМ 1 при варианте использования СЗИ №1**	
2.1.	В окне «Список машин» выбрать ЭВМ1, в окне «Настройки машины» выбрать: 1) Список пользователей; 2) User1; 3) Контроль процессов.	В основной панели настроек отображаются настройки **Контроля процессов**
2.2	В вкладке «Основная панель настроек клиента» выполнить следующие действия: 1) Выбрать «Разрешенные процессы;» 2) Установить параметр «Отображение процессов всех пользователей»; 3) Перейти в список процессов и нажать сочетание клавиш CTRL + A (Выделить всё) 4) Перенести все процессы по поле разрешённых 5) Установить параметр «Установленные продукты»; 6) Перейти в список процессов и нажать сочетание клавиш CTRL + A (Выделить всё); 7) Перенести все процессы по поле разрешённых 8) Установить параметр «Контролировать»	Список разрешенных процессов сформирован. Параметры в поле «Аудит» проставлены автоматически.
2.3	В поле «Разрешенные процессы» выполнить следующие действия:	Процесс notepad.exe исключён из списка разрешенных

№ п/п	Действия	Ожидаемый результат
	1) Перейти в список процессов и нажать сочетание клавиш CTRL + F (Поиск); 2) В строке поиска ввести значение «notepad.exe»; 3) Найденный процесс «notepad.exe» удалить из списка	процессов
2.4	В поле «Разрешенные процессы» выполнить следующие действия: 1) Перейти в список процессов и нажать сочетание клавиш CTRL + F (Поиск); 2) В строке поиска ввести значение «notepad.exe»; 3) Найденный процесс «regedit.exe» удалить из списка	Процесс «regedit.exe» исключён из списка разрешенных процессов
2.5.	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»	Сохранение настроек
3	**Проверка запуска процессов пользователем User1 ЭВМ 1**	
3.1.	Выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
3.2	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «notepad.exe»	Отказ в доступе. Появляется сообщение «Windows не удаётся получить доступ к указанному устройству, пути или файлу. Возможно у Вас нет нужных разрешений для доступа к этому объекту.»
3.3.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «regedit.exe»	Отказ в доступе. Появляется сообщение «Windows не удаётся получить доступ к указанному устройству, пути или файлу. Возможно у Вас нет нужных разрешений для доступа к этому объекту.»
3.4.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «Calc.exe»	Программа «Калькулятор» запущена
4	**Проверка запуска процессов пользователем User2 ЭВМ 1**	
4.1.	Выполнить вход в систему от имени и с правами пользователя User2	Загрузка рабочего стола
4.2.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «notepad.exe»	Программа «Блокнот» запущена
4.3.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать	Программа «редактор реестра» запущена

№ п/п	Действия	Ожидаемый результат
	команду «regedit.exe».	
4.4.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «Calc.exe».	Программа «Калькулятор» запущена
5	**Настройка политики разрешённых процессов для ЭВМ, подключенных к серверу СЗИ при варианте использования СЗИ № 2**	
5.1.	Запустить консоль сервера СЗИ «Блокхост-Сеть 3» на ЭВМ1 под учетной записью Admin	Загрузка консоли администрирования
5.2.	В консоли администрирования выполнить следующие действия: 1) В окне «Список машин» выбрать «Все_машины»; 2) В окне «Настройки группы «Все_машины» выбрать «Список пользователей»; 3) Через контекстное меню выбрать команду «Задать»; 4) В подменю «Все пользователи БхСети» перейти на «Контроль процессов»; 5) Через контекстное меню выбрать команду «Задать».	Вкладка «Основная панель настроек клиентов» активна
5.3	В вкладке «Основная панель настроек клиента» выполнить следующие действия: 1) Выбрать «Разрешенные процессы;» 2) Установить параметр «Отображение процессов всех пользователей»; 3) Перейти в список процессов и нажать сочетание клавиш CTRL + A (Выделить всё) 4) Перенести все процессы по поле разрешённых 5) Установить параметр «Установленные продукты»; 6) Перейти в список процессов и нажать сочетание клавиш CTRL + A (Выделить всё); 7) Перенести все процессы по поле разрешённых; 8) Установить параметр «Контролировать».	Список разрешенных процессов сформирован. Параметры в поле «Аудит» проставлены автоматически.
5.4	В поле «Разрешенные процессы» выполнить следующие действия: 1) Перейти в список процессов и нажать сочетание клавиш CTRL + F (Поиск); 2) В строке поиска ввести значение «notepad.exe»; Найденный процесс «notepad.exe» удалить из списка	Процесс notepad.exe исключён из списка разрешенных процессов
5.5	В поле «Разрешенные процессы» выполнить следующие действия: 1) Перейти в список процессов и нажать сочетание клавиш CTRL + F (Поиск); 2) В строке поиска ввести значение «notepad.exe»; Найденный процесс «regedit.exe» удалить из списка	Процесс «regedit.exe» исключён из списка разрешенных процессов
5.6	Сохранить произведенные настройки, выбрав пункт меню «Главная» → «Сохранить все»	Сохранение настроек
6	**Проверка функционирования политики разрешенных процессов на ЭВМ, подключенных**	

№ п/п	Действия	Ожидаемый результат
	к серверу безопасности при варианте использования СЗИ № 2	
6.1.	Последовательно выполнить вход в систему на ЭВМ1, ЭВМ2, ЭВМ3, ЭВМ4 от имени и с правами пользователя User1 и User2 и повторить действия п.п. 6.1.1, 6.1.2. и 6.1.3.	Загрузка рабочего стола
6.1.1.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «notepad.exe»	Отказ в доступе. Появляется сообщение «Windows не удаётся получить доступ к указанному устройству, пути или файлу. Возможно у Вас нет нужных разрешений для доступа к этому объекту.»
6.1.2.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «regedit.exe»	Отказ в доступе. Появляется сообщение «Windows не удаётся получить доступ к указанному устройству, пути или файлу. Возможно у Вас нет нужных разрешений для доступа к этому объекту.»
6.1.3.	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «Calc.exe»	Программа «Калькулятор» запущена
7	**Регистрация событий безопасности**	
7.1.	Войти в систему ЭВМ 1 от имени и с правами пользователя **Admin** с ролью в СЗИ «Администратор» и «Аудитор»	Загрузка рабочего стола
7.2.	Запустить консоль «Система развертывания и аудита» и выполнить действия: 1) Перейти в раздел «Мониторинг», 2) Нажать кнопку «Выполнить запрос»	Информация о событиях безопасности загружена
8	Выполнить указанные в пунктах 1–7 действия для остальных поддерживаемых ОС на рабочих станциях	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если:

- СЗИ контролирует запуск процессов, по модели разрешённых процессов, указанных в явном виде, для каждого пользователя;
- СЗИ реализует политику контроля процессов;
- СЗИ реализует регистрацию событий, связанных с контролем состояния запускаемых компонентов.

1.1.2 Проверка мандатного принципа контроля доступа

1.1.2.1 Проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта

Описание функции

Мандатный механизм контроля доступа обеспечивает разграничение доступа субъектов (пользователей, процессов) к объектам (дискам, каталогам, папкам и файлам) с помощью классификационных уровней – комбинации иерархических и неиерархических категорий, назначаемых каждому объекту и субъекту доступа. Иерархическая категория определяет уровень конфиденциальности защищаемой информации (чем метка больше, тем выше степень конфиденциальности). Иерархические метки служат основой мандатного принципа разграничения доступа. Неиерархические категории выступают в качестве ограничений по доступу субъектов к объектам, соответствующих неиерархических категорий.

В качестве иерархических меток в СЗИ используются целые числа в диапазоне от 1 (низший уровень) до 255 (высший уровень).

Назначать классификационные уровни можно логическим дискам, каталогам и файлам. Назначение классификационного уровня каталогу означает, что все его содержимое, а также содержимое подкаталогов будет иметь указанный классификационный уровень, но только в случае, если вложенным объектам дополнительно не присвоен другой классификационный уровень. Одному субъекту или объекту доступа может быть назначена только одна (максимальная) иерархическая метка. Одному объекта или субъекту доступа может быть назначено несколько неиерархических категорий.

Общие правила разграничения доступа мандатного механизма состоят в следующем:

- субъект получает доступ к объекту по чтению, если его иерархическая метка не меньше иерархической метки объекта (ИМС ≥ ИМО) и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта.
- субъект получает доступ к объекту по записи, если его иерархическая метка равна иерархической метке объекта (ИМС = ИМО) и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Мандатный механизм контроля доступа настраивает администратор безопасности, при этом он в соответствии с заданной политикой безопасности:

- указывает значения классификационных меток и категорий и их названия;
- назначает каждому пользователю максимально возможный для этого пользователя классификационный уровень доступа;
- задает защищаемые ресурсы и присваивает классификационный уровень доступа, соответствующий степени конфиденциальности ресурса.

Тестирование мандатного механизма разграничения доступа ресурсам файловой системы проводится на основе разработанной матрицы разграничения доступа, представленной в таблице П4.14.

Таблица П4.14 – Матрица разграничения доступа

СУБЪЕКТЫ	**ОБЪЕКТЫ**			
	D:\M1	**D:\M2**	**D:\M3**	**D:\M4**
	мандатная метка	мандатная метка	мандатная метка	мандатная метка
	1	**2**	**3**	**1**
	Категория	Категория	Категория	Категория
	Public	**Public, Work**	**Public, Work, Secret**	**Public, Secret**
User1 мандатная метка = **1, Public**	RW	-	-	-
User2 мандатная метка = **2, Public, Work**	R	RW	-	-
User3 мандатная метка = **3, Public, Work, Secret**	R	R	RW	R
User4 мандатная метка = **1, Public, Secret**	R	-	-	RW
UserTest1 мандатная метка = **1 (**Default)	-	-	-	-
UserTest2	-	-	-	-

Действия

Действия, выполняемые при проверке, приведены в таблице П4.15.

Таблица П4.15 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	**Действия**	**Ожидаемый результат**
1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Загрузить серверную консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ2	Запуск консоли администрирования
3	**Создание объектов файловой системы**	
3.1	Создать каталоги D:\M1, D:\M2, D:\M3, D:\M4	Созданы каталоги D:\M1, D:\M2, D:\M3, D:\M4
3.2	Создать файлы: 1) D:\M1\Test1.txt; 2) D:\M2\Test 2.txt;	Созданы файлы D:\M1\ Test 1.txt, D:\M2\ Test 2.txt, D:\M3\ Test 3.txt D:\M4\ Test 4.txt

№ п/п	Действия	Ожидаемый результат
	3) D:\M3\Test 3.txt 4) D:\M4\Test 4.txt	
4	**Задание классификационных уровней (меток) объектам доступа**	
4.1	В консоли администрирования СЗИ в окне **«Настройки машины»** выбрать пункт «**Мандатное разграничение»**. Для добавления иерархических меток и категорий в СЗИ нажать кнопку «**Добавить»** в области Мандатные метки и категории «**Основной панели настроек клиентов».**	Появление окна «**Добавление мандатной метки»**
4.2	В окне **«Добавление мандатной метки»** отметить параметр **Метка** и ввести в поле **Ключ** значение метки **2**, ввести описание метки **2** и нажать кнопку «**Добавить».**	Метка с именем **2** появилась в области Мандатные метки и категории
4.3	В окне **«Добавление мандатной метки»** отметить параметр **Метка** и ввести в поле **Ключ** значение метки **3**, ввести описание метки **3** и нажать кнопку «**Добавить».**	Метка с именем **3** появилась в области Мандатные метки и категории
4.3	В окне **«Добавление мандатной метки»** отметить параметр «**Категория»** и ввести в поле **Ключ** значение категории **Public**, ввести описание категории **Общедоступная информация** и нажать кнопку **Добавить**	Категория с именем **Public** появилась в области Мандатные метки и категории
4.3	В окне **«Добавление мандатной метки»** отметить параметр «**Категория»** и ввести в поле **Ключ** значение категории **Work**, ввести описание категории «**Служебная информация»** и нажать кнопку «**Добавить».**	Категория с именем **Work** появилась в области Мандатные метки и категории
4.3	В окне **«Добавление мандатной метки»** отметить параметр «**Категория»** и ввести в поле **Ключ** значение категории **Secret**, ввести описание категории «**Секретная информация»** и нажать кнопку «**Добавить»**	Категория с именем **Secret** появилась в области Мандатные метки и категории
5	**Определение классификационных уровней (мандатных меток и категорий) для объектов доступа**	
5.1	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем «**Документы общего пользования»**	В области Список правил мандатной метки или категории отображается список ресурсов, сопоставленных данной метке – все подключенные к серверу безопасности диски
5.2	Перетащить мышью папки D:\M1 и D:\M4 из Списка объектов файловой системы ЭВМ2 в область Список правил мандатной метки или категории. В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области Список правил мандатной метки или категории отображаются папки M1, M4, сопоставленных данной метке. Параметр **Аудит** установлен.
5.3	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем **2**	В области Список правил мандатной метки или категории отображается пустой список ресурсов, сопоставленных данной метке
5.4	Перетащить мышью папку D:\M2 из Списка объектов файловой системы в область Список правил мандатной метки или категории.	В области Список правил мандатной метки или категории отображается папка M2, сопоставленная данной

№ п/п	Действия	Ожидаемый результат
	В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	метке. Параметр **Аудит** установлен.
5.5	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем **3**	В области Список правил мандатной метки или категории отображается пустой список ресурсов, сопоставленных данной метке
5.6	Перетащить мышью папку D:\M3 из Списка объектов файловой системы ЭВМ2 в область Список правил мандатной метки или категории. В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области Список правил мандатной метки или категории отображается папка M3, сопоставленная данной метке. Параметр **Аудит** установлен.
5.7	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить категорию с именем **Public**	В области Список правил мандатной метки или категории отображается пустой список ресурсов, сопоставленных данной категории
5.8	Перетащить мышью папки D:\M1, D:\M2, D:\M3 и D:\M4 из Списка объектов файловой системы ЭВМ2 в область Список правил мандатной метки или категории. В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области Список правил мандатной метки или категории отображается папки M1, M2, M3 и M4, сопоставленные данной категории. Параметр **Аудит** установлен.
5.9	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить категорию с именем **Work**	В области Список правил мандатной метки или категории отображается пустой список ресурсов, сопоставленных данной категории
5.10	Перетащить мышью папки D:\M2 и D:\M3 из Списка объектов файловой системы ЭВМ2 в область Список правил мандатной метки или категории. В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области Список правил мандатной метки или категории отображаются папки M2 и M3, сопоставленные данной категории. Параметр **Аудит** установлен.
5.11	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить категорию с именем **Secret**	В области Список правил мандатной метки или категории отображается пустой список ресурсов, сопоставленных данной категории
5.12	Перетащить мышью папки D:\M3 и D:\M4 из Списка объектов файловой системы ЭВМ2 в область Список правил мандатной метки или категории. В области Список правил мандатной метки или категории включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области Список правил мандатной метки или категории отображаются папки M3 и M4, сопоставленные данной категории. Параметр **Аудит** установлен.

№ п/п	Действия		Ожидаемый результат
5.13	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»		Настройки сохранены
6	**Задание классификационных меток субъектам доступа**		
6.1.	Для пользователей User1, User2, User3, User4, UserTest1 выполнить следующие действия: • создать и присвоить персональные идентификаторы; • в параметре «Аутентификация» установить параметр «Вход с токеном».		Параметры аутентификации пользователей установлены
6.2	Пользователю User1 присвоить мандатную метку «1» и категорию «Public»		Присвоены соответствующие мандатные метки и категории пользователям
	Пользователю User2 присвоить мандатную метку «2» и категорию «Public, Work»		
	Пользователю User3 присвоить мандатную метку «3» и категорию «Public, Work, Secret»		
	Пользователю User4 присвоить мандатную метку «1» и категорию «Public, Secret»		
	В окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. Проверить значения классификационных уровней пользователей в соответствии с таблицей П4.12		
6.3	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»		Настройки сохранены
7	**Просмотр событий аудита**		
7.1	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос»**		Появление сообщений, фиксирующих произведенные изменения настроек
7.2	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа**		
8.1	Выполнить вход в систему от имени и с правами пользователя **User1** и значением мандатной метки **1, Public**		
8.2	Чтение файлов	D:\M1\Test1.txt	Успешно
		D:\M2\Test2.txt	Неудачно. Отказ в доступе к папке
		D:\M3\Test3.txt	Неудачно. Отказ в доступе к папке
		D:\M4\Test4.txt	Неудачно. Отказ в доступе к папке
8.3	Запись файлов	D:\M1\Test1.txt в D:\M1	Успешно. Создана копия файла
		D:\M1\Test1.txt в D:\M2	Неудачно. Отказ в доступе к папке
		D:\M1\Test1.txt в D:\M3	Неудачно. Отказ в доступе к папке
		D:\M4\Test4.txt	Неудачно. Отказ в доступе к папке
8.4	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8.5	Выполнить вход в систему от имени и с правами пользователя **User2** и значением мандатной метки		

№ п/п	Действия		Ожидаемый результат
	2, Public, Work		
8.6	Чтение файлов	D:\M1\Test1.txt	Успешно
		D:\M2\Test2.txt.	Успешно
		D:\M3\Test3.txt	Неудачно. Отказ в доступе к папке
		D:\M4\Test4.txt	Неудачно. Отказ в доступе к папке
	Запись файлов	D:\M2\Test2.txt в D:\M1	Неудачно
		D:\M2\Test2.txt в D:\M2	Успешно. Создана копия файла
		D:\M1\Test1.txt в D:\M2	Успешно. Создана копия файла
8.7	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8.8	Выполнить вход в систему от имени и с правами пользователя **User3** и значением мандатной метки **3, Public, Work, Secret**		
8.9	Чтение файлов	D:\M1\Test1.txt	Успешно
		D:\M2\Test2.txt	Успешно
		D:\M3\Test3.txt	Успешно
		D:\M4\Test4.txt	Успешно
	Запись файлов	D:\M1\Test1.txt в D:\M1	Неудачно
		D:\M2\Test2.txt в D:\M2	Неудачно
		D:\M3\Test3.txt в D:\M3	Успешно. Создана копия файла
		D:\M4\Test4.txt в D:\M4	Неудачно
		D:\M1\Test1.txt в D:\M3	Успешно
		D:\M2\Test2.txt в D:\M3	Успешно
		D:\M4\Test4.txt в D:\M3	Успешно
		D:\M3\Test3.txt в D:\M1	Неудачно
		D:\M3\Test3.txt в D:\M2	Неудачно
		D:\M3\Test3.txt в D:\M4	Неудачно
8.10	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8.11	Выполнить вход в систему от имени и с правами пользователя **User4** и значением мандатной метки **1, Public, Secret**		
8.12	Чтение файлов	D:\M1\Test1.txt	Успешно
		D:\M2\Test2.txt	Неудачно. Отказ в доступе к папке
		D:\M3\Test3.txt	Неудачно. Отказ в доступе к папке
		D:\M4\Test4.txt	Успешно
	Запись файлов	D:\M4\Test4.txt в D:\M1	Неудачно
		D:\M4\Test4.txt в D:\M4	Успешно. Создана копия файла
		D:\M1\Test1.txt в D:\M4	Успешно
	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8.13	Выполнить вход в систему от имени и с правами пользователя **UserTest1** и значением мандатной метки **1**		
	Чтение файлов	D:\M1\Test1.txt	Неудачно. Отказ в доступе к папке
		D:\M2\Test2.txt	Неудачно. Отказ в доступе к папке
		D:\M3\Test3.txt	Неудачно. Отказ в доступе к папке

№ п/п	Действия		Ожидаемый результат
		D:\M4\Test4.txt	Неудачно. Отказ в доступе к папке
8.14	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
8.15	Выполнить вход в систему от имени и с правами пользователя **UserTest2**		
	Чтение файлов	D:\M1\Test1.txt	Неудачно. Отказ в доступе к папке
		D:\M2\Test2.txt	Неудачно. Отказ в доступе к папке
		D:\M3\Test3.txt	Неудачно. Отказ в доступе к папке
		D:\M4\Test4.txt	Неудачно. Отказ в доступе к папке
8.16	Перезагрузить ЭВМ2		Появление окна аутентификации СЗИ
9	**Просмотр событий аудита**		
9.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**		Загрузка рабочего стола
9.2	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос»**		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
10	Выполнить указанные в пунктах 1 – 9 действия для рабочих станций ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем		Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания механизма сопоставления классификационных меток каждого субъекта и каждого объекта считаются успешными, если результатами проверок подтверждено, что:

- средства СЗИ обеспечивают назначение классификационных меток (уровней конфиденциальности) объектам файловой системы и пользователям с помощью меток конфиденциальности;
- СЗИ обеспечивают управление потоками информации (при работе с объектами доступа, расположенными на локальной рабочей станции) на основе сопоставления меток конфиденциальности (субъект получает доступ к объекту по чтению, если его метка больше или равна метке объекта; субъект получает доступ к объекту по записи, если его метка не больше метки объекта);
- СЗИ реализует мандатный механизм контроля доступа к защищаемым ресурсам для всех пользователей СЗИ и ОС;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым локальным объектам.

1.1.2.2 Проверка запроса и получения классификационных меток при вводе новых данных в систему

Описание функции

СЗИ «Блокхост-Сеть 3» при вводе новых данных в систему должно запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток.

Действия

Проверка выполняется на основе действий, выполняемых в п. 1.1.2.1. По умолчанию любой субъект имеет мандатную метку со значением **1 и не назначены неиерархические категории**. Изменение присвоенной пользователю классификационной метки возможно только после его добавления в список пользователей.

При добавлении новых объектов классификационная метка, равная классификационной метке родительского объекта, присваивается ему автоматически. В случае, когда новый объект не имеет родительского объекта (например, использование накопителей информации с собственной файловой системой), такому объекту по умолчанию присваивается классификационная метка с низшим значением (со значением **1** без неиерархических категорий). Изменение классификационной метки нового объекта возможно сразу после его появления в СВТ.

Действия при проверке данного пункта указаны в таблице П4.16.

Таблица П4.16 – Действия при проверке запроса и получения классификационных меток при вводе новых данных в систему в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	**Создание объекта доступа**	
2.1	Создать файл C:\test_label.txt	Создание файла
3	Запустить консоль администрирования СЗИ	Окно консоли администрирования СЗИ
4	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Мандатный механизм»**. В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем **3**	В области Список правил мандатной метки или категории отображается список ресурсов, сопоставленных данной метке.
5	Перетащить мышью файл C:\test_label.txt из дерева ресурсов в область настроек	В области Список правил мандатной метки или категории в списке ресурсов, сопоставленных данной метке появился файл C:\test_label.txt

№ п/п	Действия	Ожидаемый результат
6	Сохранить произведенные настройки, выбрав пункт меню **Главная →Сохранить все**	Сохранение настроек
7	**Создание субъекта доступа**	
7.1	В окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. Выбрать пункт главного меню «**Управление пользователями» → «Добавление пользователей»**.	Появление окна **«Добавление пользователей»**
7.2	В окне **«Добавление пользователей»** дважды щелкнуть левой клавишей мыши по пункту **- «Добавить пользователя»**. Заполнить соответствующие пункты окна создания пользователя и нажать «**Создать».** В окне **«Добавление пользователей»** нажать кнопку «**Добавить».**	Появление окна **«Создание локального пользователя»** Созданный пользователь появился в «**Основной панели настроек клиентов»** в списке пользователей СЗИ
7.3	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
7.4	Изменить мандатную метку пользователя на значение **2** и назначить ему категорию **Public**	Изменение мандатной метки
7.5	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
8	Запустить консоль «Системы развертывания и аудита» в окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос»**	Появление сообщений, фиксирующих произведенное в СЗИ изменение параметров учетной записи пользователя
9	Выполнить указанные в пунктах 1 – 8 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания проверки запроса и получения классификационным меток при вводе новых данных в систему считаются успешными, если:

- новые данные при вводе в систему санкционированным пользователем получают мандатные метки;
- новым субъектам сопоставляются классификационные метки при санкционированном добавлении их в список пользователей.

1.1.2.3 Проверка реализации мандатного принципа контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов

Описание функции

СЗИ «Блокхост-Сеть 3» должна реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.2.1 согласно таблице П4.17.

Таблица П4.17 – Действия при проверке реализации мандатного принципа контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в ОС ЭВМ2 от имени и с правами пользователя **User2** и значением мандатной метки **2, Public, Work**	Загрузка рабочего стола
2	Запустить программу **Far**	Появление интерфейса программы
3	Прочитать файл D:\M1\read_1.txt	Успешно
4	Прочитать файл D:\M2\read_2.txt	Успешно
5	Прочитать файл D:\M3\read_3.txt	Неудачно
6	Записать D:\M2\read_2.txt в D:\M1	Неудачно
7	Записать D:\M2\read_2.txt в D:\M3	Неудачно
8	Записать D:\M2\read_2.txt в D:\M2 (клавиша **F5**, изменить имя файла на read_2-2.txt)	Успешно. Создана копия
9	Запустить консоль «**Системы развертывания и аудита**». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Наличие записей о попытках доступа к объектам
10	Выполнить указанные в пунктах 1 – 9 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если результаты явного доступа и скрытого доступа при проверке по п. 1.1.2.3 совпадают с результатами, полученными при проверке пункта 1.1.2.1.

1.1.2.4 Проверка возможности изменения классификационных уровней субъектов и объектов специально выделенными субъектами при реализации мандатных ПРД

Описание функции

Реализация мандатных ПРД должна предусматривать возможности сопровождения (изменения) классификационных уровней субъектов и объектов специально выделенными субъектами.

Действия

Проверка осуществляется на основе действий, выполняемых в п. 1.1.1.1. и п. 1.1.2.1.

Действия при проверке данного пункта указаны в таблице П4.18.

Таблица П4.18 – Действия при проверке возможности сопровождения (изменения) классификационных уровней субъектов и объектов специально выделенными субъектами

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Запуск консоли администрирования СЗИ. В окне **«Список машин»** выбрать ЭВМ2	В «**Основной панели настроек клиентов»** отобразились настройки механизмов СЗИ для ЭВМ2
3	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** →**User1**. Выбрать параметр «**Полномочия»**	Появление в «**Основной панели настроек клиента»** настроек механизма разграничения доступа пользователя к администрированию СЗИ
4	Задать в «**Основной панели настроек клиента»** для пользователя **User1** параметр «Администратор»	Отображение в «**Основной панели настроек клиента»** установленных пользователю **User1** параметра «Администратор»
5	Сохранить произведенные настройки, выбрав пункт «**Сохранить все»**	Сохранение настроек
6	Перезагрузить ЭВМ2	Появление интерфейса аутентификации в СЗИ
7	Выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
8	Запуск консоли администрирования СЗИ	Успешно
9	Изменить каталогу D:\M1 мандатную метку с **1** на **2**	Успешное изменение мандатной метки
10	Добавить каталог D:\M1 в список объектов мандатной категории **Work**	Успешное изменение мандатной категории
11	Сохранить произведенные настройки, выбрав пункт «**Сохранить все»**	Сохранение настроек
12	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать	Появление сообщений, фиксирующих произведенное изменение настроек

№ п/п	Действия	Ожидаемый результат
	ЭВМ2. Нажать кнопку «**Выполнить запрос»**	
13	Выполнить указанные в пунктах 1 – 11 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если предусмотрена возможность изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

1.1.2.5 Проверка реализации диспетчера доступа

Описание функции

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

На основе проверок согласно п. 1.1.1.1 диспетчер доступа реализует функциональность контроля и разграничения доступа в соответствии с требованиями РД в полном объеме.

Диспетчер доступа реализован в модуле «Модуль диспетчера доступа и гарантированного удаления». По умолчанию всем объектам присвоена иерархическая мандатная метка «**Документы общего пользования»**, равная «**1»** и не назначены неиерархические категории.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.2.1 согласно таблице П4.19.

Таблица П4.19 – Действия при проверке реализации диспетчера доступа

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Создать файлы на ЭВМ2: - D:\M1\test1.txt; - D:\M1\test2.txt; - D:\M2\test3.txt; - D:\M2\test4.txt;	Успешное создание указанных файлов

№ п/п	Действия	Ожидаемый результат
	- D:\M3\test5.txt; - D:\M3\test6.txt	
3	Запустить консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ2 и установить дискреционные права доступа на папки следующим образом для пользователя **User2**: - D:\M1\ = **R/W**; - D:\M2\ = **R/W**; - D:\M3\ = **R/W**	В **Основной панели настроек клиентов** отображаются параметры дискреционного механизма, установленные для пользователя **User2**
4	Выполнить вход в систему от имени и с правами пользователя **User2** и мандатной меткой **2, Public, Work**	Загрузка рабочего стола
5	Попытаться прочитать файлы D:\M3\test5.txt и D:\M3\test6.txt	Нет доступа
6	Прочитать D:\M1\test1.txt	Успешно
7	Открыть файл D:\M1\test2.txt, внести изменения в файл и попытаться сохранить	Неудачно
8	Сохранить измененный файл D:\M1\test2.txt в D:\M2\	Неудачно
9	Выполнить вход в систему на ЭВМ1 от имени и с правами пользователя **Admin**, запустить консоль администрирования СЗИ	Загрузка рабочего стола и открытие консоли администрирования СЗИ
10	Удалить из списка объектов мандатной метки **3** директорию D:\M3\	Успешное удаление D:\M3\ из списка объектов мандатной метки **3**
11	Удалить из списка объектов мандатной категории **Secret** директорию D:\M3\	Успешное удаление D:\M3\ из списка объектов мандатной категории **Secret**
12	Установить дискреционные права доступа на директорию D:\M3\ для пользователя **User2**: D:\M3\ = **-/-**.	Отображение установленных прав доступа
13	Сохранить произведенные настройки, выбрав пункт «**Сохранить все»**	Сохранение настроек
14	Выполнить вход в систему от имени и с правами пользователя **User2** и мандатной меткой **2, Public, Work**	Загрузка рабочего стола
15	Попытаться прочитать файлы D:\M3\test5.txt и D:\M3\test6.txt	Неудачно
16	Перезагрузить ЭВМ1, выполнить вход в систему от имени и с правами пользователя **Admin**, запустить консоль администрирования СЗИ	Загрузка рабочего стола и открытие консоли администрирования СЗИ
17	Установить дискреционные права доступа на директорию D:\M3\ для пользователя **User2**: D:\M3\ = **R/W**.	Отображение установленных прав доступа
18	Перезагрузить ЭВМ2, вход в систему от имени и с правами пользователя **User2** и мандатной меткой **2, Public, Work**	Загрузка рабочего стола
19	Прочитать файл D:\M3\test5.txt	Успешно

№ п/п	Действия	Ожидаемый результат
20	Прочитать файл D:\M3\test6.txt	Успешно
21	Скопировать файлы D:\M3\test5.txt и D:\M3\test6.txt в D:\M2	Успешно
22	Перезагрузить ЭВМ1, выполнить вход в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
23	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих произведенные изменения настроек и попытки доступа к контролируемым объектам
24	Выполнить указанные в пунктах 1 – 22 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Положительные результаты проверки согласно пункту 1.1.1.1 и положительные результаты при проверке настоящего пункта является достаточными признаками для принятия решения о реализации в СЗИ диспетчера доступа.

При реализации диспетчера доступа решение о санкционированности запроса принимается только при одновременном разрешении его как дискреционными, так и мандатными ПРД, потоки информации являются контролируемыми.

1.1.2.6 Проверка сетевого мандатного принципа разграничения доступа

Описание функции

Функция сетевого мандатного доступа реализуется при использовании MS Active Directory. СЗИ «Блокхост-Сеть 3» использует доменные учетные записи для предоставления доступа к сетевым папкам. Пользователям, как субъектам и сетевым папкам, как объектам доступа назначаются иерархические и неиерархические метки.

Субъекту или объекту доступа может быть назначена только одна иерархическая метка.

Субъекту или объекту доступа могут быть назначены несколько неиерархических меток.

Подробное описание общего принципа мандатного разграничения доступа приведено в разделе 1.1.2.1.

Действия

Для проведения проверки на ЭВМ1 создаются сетевые папки и назначаются права доступа согласно таблице П4.20. Пользователям предоставляются полные права.

Таблица П4.20 – Матрица разграничения доступа, реализуемая средствами ОС

Каталог	D:\M1	D:\M2	D:\M3	D:\D4
Администраторы	Владелец	Владелец	Владелец	Владелец
Admin	Чтение и запись	Чтение и запись	Чтение и запись	Чтение и запись
Все	Чтение и запись	Чтение и запись	Чтение и запись	Чтение и запись
GIS\User1	Полный доступ	Полный доступ	Полный доступ	Полный доступ
GIS\User2	Полный доступ	Полный доступ	Полный доступ	Полный доступ
GIS\User3	Полный доступ	Полный доступ	Полный доступ	Полный доступ
GIS\User4	Полный доступ	Полный доступ	Полный доступ	Полный доступ
GIS\UserTest1	Полный доступ	Полный доступ	Полный доступ	Полный доступ

Далее разграничение доступа реализуется средствами СЗИ.

В качестве субъектов доступа используются:

- доменный пользователь - GIS\UserTest1;
- доменные пользователи, являющиеся пользователями СЗИ:
  - GIS\User1;
  - GIS\User2;
  - GIS\User3;
  - GIS\User4;
- локальный пользователь UserTest;

которые будут обращаться к объектам доступа (сетевым папкам) находящимся на ЭВМ1.

ЭВМ1, ЭВМ2, ЭВМ3 и ЭВМ4 должны быть подключены к домену GIS.LAN.

В СЗИ не создаются групповые политики безопасности для группы пользователей «Гость БхСети».

Тестирование мандатного механизма разграничения доступа к ресурсам файловой системы проводится на основе разработанной матрицы разграничения доступа, представленной в таблице П4.21.

Таблица П4.21 – Матрица разграничения доступа к сетевым ресурсам

ЭВМ	**СУБЪЕКТЫ**	**ОБЪЕКТЫ**			
		\\PC1\M1	**\\PC1\M2**	**\\PC1\M3**	**\\PC1\M4**
		мандатная метка	мандатная метка	мандатная метка	мандатная метка
		1	**2**	**3**	**1**
		Категория	Категория	Категория	Категория
		Public	**Public, Work**	**Public, Work, Secret**	**Public, Secret**
ЭВМ1	**GIS\User1** мандатная метка = **1, Public**	RW	-	-	-
ЭВМ2	**GIS\User2**	R	RW	-	-

ЭВМ	СУБЪЕКТЫ	ОБЪЕКТЫ			
		\\PC1\M1	**\\PC1\M2**	**\\PC1\M3**	**\\PC1\M4**
		мандатная метка	мандатная метка	мандатная метка	мандатная метка
		1	**2**	**3**	**1**
		Категория	Категория	Категория	Категория
		Public	**Public, Work**	**Public, Work, Secret**	**Public, Secret**
	мандатная метка = **2, Public, Work**				
ЭВМ3	**GIS\User3** мандатная метка = **3,Public,Work,Secret**	R	R	RW	R
ЭВМ4	**GIS\User4** мандатная метка = **1, Public, Secret**	R	-	-	RW
ЭВМ4	**GIS\UserTest1**	X	X	X	X
ЭВМ4	**UserTest2**	X	X	X	X

Дальнейшие действия, выполняемые при проверке, приведены в таблице П4.22.

Таблица П4.22 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**.	Загрузка рабочего стола
2	Создать каталоги: D:\M1 D:\M2 D:\M3 D:\M4	Каталоги созданы
3	**Создание пользователей**	
3.1.	Запустить консоль «Active Directory – пользователи и компьютеры» и выполнить следующие действия: 1) Перейти по ветке «GIS.LAN» - «Users» 2) Создать пользователей - **GIS\User1;** - **GIS\User2;** - **GIS\User3;** - **GIS\User4;** - **GIS\UserTest1.**	Доменные пользователи созданы
3.2.	Войти в ОС **ЭВМ5** от имени и с правами пользователя Admin и загрузить серверную консоль администрирования СЗИ	Консоль запущена
3.3	Выбрать **ЭВМ2** и выполнить следующие действия: • в окне **«Настройки машины»** выбрать пункт	Появление окна **«Добавление пользователей»**

№ п/п	Действия	Ожидаемый результат
	«**Список пользователей»**. • выбрать пункт главного меню «**Управление пользователями»** нажать кнопку **«Добавление пользователей»**.	
3.3.1	В окне **«Добавление пользователей»** выполнить следующие действия: • дважды щелкнуть левой клавишей мыши по домену GIS.LAN; • в окне авторизации «Подключение к Active Directory» ввести имя и пароль доменного администратора; • в папке «USERS» выбрать пользователя **User1** и нажать кнопку «Добавить»; • Аналогичным образом добавить **User2 и User3**	Пользователи **User1, User2 и User3,** появились в «**Основной панели настроек клиентов»** в списке пользователей СЗИ.
3.4	Выбрать **ЭВМ3** и выполнить следующие действия: • в окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. • выбрать пункт главного меню «**Управление пользователями»** нажать кнопку **«Добавление пользователей»**.	Появление окна **«Добавление пользователей»**
3.4.1	В окне **«Добавление пользователей»** выполнить следующие действия: • дважды щелкнуть левой клавишей мыши по домену GIS.LAN; • в окне авторизации «Подключение к Active Directory» ввести имя и пароль доменного администратора; • в папке «USERS» выбрать пользователя **User4** и нажать кнопку «Добавить». • Аналогичным образом добавить **UserTest1**	Пользователи **User4 и UserTest1** появились в «**Основной панели настроек клиентов»** в списке пользователей СЗИ
3.5	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
3.6	Войти на ОС **ЭВМ4** от имени и с правами пользователя **Admin**	Загрузка рабочего стола
3.6.1	Создать средствами ОС пользователя **UserTest2**	Пользователь создан.
3.7	Войти на ОС **ЭВМ3** от имени и с правами пользователя **Admin**	Загрузка рабочего стола
3.7.1	Создать средствами ОС пользователя **UserTest2**	Пользователь создан.
4	**Настройка сетевого доступа к папкам**	
4.1	Через контекстное меню, выбрать свойства каталога D:\M1, и в вкладке «Доступ» средствами опций «Общий доступ» и «Расширенная настройка» установить разрешения согласно матрице доступа, приведенной в таблице П4.21	Общий доступ к папке M1 установлен. Разрешения установлены.

№ п/п	Действия	Ожидаемый результат
4.2	Повторить действия, указанные в п. 3.1 для каталогов D:\M2, D:\M3, D:\M4	Общий доступ и разрешения к папкам M2, M3, M4 установлены
5	**Проверка доступности созданных сетевых ресурсов до назначения мандатных меток**	
5.1	Войти на ОС **ЭВМ2** от имени и с правами пользователя **GIS\User1**	Загрузка рабочего стола
5.1.1.	Перейти к сетевой папке **\\PC1\M1** и создать файл read_1.txt	Сетевой ресурс **\\PC1\M1** доступен и файл read_1.txt создан.
5.2	Войти на ОС **ЭВМ2** от имени и с правами пользователя **GIS\User2**	Загрузка рабочего стола
5.2.1	Перейти к сетевой папке **\\PC1\M2** и создать файл read_2.txt	Сетевой ресурс **\\PC1\M2** доступен и файл read_2.txt создан.
5.3	Войти на ОС **ЭВМ2** от имени и с правами пользователя **GIS\User3**	Загрузка рабочего стола
5.3.1	Перейти к сетевой папке **\\PC1\M3** и создать файл read_3.txt	Сетевой ресурс **\\PC1\M3** доступен и файл read_3.txt создан.
5.4.	Войти на ОС **ЭВМ3** от имени и с правами пользователя **GIS\User4**	Загрузка рабочего стола
5.4.1.	Перейти к сетевой папке **\\PC1\M4** и создать файл read_4.txt	Сетевой ресурс **\\PC1\M4** доступен и файл read_4.txt создан.
5.5	Войти на ОС **ЭВМ3** от имени и с правами доменного пользователя **GIS\UserTest1**	Загрузка рабочего стола
5.6.	Войти на ОС **ЭВМ3** от имени и с правами локального пользователя **PC3\UserTest2 стандартным способом аутентификации**	**Отказ в доступе** (Пользователю запрещен интерактивный вход в систему)
5.7	Войти на ОС **ЭВМ4** от имени и с правами доменного пользователя **GIS\UserTest1**	Загрузка рабочего стола
5.7.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**	Сетевые ресурсы **доступны**
5.8	Войти на ОС **ЭВМ4** от имени и с правами локального пользователя **PC4\UserTest2 стандартным способом аутентификации**	Загрузка рабочего стола
5.8.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**	Сетевые ресурсы **доступны**
6	**Задание классификационных меток субъектам доступа**	
6.1.	Войти в ОС **ЭВМ5** от имени и с правами пользователя Admin и загрузить серверную консоль администрирования СЗИ	Консоль запущена
6.2	Для пользователей User1, User2, User3, User4, UserTest1 на **ЭВМ1, ЭВМ2** и **ЭВМ3** выполнить следующие действия: • создать и присвоить персональные идентификаторы; • в параметре «Аутентификация» установить параметр «Вход с токеном».	Параметры аутентификации пользователей установлены
6.3	Пользователю User1 присвоить мандатную метку «1» и категорию «Public»	Присвоены соответствующие мандатные метки и категории

№ п/п	Действия		Ожидаемый результат
	Пользователю User2 присвоить мандатную метку «2» и категорию «Public, Work»		пользователям
	Пользователю User3 присвоить мандатную метку «3» и категорию «Public, Work, Secret»		
	Пользователю User4 присвоить мандатную метку «1» и категорию «Public, Secret»		
	В окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. Проверить значения классификационных уровней пользователей в соответствии с таблицей П4.21		
6.4	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**		Настройки сохранены
7	**Проверка заданных классификационных меток объектам доступа**		
7.1	Выбрать во вкладке «Список машин» выбрать ЭВМ1 и в вкладке «Настройки машины ЭВМ1» перейти в опцию «Мандатное разграничение».		Иерархические и неиерархические мандатные метки соответствуют указанным в таблице П4.21
8	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа из защищённого сегмента сети**		
8.1	Выполнить вход в систему **ЭВМ2** от имени и с правами пользователя GIS**User1** и значением мандатной метки **1, Public**		
8.2	Чтение файлов	\\PC1\M1\read_1.txt	Успешно
		\\PC1\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\PC1\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\PC1\M4\read_4.txt	Неудачно. Отказ в доступе к папке
8.3	Запись файлов	\\PC1\M1\read_1.txt в \\PC1\M1	Успешно. Создана копия файла
8.4		\\PC1\M1\read_1.txt в \\PC1\M2	Неудачно. Отказ в доступе к папке
		\\PC1\M1\read_1.txt в \\PC1\M3	Неудачно. Отказ в доступе к папке
		\\PC1\M4\read_4.txt	Неудачно. Отказ в доступе к папке
8.5	Выполнить вход в систему **ЭВМ2** от имени и с правами пользователя **GIS\User2** и значением мандатной метки **2, Public, Work**		
8.6	Чтение файлов	\\PC1\M1\read_1.txt	Успешно
		\\PC1\M2\read_2.txt.	Успешно
		\\PC1\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\PC1\M4\read_4.txt	Неудачно. Отказ в доступе к папке
	Запись файлов	\\PC1\M2\read_2.txt в \\PC1\M1	Неудачно
		\\PC1\M2\read_2.txt в \\PC1\M2	Успешно. Создана копия файла
		\\PC1\M1\read_1.txt в \\PC1\M2	Успешно. Создана копия файла
8.8	Выполнить вход в систему **ЭВМ2** от имени и с правами пользователя **GIS\User3** и значением мандатной метки **3, Public, Work, Secret**		
8.9	Чтение файлов	\\PC1\\M1\read_1.txt	Успешно
		\\PC1\M2\read_2.txt	Успешно
		\\PC1\M3\read_3.txt	Успешно
		\\PC1\M4\read_4.txt	Успешно
	Запись файлов	\\PC1\M1\read_1.txt в \\PC1\M1	Неудачно
		\\PC1\M2\read_2.txt в \\PC1\M2	Неудачно
		\\PC1\M3\read_3.txt в \\PC1\M3	Успешно. Создана копия файла

№ п/п	Действия		Ожидаемый результат
		\\PC1\M4\read_4.txt в \\PC1\M4	Неудачно
		\\PC1\M1\read_1.txt в \\PC1\M3	Неудачно
		\\PC1\M2\read_2.txt в \\PC1\M3	Успешно
		\\PC1\M4\read_4.txt в \\PC1\M3	Успешно
		\\PC1\M3\read_3.txt в \\PC1\M1	Неудачно
		\\PC1\M3\read_3.txt в \\PC1\M2	Неудачно
		\\PC1\M3\read_3.txt в \\PC1\M4	Неудачно
8.11	Выполнить вход в систему **ЭВМ3** от имени и с правами пользователя **GIS\User4** и значением мандатной метки **1, Public, Secret**		
8.12	Чтение файлов	\\PC1\M1\read_1.txt	Успешно.
		\\PC1\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\PC1\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\PC1\M4\read_4.txt	Успешно
	Запись файлов	\\PC1\M4\read_4.txt в \\PC1\M1	Неудачно
		\\PC1\M4\read_4.txt в \\PC1\M4	Успешно. Создана копия файла
		\\PC1\M1\read_1.txt в \\PC1\M4	Успешно
8.13	Войти на ОС **ЭВМ3** от имени и с правами доменного пользователя **GIS\UserTest1**		Загрузка рабочего стола
8.13.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**		Сетевые ресурсы **не доступны**
8.14	Войти на ОС **ЭВМ3** от имени и с правами локального пользователя **PC4\UserTest2 стандартным способом аутентификации**		Отказ в доступе. Пользователю запрещен интерактивный доступ в систему
8.14.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**		Сетевые ресурсы **не доступны**
9	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа из незащищённого сегмента сети**		
9.1	Войти на ОС **ЭВМ4** от имени и с правами доменного пользователя **GIS\UserTest1**		Загрузка рабочего стола
9.1.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**		Сетевые ресурсы **не доступны**
9.2	Войти на ОС **ЭВМ4** от имени и с правами локального пользователя **PC4\UserTest2 стандартным способом аутентификации**		Загрузка рабочего стола
9.2.1	Последовательно перейти к сетевым папкам **\\PC1\M1, \\PC1\M2, \\PC1\M3, \\PC1\M4**		Сетевые ресурсы **не доступны**
10	**Просмотр событий аудита**		
10.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**		Загрузка рабочего стола
10.2	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос»**		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

Критерии оценки

Испытания механизма сопоставления классификационных меток каждого субъекта и каждого объекта считаются успешными, если результатами проверок подтверждено,

что:

- средства СЗИ обеспечивают назначение классификационных меток (уровней конфиденциальности) локальным и доменным пользователям, а также сетевым ресурсам (каталогам) с помощью меток конфиденциальности;
- СЗИ обеспечивают управление потоками информации (при работе с объектами доступа, расположенными на сетевой рабочей станции) на основе сопоставления меток конфиденциальности (субъект получает доступ к объекту по чтению, если его метка больше или равна метке объекта; субъект получает доступ к объекту по записи, если его метка не больше метки объекта);
- СЗИ реализует мандатный механизм контроля доступа к защищаемым ресурсам для всех пользователей СЗИ и ОС;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым локальным объектам.

1.1.2.7 Проверка сетевого мандатного доступа без использования MS Active Directory

Описание функции

Функция сетевого мандатного доступа реализуется средствами СЗИ в одноранговой сети без использования MS Active Directory. СЗИ «Блокхост-Сеть 3» использует учетные записи пользователей СЗИ. Пользователям, как субъектам и сетевым папкам, как объектам доступа назначаются иерархические и неиерархические метки.

Подробное описание общего принципа мандатного разграничения доступа приведено в разделе 1.1.2.1.

Действия

Проверка проводится в виртуальной сети. Для проведения проверки используется Сервер БХС1 уровня иерархии II ЭВМ13 и подключенные к нему ЭВМ 6-9.

Средствами системы развертывания и аудита ЭВМ9 выводиться из защищенного СЗИ сегмента сети для осуществления попыток доступа пользователем UserTest1 к защищаемым сетевым ресурсам. Удаление клиента «Блокхост-Сеть» с ЭВМ9 выполняется в соответствии с п. 3.3.4.1. Руководства администратора безопасности «Система развёртывания и аудита».

ЭВМ должны находиться в типе сетевого размещения «Сеть предприятия». Для этого в «Центре управления сетями и общим доступом» требуется перейти по ссылкам «Выбор домашней группы и параметров общего доступа» - «Что такое расположение в сети» и в открывшемся окне «Настройка сетевого размещения» выбрать «Сеть предприятия».

В профиле «Общий (текущий профиль)» должны быть установлены параметры:

- «Включить сетевое обнаружение»;

- «Включить общий доступ к файлам и принтерам»;
- «Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках»;
- «Использовать 128-битное шифрование для защиты подключений общего доступа»;
- «Включить общий доступ с парольной защитой».

Установка параметров выполняется переходом по ссылкам «Центр управления сетями и общим доступом» - «Выбор домашней группы и параметров общего доступа» - «Изменение дополнительных параметров общего доступа», в окне «Дополнительные параметры общего доступа».

Дополнительно на ЭВМ проверяется установки локальной политики безопасности.

Для проверки локальной политики безопасности следует перейти по ветке «Панель управления» - «Администрирование» - «Локальная политика безопасности».

В открывшимся окне «Локальная политика безопасности» перейти по иерархическому списку «Параметры безопасности» – «Локальные политики» – «Параметры безопасности» – Политика «Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей». Должен быть установлен параметр безопасности «Обычная – локальные пользователи удостоверяются как они сами».

Схема испытательного стенда и подключений пользователей для проверки сетевого мандатного принципа разграничения доступа приведена на рисунке П4.1.

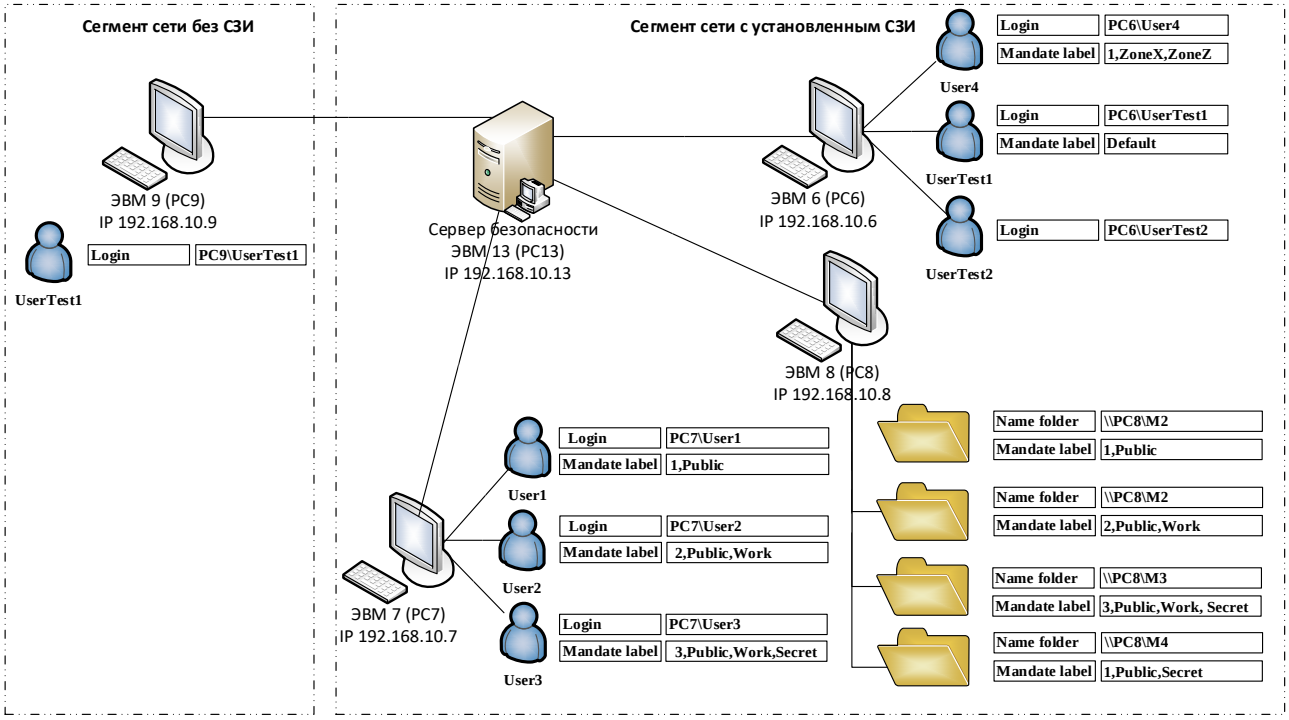

Рисунок П4.1 – Схема подключения испытательного стенда

Для проведения проверки на ЭВМ8 средствами операционной системы создаются сетевые папки и назначаются права доступа согласно таблице П4.23. Пользователям предоставляются полные права.

Таблица П4.23 – Матрица разграничения доступа, реализуемая средствами ОС

Каталог	**D:\M1**	**D:\M2**	**D:\M3**	**D:\D4**
Администраторы	Владелец	Владелец	Владелец	Владелец
Admin	Чтение и запись	Чтение и запись	Чтение и запись	Чтение и запись
Все	Чтение и запись	Чтение и запись	Чтение и запись	Чтение и запись

Учетные записи пользователей создаются средствами СЗИ. Для корректности работы их профилей требуется пройти авторизацию на всех ЭВМ, участвующих в проверке, в том числе и на ЭВМ8. Далее ЭВМ8 для доступа пользователями к защищаемым сетевым ресурсам не используется.

При авторизации на ЭВМ проверяется доступность сетевых ресурсов.

После проверки доступности сетевых ресурсов, объектам и субъектам доступа назначаются мандатные метки и категории согласно таблице П4.24.

В ходе проведения проверки пользователь:

- UserTest1 являясь пользователем и ОС и СЗИ, пытается получить доступ к сетевым папкам из защищенного сегмента сети с ЭВМ6 и из незащищённого сегмента, с ЭВМ9;
- UserTest2 являясь пользователем операционной системы, но не пользователем СЗИ, пытается получить доступ защищаемым ресурсам с ЭВМ6.

Таблица П4.24 – Матрица разграничения доступа к сетевым ресурсам

ЭВМ	**СУБЪЕКТЫ**	**ОБЪЕКТЫ**			
		\\PC8\M1	**\\PC8\M2**	**\\PC8\M3**	**\\PC8\M4**
		мандатная метка	мандатная метка	мандатная метка	мандатная метка
		1	**2**	**3**	**1**
		Категория	Категория	Категория	Категория
		Public	**Public, Work**	**Public, Work, Secret**	**Public, Secret**
ЭВМ7	**PC7\User1** мандатная метка = **1, Public**	RW	-	-	-
ЭВМ7	**PC7\User2** мандатная метка = **2, Public, Work**	R	RW	-	-
ЭВМ7	**PC7\User3** мандатная метка = **3, Public, Work, Secret**	R	R	RW	R
ЭВМ6	**PC6\User4** мандатная метка = **1, Public, Secret**	R	-	-	RW

ЭВМ6	**PC6\UserTest1** мандатная метка = **default**	X	X	X	X
ЭВМ6	**UserTest2**	X	X	X	X
ЭВМ9	**UserTest1**	X	X	X	X

Дальнейшие действия, выполняемые при проверке, приведены в таблице П4.25.

Таблица П4.25 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	Действия	Ожидаемый результат
1	**Создание каталогов**	
1.1	Войти в ОС ЭВМ8 от имени и с правами пользователя **Admin**.	Загрузка рабочего стола
1.2	Создать каталоги: D:\M1 D:\M2 D:\M3 D:\M4	Каталоги созданы
1.3	Установить общий доступ к каталогам и права доступа пользователей	Общий доступ и права пользователей к каталогам установлены согласно таблице П4.22
2	**Создание пользователей**	
2.1.	Войти в ОС ЭВМ13 от имени и с правами пользователя **Admin**.	Загрузка рабочего стола
2.1.1	Запустить серверную консоль сервера безопасности «Блокхост-Сеть 3» и создать средствами СЗИ пользователей.	Пользователи согласно таблицы П4.23 созданы.
2.2	Удалить пользователя UserTest2 из настроек ЭВМ6	Пользователь UserTest2 из настроек ЭВМ6 удалён.
3	**Удаление клиента СЗИ с ЭВМ9**	
3.1	Запустить СРиА, создать и запустить задачу «Удаление Блокхост-Сеть Клиент» для ЭВМ9	Клиент СЗИ с ЭВМ9 удалён.
4	**Проверка доступности сетевых ресурсов**	
4.1	Войти на ОС **ЭВМ7** от имени и с правами пользователя **User1**	Загрузка рабочего стола
4.1.1	Перейти к сетевой папке **\\PC8\M1** и создать файл read_1.txt	Сетевой ресурс **\\PC8\M1** доступен и файл read_1.txt создан.
4.2	Войти на ОС **ЭВМ7** от имени и с правами пользователя **User2**	Загрузка рабочего стола
4.2.1	Перейти к сетевой папке **\\PC8\M2** и создать файл read_2.txt	Сетевой ресурс **\\PC8\M2** доступен и файл read_2.txt создан.
4.3	Войти на ОС **ЭВМ7** от имени и с правами пользователя **User3**	Загрузка рабочего стола

4.3.1	Перейти к сетевой папке **\\PC8\M3** и создать файл read_3.txt	Сетевой ресурс **\\PC8\M3** доступен и файл read_3.txt создан.
4.4.	Войти на ОС **ЭВМ6** от имени и с правами пользователя **User4**	Загрузка рабочего стола
4.4.1	Перейти к сетевой папке **\\PC8\M4** и создать файл read_4.txt	Сетевой ресурс **\\PC8\M4** доступен и файл read_4.txt создан.
4.5.	Войти на ОС **ЭВМ6** от имени и с правами пользователя **UserTest1**	Загрузка рабочего стола
4.6.	Перейти к сетевой папке **\\PC8\M4**	Сетевой ресурс **\\PC8\M4** доступен
4.6.1	Войти на ОС **ЭВМ6** от имени и с правами пользователя **UserTest2**	Отказ в доступе. Пользователю запрещен интерактивный вход в систему.
4.7	Войти на ОС **ЭВМ9** от имени и с правами пользователя **UserTest1**	Загрузка рабочего стола
4.7.1	Перейти к сетевой папке **\\PC8\M4**	Сетевой ресурс **\\PC8\M4** доступен
5	**Задание политики для группы «Гость БхСети»**	
5.1	Создать политику перейдя по опциям «Все_машины» – «Список пользователей» – «Добавление пользователей», выбрать группу «Гость БхСети» и нажать кнопку «Добавить».	Политика для группы «Гость БхСети» задана.
5.2	Задать способы «Аутентификации» для группы «Гость БхСети» установив параметры в параметрах: • Вход с токеном • Локальный вход • Сетевой вход	Параметры аутентификации установлены
5.3	Задать мандатную метку «3» для группы «Гость БхСети»	Мандатная метка установлена
6	**Установка параметров авторизации пользователей**	
6.1.	Для пользователей User1, User2, User3, User4, UserTest1 на **ЭВМ13, ЭВМ6, ЭВМ7** и **ЭВМ8** установить параметры авторизации выполнив следующие действия: • создать и присвоить персональные идентификаторы; • в параметре «Аутентификация» установить параметр «Вход с токеном».	Параметры аутентификации пользователей установлены
7	**Задание классификационных меток и категорий субъектам доступа и объектам доступа**	
7.1.	Для пользователей User1, User2, User3, User4 на **ЭВМ13, ЭВМ6, ЭВМ7** и **ЭВМ8** задать классификационные метки и категории пользователям согласно таблице П4.23 на ЭВМ13, ЭВМ6, ЭВМ7, ЭВМ8	Классификационные метки и категории заданы согласно таблице П4.23.
7.2.	Для созданных каталогов **\\PC8\M1 \\PC8\M2 \\PC8\M3 \\PC8\M4** задать классификационные метки и категории согласно таблице П4.23	Классификационные метки и категории заданы согласно таблице П4.23.
7.3.	Перезагрузить ЭВМ13, ЭВМ6, ЭВМ7 и ЭВМ8	ЭВМ перезагружены

8	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа из не защищённого сегмента сети**		
8.1	Выполнить вход в систему **ЭВМ9** от имени и с правами пользователя **PC9\UserTest1**		
8.2.	Чтение файлов	\\192.168.10.8\M1\read_1.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
9	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа из защищённого сегмента сети**		
9.1	Выполнить вход в систему **ЭВМ7** от имени и с правами пользователя **PC7\User1** и значением мандатной метки **1, Public**		
9.1.1	Чтение файлов	\\192.168.10.8\M1\read_1.txt	Успешно
		\\192.168.10.8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
9.1.2.	Запись файлов	\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M1	Успешно. Создана копия файла
		\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M2	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M1\read_1.txt в \\PC1\M3	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
9.2	Выполнить вход в систему **ЭВМ7** от имени и с правами пользователя **PC7\User2** и значением мандатной метки **2, Public, Work**		
9.2.1	Чтение файлов	\\192.168.10.8\M1\read_1.txt	Успешно
		\\192.168.10.8\M2\read_2.txt.	Успешно
		\\192.168.10.8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
9.2.1.	Запись файлов	\\192.168.10.8\M2\read_2.txt в \\192.168.10.8\M1	Неудачно
		\\192.168.10.8\M2\read_2.txt в \\192.168.10.8\M2	Успешно. Создана копия файла
		\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M2	Успешно. Создана копия файла
9.3.	Выполнить вход в систему **ЭВМ7** от имени и с правами пользователя **PC7\User3** и значением мандатной метки **3, Public, Work, Secret**		
9.3.1	Чтение файлов	\\192.168.10.8\\M1\read_1.txt	Успешно
		\\192.168.10.8\M2\read_2.txt	Успешно
		\\192.168.10.8\M3\read_3.txt	Успешно

		\\192.168.10.8\M4\read_4.txt	Успешно
9.3.2.	Запись файлов	\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M1	Неудачно
		\\192.168.10.8\M2\read_2.txt в \\192.168.10.8\M2	Неудачно
		\\192.168.10.8\M3\read_3.txt в \\192.168.10.8\M3	Успешно. Создана копия файла
		\\192.168.10.8\M4\read_4.txt в \\192.168.10.8\M4	Неудачно
		\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M3	Неудачно
		\\192.168.10.8\M2\read_2.txt в \\192.168.10.8\M3	Успешно
		\\192.168.10.8\M4\read_4.txt в \\192.168.10.8\M3	Успешно
		\\192.168.10.8\M3\read_3.txt в \\192.168.10.8\M1	Неудачно
		\\192.168.10.8\M3\read_3.txt в \\192.168.10.8\M2	Неудачно
		\\192.168.10.8\M3\read_3.txt в \\192.168.10.8\M4	Неудачно
9.4.	Выполнить вход в систему **ЭВМ6** от имени и с правами пользователя **PC6\User4** и значением мандатной метки **1, Public, Secret**		
9.4.1.	Чтение файлов	\\192.168.10.8\M1\read_1.txt	Успешно.
		\\192.168.10.8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Успешно
9.4.2.	Запись файлов	\\192.168.10.8\M4\read_4.txt в \\192.168.10.8\M1	Неудачно
		\\192.168.10.8\M4\read_4.txt в \\192.168.10.8\M4	Успешно. Создана копия файла
		\\192.168.10.8\M1\read_1.txt в \\192.168.10.8\M4	Успешно
9.5.	Выполнить вход в систему **ЭВМ6** от имени и с правами пользователя **PC6\UserTest1** и значением мандатной метки **1 (default)**		
9.5.1	Чтение файлов	\\192.168.10.8\M1\read_1.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\192.168.10.8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
10	**Просмотр событий аудита**		
10.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**		Загрузка рабочего стола

10.2	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ8. Нажать кнопку «**Выполнить запрос»**	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

Критерии оценки

Испытания механизма сопоставления классификационных меток каждого субъекта и каждого объекта считаются успешными, если результатами проверок подтверждено, что:

- средства СЗИ обеспечивают назначение классификационных меток (уровней конфиденциальности) пользователям, а также сетевым ресурсам (каталогам) с помощью меток конфиденциальности;
- СЗИ обеспечивают управление потоками информации (при работе с объектами доступа, расположенными на сетевой рабочей станции) на основе сопоставления меток конфиденциальности (субъект получает доступ к объекту по чтению, если его метка больше или равна метке объекта; субъект получает доступ к объекту по записи, если его метка не больше метки объекта);
- СЗИ реализует мандатный механизм контроля доступа к защищаемым ресурсам для всех пользователей СЗИ и ОС;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым локальным объектам.

1.2 Проверка очистки памяти

1.2.1 Проверка возможности очистки внешней памяти

Описание функции

В СЗИ «Блокхост-Сеть 3» очистка внешней памяти выполняется модулем диспетчера доступа и гарантированного удаления. При попытке удаления поставленного на контроль гарантированного удаления файла диспетчер доступа запрещает удаление средствами ОС и запускает модуль гарантированного удаления. Модуль гарантированного удаления перехватывает запрос на удаление только при включенной политике в настройках СЗИ от НСД. Поставленные на контроль файлы удаляются путем затирания их содержимого по специальному алгоритму, который исключает считывание остаточной информации на диске после удаления.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.26.

Таблица П4.26 – Действия при проверке очистки внешней памяти

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС ЭВМ2 под именем и с правами пользователя **Admin**	Загрузка ОС. Появление рабочего стола
2	Создать текстовый файл с уникальным именем D:\TestDel.txt. Набрать в указанном файле текст, содержащий следующую тестовую последовательность: Secret File 0xjhqWXpTHWAFhHfjXjGd5fAwrLAbB1XJlE4IsAUYd2tQ1d6gh&8 *(hyrt%4#erj90 Сохранить файл TestDel.txt	Созданный файл D:\TestDel.txt сохранен
3	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность найдена
4	Загрузить серверную консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ2	Открытие консоли администрирования СЗИ
5	Выбрать «**Очистка остаточной информации»** и установить атрибут гарантированного удаления на «**Системный диск»** и «**Не системные диски»**, так же установить атрибут аудит.	Атрибуты гарантированного удаления и аудита установлены
6	Перезагрузить ЭВМ2, выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
7	Произвести удаление тестового файла D:\TestDel.txt (поместить в «Корзину»)	Файл D:\TestDel.txt удален (помещен в «Корзину»)
8	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность найдена
9	Восстановить файл из «Корзины» и удалить с помощью сочетания клавиш **<Shift>+<Del>**	«Корзина» пуста. Файл удален.
10	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность не найдена
11	Перегрузить ЭВМ2, войти в систему под именем и с правами пользователя **Admin**	Загрузка ОС. Появление рабочего стола
12	Создать текстовый файл с уникальным именем D:\TestDel.txt. Набрать в указанном файле текст, содержащий следующую тестовую последовательность: Secret File 0xjhqWXpTHWAFhHfjXjGd5fAwrLAbB1XJlE4IsAUYd2tQ1d6gh&8 *(hyrt%4#erj90 Сохранить файл TestDel.txt	Созданный файл D:\TestDel.txt сохранен
13	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск указанной тестовой последовательности на	Тестовая последовательность найдена

№ п/п	Действия	Ожидаемый результат
	диске D:\	
16	Перезагрузить ЭВМ1, выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
17	Произвести удаление тестового файла D:\TestDel.txt (поместить в «корзину»)	Файл D:\TestDel.txt удален (помещен в «Корзину»)
18	Очистить корзину	«Корзина» пуста. Файл TestDel.txt удален.
19	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность не найдена
20	Выполнить вход в систему ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
21	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос»**	Появление сообщений, фиксирующих успешные попытки доступа к контролируемому объекту
22	Выполнить указанные в пунктах 1 – 21 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если в области физического размещения удаленного файла не содержится информация, которая была в файле до его удаления, а само гарантированное удаление происходит в случаях, когда пользователь удаляет файл мимо «корзины» или, когда файл был помещен в корзину, а потом произведена очистка корзины.

1.2.2 Проверка очистки оперативной памяти

Описание функции

Очистка оперативной памяти выполняется с целью удаления остаточной информации после работы контролируемого процесса.

Модуль очистки оперативной памяти контролирует завершение определенных (критических) процессов, поставленных на контроль, и после их завершения производит очистку всей свободной физической памяти путем обнуления ее содержимого.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.27.

Таблица П4.7 – Действия при проверке очистки оперативной памяти

№ п/п	Действия	Ожидаемый результат
1	**Настройка механизма очистки оперативной памяти**	
1.1	Войти в систему ЭВМ1 под именем и с правами пользователя **Admin**	Загрузка ОС. Появление рабочего стола
1.2	Запустить консоль администрирования СЗИ»	Открытие консоли администрирования СЗИ
1.3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Очистка остаточной информации»**. Включить механизм очистки памяти, выбрав пункт «**Включить очистку памяти»**	Отображение произведенных настроек в **Основной панели настроек клиентов**
1.4	В **Основной панели настроек клиентов** перетащить мышью из Списка объектов файловой системы в Список контролируемых объектов тестовое приложение C:\CheckMemoryCleaner.exe, после завершения которого будет выполняться очистка памяти (или добавить на контроль необходимое приложение с помощью кнопки «**Добавить»**). Для фиксации событий, связанных с очисткой памяти приложением C:\CheckMemoryCleaner.exe, включить параметр «**Аудит»** для контролируемого процесса.	Появление выбранного процесса в Списке контролируемых объектов в **Основной панели настроек клиентов**
1.5	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Новые настройки сохраняются в базе данных СЗИ.
2	**Проверка механизма очистки памяти**	
2.1	В свойствах компьютера ЭВМ2 «**Панель управления» → «Система» → «Дополнительные параметры системы» → «Дополнительно» → «Загрузка и восстановление» → «Параметры»** установить параметры сохранения полного дампа памяти при крахе системы на диск D:	Параметры установлены
2.2	Перезагрузить ЭВМ2, выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
2.3	Запустить приложение C:\CheckMemoryCleaner.exe	Открытие диалогового окна приложения
2.3	В окне приложения указать длину блока в байтах и путь к файлу C:\test_message.txt для записи фрагмента и нажать кнопку «**Генерировать»**. Указанный файл и дамп памяти обязательно необходимо сохранить на разных дисковых пространствах	Запись тестового фрагмента в оперативную память и в файл по указанному пути
2.4	Открыть диспетчер задач и найти в отображаемых процессах: 1) контролируемый процесс CheckMemoryCleaner.exe; 2) процесс механизма очистки памяти GIS.Client.MemoryCleaner.exe; В открытом диалоговом окне контролируемого приложения нажать кнопку «**Завершить программу»**,	Создан файл C:\test_message.txt Изменение в диспетчере задач показателя загрузки центрального процессора, происходящего в результате работы механизма очистки памяти

№ п/п	Действия	Ожидаемый результат
	при этом следить в диспетчере задач за процессом механизма очистки памяти и дождаться его завершения	
2.5	Запустить приложение NotMyFault.exe для выполнения критической ошибки системы	Появление синего экрана. Перезагрузка операционной системы
2.6	Открыть файл C:\test_message.txt	Открытие файла
2.7	Запустить программное средство **TERRIER 3.0** (**WinHex**)	Открытие диалогового окна программного средства **TERRIER 3.0** (**WinHex**)
2.8	Выполнить с помощью программного средства **TERRIER 3.0** (**WinHex**) поиск на диске D:\ фрагмента тестового файла C:\test_message.txt (включая дамп памяти D:\MEMORY.DMP)	Последовательность не найдена
2.9	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих события очистки памяти
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания механизма очистки оперативной памяти считаются успешными, если:

- результатами проверок подтверждено, что средства СЗИ обеспечивают надежную очистку освобождаемых областей оперативной памяти, используемой для хранения защищаемой информации;
- средства СЗИ обеспечивают надежную регистрацию всех процедур очистки памяти.

1.3 Проверка маркировки документов

1.3.1 Проверка наличия и заполнение штампа №1 при выводе на печать документа, содержащего защищаемую информацию

Описание функции

СЗИ должно предусматривать маркировку выводимых на печать конфиденциальных документов. Маркированные документы должны иметь специальный штамп в колонтитуле на страницах печатаемых документов.

Специальный штамп содержит следующие поля:

- дату/время распечатки;
- имя файла документа;
- уровень конфиденциальности документа;

- порядковый номер в формате «текущий номер страницы из общего числа листов»;
- имя пользователя, производившего печать.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.28.

Таблица П4.28 – Действия при проверке наличия и заполнения штампа №1 при выводе на печать документа, содержащего защищаемую информацию

№ п/п	Действия	Ожидаемый результат
1	**Настройка контроля печати**	
1.1	Выполнить вход в систему ЭВМ2 от имени и с правами пользователя **Admin**. Создать документы с произвольным содержимым: C:\print1.doc, C:\print2.doc	Создание документов с указанными именами
1.2	Запустить консоль администрирования СЗИ	Открытие окна консоли администрирования СЗИ
1.3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ2. Отредактировать параметры мандатного механизма – файлу print1.doc присвоить иерархическую мандатную метку **1**, файлу print2.doc – мандатную метку **2**	Успешное сопоставление иерархических мандатных меток документам
1.4	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → «User1»** → «**Контроль печати»**. Включить механизм контроля печати, отметив в «**Основной панели настроек клиентов»** пункт «**Включить контроль печати» и «Полный аудит»**	Успешная настройка параметров механизма контроля печати
1.5	В **Основной панели настроек клиентов** добавить в список процессов, для которых будет осуществляться контроль печати, следующие процессы: - текстовый редактор **Winword** (C:\Program Files\Microsoft Office\Office14\Winword.exe); - приложение **Wordicon.exe** (C:\Program Files\Microsoft Office\Office14\Wordicon.exe); Разрешить печать из приложения **Winword.exe**, установив флажок в поле **Разрешение** напротив приложения и **Колонтитулы**.	Список объектов, печать из которых контролируется СЗИ. Отображение произведенных настроек
1.6	В «**Основной панели настроек клиентов»** нажать кнопку «**Настройки шаблона печати»** В окне **«Редактирование настроек шаблона печати»** выбрать все маркеры, отметив флажками соответствующие поля и ввести необходимые описания.	Отображение окна **«Редактирование настроек шаблона печати»**. Отображение произведенных настроек
1.7	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → «User1»** → «**Монопольный доступ»** и добавить на контроль шаблоны печати:	Отображение произведенных настроек

№ п/п	Действия	Ожидаемый результат
	1) C:\Blockhost\PrintControl\BlockHost.dot; 2) C:\Users\user1\AppData\Roaming\Microsoft\ Шаблоны\Normal.dot	
1.8	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → «User2» → «Контроль печати»**. Включить механизм контроля печати, отметив в «**Основной панели настроек клиентов»** пункт «**Включить контроль печати» и «Полный аудит»**	Успешная настройка параметров механизма контроля печати
1.9	В «**Основной панели настроек клиентов»** добавить в список процессов, для которых будет осуществляться контроль печати, следующие процессы: - текстовый редактор **Winword** (C:\Program Files\Microsoft Office\Office14\Winword.exe); - приложение **Wordicon.exe** (C:\Program Files\Microsoft Office\Office14\Wordicon.exe); Запретить печать из этих приложений – параметр «**Разрешение»** не установлен.	Список объектов, печать из которых контролируется СЗИ. Отображение произведенных настроек
1.10	В «**Основной панели настроек клиентов»** нажать кнопку «**Настройка шаблона печати»** В окне **«Редактирование настроек шаблона печати»** выбрать все маркеры, отметив флажками соответствующие поля и ввести необходимые описания.	Отображение окна **«Редактирование настроек шаблона печати»**. Отображение произведенных настроек
1.11	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → «User2» → «Монопольный доступ»** и добавить шаблоны печати: 1) C:\Blockhost\PrintControl\BlockHost.dot; 2) C:\Users\user2\AppData\Roaming\Microsoft\ Шаблоны\Normal.dot	Отображение произведенных настроек
1.12	Сохранить произведенные в серверной консоли СЗИ настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
2	**Вывод документов на печать**	
2.1	Вход в систему от имени и с правами пользователя **User1** и мандатной меткой **1**	Загрузка рабочего стола
2.2	Включить все макросы в настройках MS Office в пункте меню «**Файл» → «Параметры» → «Центр управления безопасностью» → «Параметры центра управления безопасностью» → «Параметры макросов»**	Успешное включение макросов
2.3	Открыть с помощью приложения **Winword.exe** документ print1.doc и отправить документ на печать	Документ доступен для записи, чтения и печати. В верхнем и нижнем колонтитулах печатного листа отражены данные, указанные при настройке шаблона печати пользователя **User1**

№ п/п	Действия	Ожидаемый результат
2.4	Запустить приложение **Winword.exe** и попытаться открыть файл print2.doc для последующей печати	Невозможность открытия файла print2.doc
2.5	Вход в систему от имени и с правами пользователя **User1** и мандатной меткой **2**	Загрузка рабочего стола
2.6	Открыть с помощью приложения **Winword.exe** документ print1.doc и отправить документ на печать	Документ доступен для чтения и печати. В верхнем и нижнем колонтитулах печатного листа отражены данные, указанные при настройке шаблона печати пользователя **User1**
2.7	Запустить приложение **Winword.exe** и попытаться открыть файл print2.doc для последующей печати	Документ доступен для чтения и печати. В верхнем и нижнем колонтитулах печатного листа отражены данные, указанные при настройке шаблона печати пользователя **User1**
2.8	Вход в систему от имени и с правами пользователя **User2** и мандатной меткой **1**	Загрузка рабочего стола
2.9	Включить все макросы в настройках MS Office в пункте меню «**Файл**» → «**Параметры**» → «**Центр управления безопасностью**» → «**Параметры центра управления безопасностью**» → «**Параметры макросов**»	Успешное включение макросов
2.10	Запустить приложение **Winword.exe** и попытаться открыть файл print2.doc для последующей печати	Невозможность открытия файла print2.doc
2.11	Вход в систему от имени и с правами пользователя **User2** и мандатной меткой **2**	Загрузка рабочего стола
2.12	Запустить приложение **Winword.exe** и попытаться открыть файл print2.doc для последующей печати	Документ доступен для чтения. Запрет печати документа
3	**Просмотр событий аудита**	
3.1	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Отображение сообщений, фиксирующих успешные и неудачные попытки вывода информации на печать
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Требования по маркировке документов считаются выполненными, если результатами проверок подтверждено, что:

- вывод конфиденциальных документов возможен только посредством процессов, включенных в список разрешенных;

- попытки напечатать конфиденциальный документ из других приложений блокируются средствами СЗИ;
- вывод конфиденциальных документов возможен только пользователями, имеющими полномочия на чтение этих документов;
- выводимый документ распечатывается по установленному шаблону и содержит специальный штамп с реквизитами;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками вывода документов на печать.

1.4 Проверка защиты ввода и вывода информации на отчуждаемый физический носитель

1.4.1 Проверка возможности различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»)

Описание функции

СЗИ должно различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»).

Действия

Проверка выполняется на основе действий, выполняемых в п. 1.1.1.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.29.

Таблица П4.29 – Действия при проверке возможности различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»)

№ п/п	Действия	Ожидаемый результат
1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Подключить к ЭВМ 1 USB-носитель	Определение подключенного к ЭВМ 1 USB-носителя средствами ОС
3	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
4	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ1. В окне **«Настройки машины»** выбрать пункт «**Мандатный разграничение»**.	В **Основной панели настроек клиентов** отображаются существующие мандатные метки
5	Создать иерархическую мандатную метку с описанием **4** и значением **4**	Добавление иерархической метки
6	В **Основной панели настроек клиентов** в области Мандатные метки и категории выделить метку **4**	В **Основной панели настроек клиентов** в Списке правил мандатной метки или категории появились объекты, которым присвоена данная мандатная метка, а в Списке объектов файловой системы отображены все ОФН, которым может быть присвоена метка

№ п/п	Действия	Ожидаемый результат
7	Перетащить объект доступа E:\ из Списка объектов файловой системы в Список правил мандатной метки или категории для мандатной метки **4**	Присвоение объекту доступа E:\ иерархической мандатной метки **4**
8	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»	Сохранение настроек
9	Запустить консоль «Системы развертывания и аудита». В окне выбрать «**Мониторинг**» выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос**»	Появление сообщений, фиксирующих изменение настроек

Результаты тестирования

Испытания считаются успешными, если результатами проверки подтверждается функциональная возможность в СЗИ различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»).

1.4.2 Проверка обеспечения соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства

Описание функции

СЗИ должно различать произвольно используемые и идентифицированные (помеченные средствами СЗИ) отчуждаемые физические носители (ОФН), а также пользователей СЗИ и сторонних пользователей разграничивая права на ввод-вывод информации.

В качестве ОФН рассматриваются гибкие диски, USB–диски и т.п. устройства.

В СЗИ должен быть предусмотрен ввод-вывод информации на ОФН для субъекта только в случае если уровень конфиденциальности субъекта меньше или равен иерархической метке «Документы общего пользования» с ключом «1».

Ввод-вывод информации с ОФН должен быть невозможен для субъекта в случае если уровень конфиденциальности субъекта выше иерархической метки «Документы общего пользования» с ключом «1» вне зависимости от назначенной ОФН иерархической метки.

Действия

Субъектами доступа выступают пользователи СЗИ с назначенными иерархическими метками и сторонний пользователь без иерархической метки.

Пользователю UserTest1мандатная метка равная «1» назначается СЗИ по умолчанию (Default).

Сторонний пользователь UserTest2 создаётся средствами ОС Windows и не является пользователем СЗИ, которому невозможно задать мандатную метку как для субъекта доступа.

Объектами доступа являются ОФН и файловые объекты с различными

иерархическими мандатными метками.

ОФН с буквой диска H:\ и именем «Flash Drive3» является произвольно используемым, которому мандатная (иерархическая) метка не назначается.

Файлу Test.txt находящемуся в папке D:\test_label\ не задается мандатная метка как для объекта доступа.

Иерархические метки для субъектов и объектов доступа назначаются в соответствии с таблицей П4.30.

Таблица П4.30 – Матрица доступа к ОФН

СУБЪЕКТЫ		**ОБЪЕКТЫ**						
		МНИ (ОФН)				**Файловые объекты**		
	Буква диска (путь)	**A:**	**F:**	**G:**	**H:**	**D:\Test_Label**		
	Имя носителя	**НГМД**	**Flash Drive1**	**Flash Drive2**	**Flash Drive3**		**Имя файла**	
	Мандатная метка	**1**	**2**	**3**	**(**Default)			**Мандатная метка**
User1		RW	–	–	RW	RW	Test.txt	
	1	RW	–	–	RW	RW	Test1.txt	**1**
		–	–	–	–	–	Test2.txt	**2**
		–	–	–	–	–	Test3.txt	**3**
User2		–	–	–	–	R	Test.txt	
		–	–	–	–	R	Test1.txt	**1**
	2	–	–	–	–	RW	Test2.txt	**2**
		–	–	–	–	–	Test3.txt	**3**
User3		–	–	–	–	R	Test.txt	
		–	–	–	–	R	Test1.txt	**1**
		–	–	–	–	R	Test2.txt	**2**
	3	–	–	–	–	RW	Test3.txt	**3**
UserTest1		RW	–	–	RW	RW	Test.txt	
	1	RW	–	–	RW	RW	Test1.txt	**1**
	(Default)	–	–	–	–	–	Test2.txt	**2**
		–	–	–	–	–	Test3.txt	**3**
UserTest2		RW	–	–	RW	RW	Test.txt	
		RW	–	–	RW	RW	Test1.txt	**1**
		–	–	–	–	–	Test2.txt	**2**
		–	–	–	–	–	Test3.txt	**3**

Дальнейшие действия, выполняемые при проверке, приведены в таблице П4.31 и выполняются после проведенной проверки указанной в таблице П4.15.

Таблица П4.31 – Действия при проверке соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой удаленного объекта при работе с «помеченным» каналом связи

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Загрузить консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ2	Запуск консоли администрирования
3	**Создание объектов файловой системы**	
3.1	Создать каталог D:\test_label\	Создан каталог
3.2.	Создать файлы: 1) D:\test_label\Test1.txt; 2) D:\test_label\Test 2.txt; 3) D:\test_label\Test 3.txt	Созданы файлы: 1) D:\test_label\Test1.txt; 2) D:\test_label\Test 2.txt; 3) D:\test_label\Test 3.txt
4	**Определение иерархического классификационного уровня мандатных меток для объектов доступа**	
4.1.	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем «**Документы общего пользования»**	В области Список правил мандатной метки отображается список ресурсов, сопоставленных данной метке
4.2.	Перетащить мышью из «Списка объектов файловой системы» ЭВМ2 в область «Список правил мандатной метки или категории»: - устройство, 1) НГМД (A); - файла, 2) D:\test_label\Test1.txt; В области Список правил мандатной метки установить параметр «Аудит»	В области «Список правил мандатной метки или категории» отображается устройство НГМД и файл Test1.txt, сопоставленных данной метке «**1**». Параметр **Аудит** установлен.
4.3.	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем **2**	В области Список правил мандатной метки отображается список ресурсов, сопоставленных данной метке
4.4	Перетащить мышью из «Списка объектов файловой системы» ЭВМ2 в область «Список правил мандатной метки или категории»: - устройство, 1) Flash Drive 1 (F); - файл, 2) D:\test_label\Test2.txt. В области Список правил мандатной метки установить параметр «Аудит»	В области «Список правил мандатной метки или категории» отображается устройство Flash Drive1 и файл Test2.txt сопоставленных данной метке «**2**». Параметр **Аудит** установлен.
4.5.	В «**Основной панели настроек клиентов»** в области Мандатные метки и категории выделить метку с именем **3**	В области Список правил мандатной метки отображается список ресурсов, сопоставленных данной метке
4.6.	Перетащить мышью из «Списка объектов файловой системы» ЭВМ2 в область «Список правил мандатной метки или категории»: - устройство,	В области «Список правил мандатной метки или категории» отображается устройство Flash Drive2 и файл Test3.txt

№ п/п	Действия	Ожидаемый результат
	1) Flash Drive 2 (G); - файл, 2) D:\test_label\Test3.txt. В области Список правил мандатной метки установить параметр «Аудит»	сопоставленных данной метке «**2**». Параметр **Аудит** установлен.
5	**Проверка «Основных настроек клиента»**	
5.1.	В «**Основной панели настроек клиентов»** выделить область «Список пользователей»	Основная панель настроек клиента открыта
5.1.1	Проверка классификационных меток субъектов доступа	Классификационные метки и классификационных уровней субъектов доступа соответствуют указанной в таблице П4.26
5.1.2.	Проверка присвоения субъектам доступа (пользователям) персональных идентификаторов	Субъектам доступа (пользователям) User1, User2, User3, присвоены персональные идентификаторы
5.2.	Проверка способа аутентификации	
5.2.1	Перейти в область «Настройка машины» и раскрыть «Список пользователей» и выполнить следующие действия: 1) выбрать пользователя User1; - перейти в поле «Аутентификация»; - установить параметр «Вход с токеном». 2) выбрать пользователя User2; - перейти в поле «Аутентификация»; - установить параметр «Вход с токеном». 3) выбрать пользователя User3; - перейти в поле «Аутентификация»; - установить параметр «Вход с токеном». 4) выбрать пользователя UserTest1 - перейти в поле «Аутентификация» - установить параметр «Доверять аутентификации Windows»	Субъектам доступа (пользователям) User1, User2, User3 установлен способ аутентификации «Вход с токеном». Пользователю UserTest1 установлен способ аутентификации «Доверять аутентификации Windows». UserTest2 отсутствует в списке пользователей СЗИ
5.3.	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Настройки сохранены
6	**Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа**	
6.1.	Выполнить вход в систему от имени и с правами пользователя **User1 с предъявлением ключевого носителя** и значением мандатной метки **1**	
6.1.1	**Операции с файлом Test.txt**	
	Чтение	D:\test_label\Test.txt — Успешно
	Изменение	D:\test_label\Test.txt — Успешно
	Копирование	D:\test_label\Test.txt копирование на A:\ — Успешно

№ п/п	Действия		Ожидаемый результат
	Копирование	D:\test_label\Test.txt копирование на F:\	Отказ в доступе
	Копирование	D:\test_label\Test.txt копирование на G:\	Отказ в доступе
	Копирование	D:\test_label\Test.txt копирование на H:\	Успешно
6.1.2.	**Операции с файлом Test1.txt**		
	Чтение	D:\test_label\Test1.txt	Успешно
	Изменение	D:\test_label\Test1.txt	Успешно
	Копирование	D:\test_label\Test1.txt копирование на A:\	Успешно
	Копирование	D:\test_label\Test1.txt копирование на F:\	Отказ в доступе
	Копирование	D:\test_label\Test1.txt копирование на G:\	Отказ в доступе
	Копирование	D:\test_label\Test1.txt копирование на H:\	Успешно
6.1.3.	**Операции с файлом Test2.txt**		
	Чтение	D:\test_label\Test2.txt	Отказ в доступе
	Копирование	D:\test_label\Test2.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.1.4.	**Операции с файлом Test3.txt**		
	Чтение	D:\Test_Label\Test3.txt	Отказ в доступе
	Копирование	D:\Test_Label\Test3.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\Test_Label\Test3.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\Test_Label\Test3.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\Test_Label\Test3.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.1.5.	Завершить сеанс пользователя User1.		Появление приглашения для входа в систему
6.2.	Выполнить вход в систему от имени и с правами пользователя **User2 с предъявлением ключевого носителя** и значением мандатной метки **2**		
6.2.1.	**Операции с файлом Test.txt**		
	Чтение	D:\test_label\Test.txt	Успешно
	Изменение	D:\test_label\Test.txt	Неуспешно
	Копирование	D:\test_label\Test.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.2.2.	**Операции с файлом Test1.txt**		
	Чтение	D:\test_label\Test1.txt	Успешно
	Изменение	D:\test_label\Test1.txt	Неуспешно

№ п/п	Действия		Ожидаемый результат
	Копирование	D:\test_label\Test1.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test1.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test1.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test1.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.2.3.	**Операции с файлом Test2.txt**		
	Чтение	D:\test_label\Test2.txt	Успешно
	Изменение	D:\test_label\Test2.txt	Успешно
	Копирование	D:\test_label\Test2.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.2.4.	**Операции с файлом Test3.txt**		
	Чтение	D:\test_label\Test3.txt	Отказ в доступе
	Копирование	D:\test_label\Test3.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.2.5.	Завершить сеанс пользователя User2.		Появление приглашения для входа в систему
6.3.	Выполнить вход в систему от имени и с правами пользователя **User3 с предъявлением ключевого носителя** и значением мандатной метки **3**		
6.3.1.	**Операции с файлом Test.txt**		
	Чтение	D:\test_label\Test.txt	Успешно
	Изменение	D:\test_label\Test.txt	Неуспешно
	Копирование	D:\test_label\Test.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.3.2.	**Операции с файлом Test1.txt**		
	Чтение	D:\test_label\Test1.txt	Успешно
	Изменение	D:\test_label\Test1.txt	Неуспешно
	Копирование	D:\test_label\Test1.txt копирование на A:\	Отказ в доступе (устройство недоступно)

№ п/п	Действия		Ожидаемый результат
	Копирование	D:\test_label\Test1.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test1.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test1.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.3.3.	**Операции с файлом Test2.txt**		
	Чтение	D:\test_label\Test2.txt	Успешно
	Изменение	D:\test_label\Test2.txt	Неуспешно
	Копирование	D:\test_label\Test2.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.3.4.	**Операции с файлом Test3.txt**		
	Чтение	D:\test_label\Test3.txt	Успешно
	Изменение	D:\test_label\Test3.txt	Успешно
	Копирование	D:\test_label\Test3.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.3.5.	Завершить сеанс пользователя User3.		Появление приглашения для входа в систему
6.4.	Выполнить вход в систему от имени и с правами пользователя **UserTest1 без предъявления ключевого носителя и значения мандатной метки, стандартным способом аутентификации**		
6.4.1.	**Операции с файлом Test.txt**		
	Чтение	D:\test_label\Test.txt	Успешно
	Изменение	D:\test_label\Test.txt	Успешно
	Копирование	D:\test_label\Test.txt копирование на A:\	Успешно
	Копирование	D:\test_label\Test.txt копирование на F:\	Отказ в доступе
	Копирование	D:\test_label\Test.txt копирование на G:\	Отказ в доступе
	Копирование	D:\Test_Label\Test.txt копирование на H:\	Успешно
6.4.2.	**Операции с файлом Test1.txt**		
	Чтение	D:\test_label\Test1.txt	Успешно
	Изменение	D:\test_label\Test1.txt	Успешно
	Копирование	D:\test_label\Test1.txt копирование на A:\	Успешно
	Копирование	D:\test_label\Test1.txt копирование на F:\	Отказ в доступе

№ п/п	Действия		Ожидаемый результат
	Копирование	D:\test_label\Test1.txt копирование на G:\	Отказ в доступе
	Копирование	D:\test_label\Test1.txt копирование на H:\	Успешно
6.4.3.	**Операции с файлом Test2.txt**		
	Чтение	D:\test_label\Test2.txt	Отказ в доступе
	Копирование	D:\test_label\Test2.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.4.4.	**Операции с файлом Test3.txt**		
	Чтение	D:\test_label\Test3.txt	Отказ в доступе
	Копирование	D:\test_label\Test3.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.4.5.	Завершить сеанс пользователя UserTest1.		Появление приглашения для входа в систему
6.5.	Выполнить вход в систему от имени и с правами пользователя **UserTest2 стандартным способом аутентификации**		
6.5.1.	**Операции с файлом Test.txt**		
	Чтение	D:\test_label\Test.txt	Успешно
	Изменение	D:\test_label\Test.txt	Успешно
	Копирование	D:\test_label\Test.txt копирование на A:\	Успешно
	Копирование	D:\test_label\Test.txt копирование на F:\	Отказ в доступе
	Копирование	D:\test_label\Test.txt копирование на G:\	Отказ в доступе
	Копирование	D:\test_label\Test.txt копирование на H:\	Успешно
6.5.2.	**Операции с файлом Test1.txt**		
	Чтение	D:\test_label\Test1.txt	Успешно
	Изменение	D:\test_label\Test1.txt	Успешно
	Копирование	D:\test_label\Test1.txt копирование на A:\	Успешно
	Копирование	D:\test_label\Test1.txt копирование на F:\	Отказ в доступе
	Копирование	D:\test_label\Test1.txt копирование на G:\	Отказ в доступе
	Копирование	D:\test_label\Test1.txt копирование на H:\	Успешно
6.5.3.	**Операции с файлом Test2.txt**		
	Чтение	D:\test_label\Test2.txt	Отказ в доступе
	Копирование	D:\Test_label\Test2.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test2.txt копирование на G:\	Отказ в доступе (устройство

№ п/п	Действия		Ожидаемый результат
			недоступно)
	Копирование	D:\test_label\Test2.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.5.4.	**Операции с файлом Test3.txt**		
	Чтение	D:\test_label\Test3.txt	Отказ в доступе
	Копирование	D:\test_label\Test3.txt копирование на A:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на F:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на G:\	Отказ в доступе (устройство недоступно)
	Копирование	D:\test_label\Test3.txt копирование на H:\	Отказ в доступе (устройство недоступно)
6.5.5.	Завершить сеанс пользователя UserTest2.		Появление приглашения для входа в систему
7	**Просмотр событий аудита**		
7.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**		Загрузка рабочего стола
7.2	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос»**		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
7.3	Выполнить указанные в пунктах 1 – 7 действия для рабочих станций ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем		Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания ввода и вывода конфиденциальной информации на отчуждаемые физические носители считаются успешными, если результатами проверок подтверждено, что:

- вывод на отчуждаемые физические носители (запись информации) доступен для субъекта только в случае если уровень конфиденциальности субъекта меньше или равен иерархической метке «Документы общего пользования» с ключом «1»;
- чтение информации с ОФН невозможен для субъекта в случае если уровень конфиденциальности субъекта выше иерархической метки «Документы общего пользования» с ключом «1»;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым ОФН.

1.4.3 Проверка обеспечения соответствия между мандатной меткой защищаемого объекта, помеченного канала связи и субъекта доступа

Описание функции

В СЗИ «Блокхост-Сеть 3» должно обеспечиваться соответствие между мандатной меткой защищаемого объекта, помеченного канала связи и субъекта доступа.

Действия

В линейной схеме процесс проверки можно представить, как последовательность, в которой субъект доступа (пользователь) обращается к объекту доступа (файлу), находящемуся на СВТ, и пытается передать его через помеченный канал связи (сетевую карту) в сетевую папку (рисунок П4.2). Субъекты и объекты доступа, как и канал связи имеют мандатные метки.

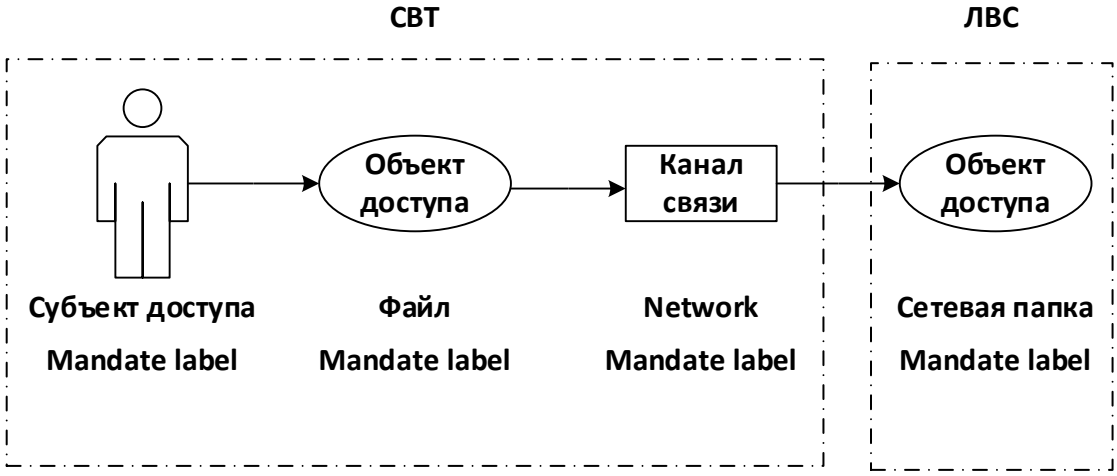

Рисунок П4.2 – Линейная схема процесса проверки

Проверка проводится после действий, описанных в пунктах 1.1.2.6 и 1.1.2.7.

Пользователи User1 и User2 подключаются с ЭВМ 7. На ЭВМ7 создаются для каждого пользователя текстовые файлы с мандатными метками и категориями.

Доступность сетевых ресурсов и файлов, находящихся локально, не проверяется, т.к. она была проверена в предыдущих проверках.

Схема подключения пользователей представлена на рисунке П4.3.

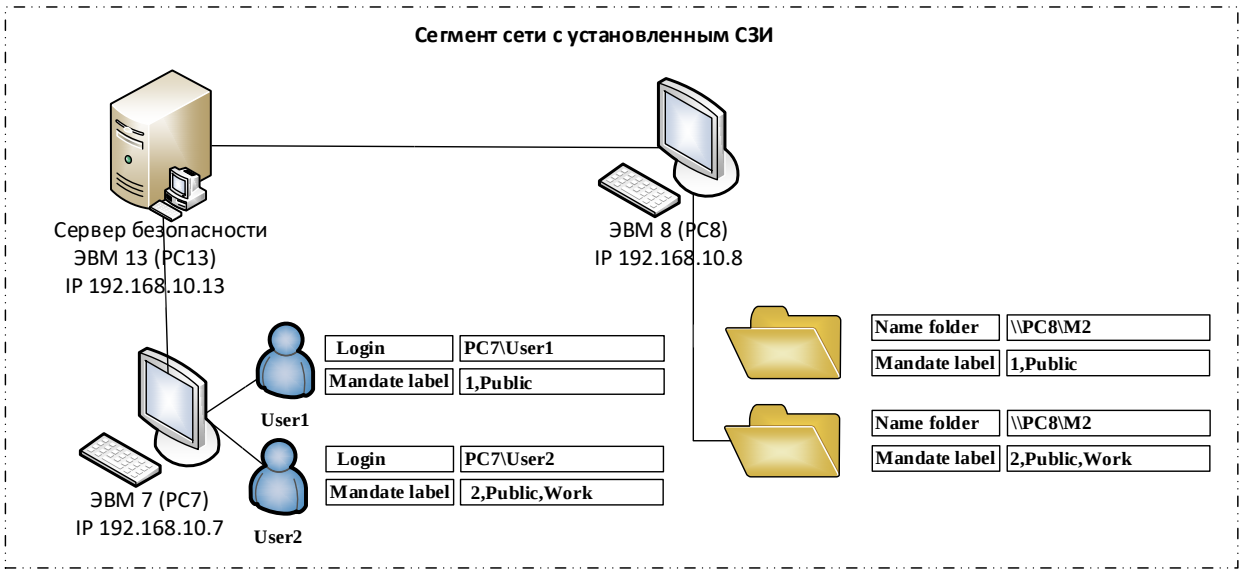

Рисунок П4.3– Схема подключения пользователей к сетевым папкам

Тестирование мандатного механизма разграничения доступа проводится на основе разработанной матрицы разграничения доступа, представленной в таблице П4.32.

Таблица П4.32 – Матрица разграничения доступа к сетевым ресурсам

ЭВМ	СУБЪЕКТЫ	ОБЪЕКТЫ			
		Файл	**Сетевая карта** (Network)	**Сетевая папка \\PC8\M1**	**Сетевая папка \\PC8\M2**
			мандатная метка	мандатная метка	мандатная метка
			1	**1**	**2**
			Категория	Категория	Категория
			Public	**Public**	**Public, Work**
ЭВМ7	**GIS\User1**	**read_1.txt**	**Connect**	RW	-
	мандатная метка = **1, Public**	мандатная метка = **1, Public**			
	GIS\User2	**read_2.txt**	**Disconnect**	-	-
	мандатная метка = **2, Public, Work**	мандатная метка = **2, Public, Work**			

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.33.

Таблица П4.33 – Действия при проверке соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой удаленного объекта при работе с «помеченным» каналом связи

№ п/п	Действия	Ожидаемый результат
1	Создание объектов файловой системы	
1.1.	Войти в систему ЭВМ 7 от имени и с правами «Администратор» и создать текстовые файлы read_1.txt и read_2.txt	Файлы созданы
2	Установка мандатных меток	
2.1	Войти в систему ЭВМ 13 от имени и справами «Администратор» и выполнить следующие действия: Запустить консоль администрирования СЗИ • выбрать ЭВМ 7 и через опцию «Мандатное разграничение» установить для сетевой карты «Network:\» мандатные метки согласно приведенным в таблице П4.31; • установить мандатные метки для созданных текстовых файлов read_1.txt и read_2.txt мандатные метки согласно приведенным в таблице П4.31;	Присвоены соответствующие мандатные метки и категории
3	Проверка соответствия выводимого объекта через помеченный канал связи	
3.1	Войти в систему ЭВМ 7 от имени и с правами пользователя USER1, по токену, с мандатной меткой «1» и с категорией «Public»	Загрузка рабочего стола
3.1.1	Открыть сетевую папку **\\PC8\M1** и скопировать в неё файл read_1.txt	Сетевая папка **доступна** и файл скопирован.

3.1.2	Открыть файл read_1.txt, внести в него изменения и сохранить его	Файл read_1.txt сохранён с изменениями
3.2.	Войти в систему ЭВМ 7 от имени и с правами пользователя USER2, по токену, с мандатной меткой «2» и с категорией «Public, Work»	Загрузка рабочего стола
3.2.1	Открыть сетевую папку **\\PC8\M1**	Сетевая папка **не доступна**
3.2.2	Открыть сетевую папку **\\PC8\M2**	Сетевая папка **не доступна**

Результаты тестирования

Проверка считается успешной, если СЗИ обеспечивает соответствие между мандатной меткой защищаемого объекта, помеченного канала связи и субъекта доступа.

1.4.4 Проверка возможности изменения в назначении и разметке устройств только под контролем СЗИ «Блокхост-Сеть 3»

Описание функции

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем СЗИ «Блокхост-Сеть 3».

Действия

Проверка выполняется на основании действий, выполняемых в п. 1.1.1.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.34.

Таблица П4.34 – Действия при проверке возможности изменения в назначении и разметке устройств только под контролем СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
1	Подключить к ЭВМ1 USB-накопитель	Идентификация накопителя средствами ОС
1.1	Подключить к ЭВМ1 дискету 3,5”	Определение носителя средствами ОС
2	Выполнить на ЭВМ1 вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
3	Попытка запуска консоли администрирования СЗИ	Неудачно
4	Выполнить вход в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
5	Попытка запуска консоли администрирования СЗИ	Успешно
6	В консоли администрирования СЗИ в окне **«Список машин»** выбрать с ЭВМ1, в окне **«Настройки машины»** выбрать пункт «**Мандатное разграничение»**.	Появление в **Основной панели настроек клиентов** параметров мандатного разграничения
7	Создать мандатную метку **4**. Присвоить мандатную метку **4** подключенному к ЭВМ1 • USB-накопителю; • дискете 3,5”	Метка успешно присвоена накопителям
8	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить»**	Сохранение настроек СЗИ
9	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
10	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос»**	Появление сообщений, фиксирующих изменение настроек

Результаты тестирования

Испытания считаются успешными, если изменения в назначении меток конфиденциальности устройствам и каналам осуществляется только под контролем СЗИ «Блокхост-Сеть 3».

1.5 Проверка сопоставления пользователя с устройством

1.5.1 Проверка возможности обеспечить вывод информации на запрошенное пользователем устройство

Описание функции

СЗИ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки). Разграничение прав доступа к портам (COM, LPT, USB) подразумевает разрешение или запрет на использование порта. Настройки данного механизма вступают в силу только после перезагрузки ОС. Для USB-портов допускается привязка к пользователям разрешенных для использования на ЭВМ USB-накопителей.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.35.

Таблица П4.35 – Действия при проверке возможности обеспечить вывод информации на запрошенное пользователем устройство

№ п/п	Действия	Ожидаемый результат
1	**Добавление пользователей в базу данных СЗИ**	
1.1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Запуск консоли администрирования СЗИ
1.2	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выделить параметр «**Список пользователей»**. Добавить в список пользователей СЗИ учетные записи пользователей **User1** – **User6** (если они отсутствуют в базе данных СЗИ)	Добавление пользователей в базу данных СЗИ
2	**Задание ПРД устройствам и портам ЭВМ1**	

<table>
<tr><th>№ п/п</th><th>Действия</th><th>Ожидаемый результат</th></tr>
<tr><td>2.1</td><td>Создание матрицы ПРД
<table>
<tr><th rowspan="2">Пользователь</th><th colspan="4">Устройства/Порты</th></tr>
<tr><th>CD/DVD</th><th>LPT</th><th>COM</th><th>USB</th></tr>
<tr><td>User1</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>User2</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>User3</td><td>-</td><td>-</td><td>-</td><td>+</td></tr>
<tr><td>User4</td><td>-</td><td>-</td><td>+</td><td>-</td></tr>
<tr><td>User5</td><td>-</td><td>+</td><td>-</td><td>-</td></tr>
<tr><td>User6</td><td>+</td><td>-</td><td>-</td><td>-</td></tr>
</table></td><td>Определение матрицы ПРД</td></tr>
<tr><td>2.2</td><td>В консоли администрирования СЗИ в окне «Настройки машины» раскрыть дерево «Список пользователей» → User1 → «Контроль портов и CD».
В «Основной панели настроек клиента» для пользователя User1 установить ПРД к портам и CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.</td><td>Появление в «Основной панели настроек клиента» текущих ПРД.

Отображение ПРД пользователя User1</td></tr>
<tr><td>2.3</td><td>В окне «Настройки машины» раскрыть дерево «Список пользователей» → User2 → «Контроль портов и CD».
В «Основной панели настроек клиента» для пользователя User2 установить ПРД к портам и CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.</td><td>Отображение ПРД пользователя User2</td></tr>
<tr><td>2.4</td><td>В окне «Настройки машины» раскрыть дерево «Список пользователей» → User3 → «Контроль портов и CD».
В «Основной панели настроек клиента» для пользователя User3 установить ПРД к портам и CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.</td><td>Отображение ПРД пользователя User3</td></tr>
<tr><td>2.5</td><td>В окне «Настройки машины» раскрыть дерево «Список пользователей» → User4 → «Контроль портов и CD».
В «Основной панели настроек клиента» для пользователя User4 установить ПРД к портам и CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.</td><td>Отображение ПРД пользователя User4</td></tr>
<tr><td>2.6</td><td>В окне «Настройки машины» раскрыть дерево «Список пользователей» →User5 → «Контроль портов и CD».
В «Основной панели настроек клиента» для пользователя User5 установить ПРД к портам и</td><td>Отображение ПРД пользователя User5</td></tr>
</table>

№ п/п	Действия	Ожидаемый результат
	CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.	
2.7	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User6** → «**Контроль портов и CD»**. В «**Основной панели настроек клиента»** для пользователя **User6** установить ПРД к портам и CD-ROM, согласно матрице ПРД (см. п. 2.1), и включить аудит событий, связанных с попытками доступа к контролируемым ресурсам.	Отображение ПРД пользователя **User6**
2.8	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
2.9	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Отображение сообщений, фиксирующих произведенное изменение настроек
2.10	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3	**Проверка доступа пользователей к устройствам и портам ЭВМ2**	
3.1	Выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
3.2	Чтение файла с CD-ROM	Успешно
	Печать на принтере (подключен к LPT-порту)	Успешно
	Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	Чтение/запись информации на подключенное к USB-порту устройство	Успешно
3.3	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.4	Выполнить вход в систему от имени и с правами пользователя **User2**	Загрузка рабочего стола
3.5	Чтение файла с CD-ROM	Неудачно. Устройство отсутствует в списке устройств
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно. Устройство отсутствует в списке устройств
3.6	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.7	Выполнить вход в систему от имени и с правами пользователя **User3**	Загрузка рабочего стола
3.8	Чтение файла с CD-ROM	Неудачно. Устройство отсутствует в списке устройств
	Печать на принтере (подключен к LPT-порту)	Неудачно

№ п/п	Действия	Ожидаемый результат
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Успешно
3.9	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.10	Выполнить вход в систему от имени и с правами пользователя **User4**	Загрузка рабочего стола
3.11	Чтение файла с CD-ROM	Неудачно. Устройство отсутствует в списке устройств
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно. Устройство отсутствует в списке устройств
3.12	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.13	Выполнить вход в систему от имени и с правами пользователя **User5**	Загрузка рабочего стола
3.14	Чтение файла с CD-ROM	Неудачно. Устройство отсутствует в списке устройств
	Печать на принтере (подключен к LPT-порту)	Успешно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно. Устройство отсутствует в списке устройств
3.15	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.16	Выполнить вход в систему от имени и с правами пользователя **User6**	Загрузка рабочего стола
3.17	Чтение файла с CD-ROM	Успешно
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно. Устройство отсутствует в списке устройств
3.18	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
4	**Просмотр событий аудита**	
4.1	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита»

№ п/п	Действия	Ожидаемый результат
4.2	В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если пользователю обеспечен вывод информации:

- на произвольно используемое устройство;
- на идентифицированное устройство.

1.5.2. Проверка механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству

Описание функции

Механизм сопоставления пользователя с устройством, на основе матрицы доступа к портам, реализует явное разрешение или запрет доступа к устройству по его идентифицированному имени, образуя матрицу доступа к устройствам.

Действия

Проверка выполняется согласно и на основании действий, выполненных в п. 1.4.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.36.

Таблица П4.36 – Действия при проверке механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству

№ п/п	Действия	Ожидаемый результат
1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
3	В окне **«Список машин»** выбрать ЭВМ2. В окне **«Настройки машины»** раскрыть дерево **Список пользователей** →**User1** →**Контроль портов и CD**.	Появление в **Основной панели настроек клиентов** всех доступных портов и CD
4	Подключить к USB портам ЭВМ2 два USB-накопителя	Идентификация накопителей

№ п/п	Действия	Ожидаемый результат
		средствами ОС
5	В «**Основной панели настроек клиентов»** раскрыть дерево устройств USB-порта	Отображение в дереве ресурсов всех зарегистрированных USB-устройств
6	В «**Основной панели настроек клиентов»** для пользователя **User1**: - Разрешить работу с обоими подключенными USB-накопителями. - Разрешить работу с COM-портом. - Разрешить работу с LPT-портом (вывод на принтер). - Разрешить работу с CD	Индикация разрешения работы в виде установленной «галочки»
7	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **«User2»** → «**Контроль портов и CD»**.	Появление в **Основной панели настроек клиентов** всех доступных портов и CD
8	В «**Основной панели настроек клиентов»** раскрыть дерево устройств USB-порта	Отображение в дереве ресурсов всех подключенных USB-устройств
9	В «**Основной панели настроек клиентов»** для пользователя **User2**: - Запретить работу с одним из подключенных USB-накопителей. - Разрешить работу с COM портом. - Разрешить работу с LPT портом (вывод на принтер). - Разрешить работу с CD	Индикация разрешения работы в виде установленной «галочки»
10	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
11	Войти в систему ЭВМ2 от имени и с правами пользователя **Admin**	Загрузка рабочего стола
12	Создать файлы C:\iotest1.txt и C:\iotest2.txt с произвольным содержимым	Создание файлов
13	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
14	Войти в систему ЭВМ2 от имени и с правами пользователя **User1**	Загрузка рабочего стола
15	Скопировать файл C:\iotest1.txt на оба USB-накопителя	Успешное копирование файла
16	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
17	Войти в систему от имени и с правами пользователя **User2**	Загрузка рабочего стола
18	Скопировать файл C:\iotest2.txt на оба USB-накопителя	Работа с запрещенным USB-накопителем невозможна
19	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
20	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита»

№ п/п	Действия	Ожидаемый результат
21	В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
22	Выполнить указанные в пунктах 1 – 20 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания механизма сопоставления пользователя с устройствами считаются успешными, если результатами проверок подтверждено, что:

- средства СЗИ обеспечивают идентификацию устройств (накопитель на гибких магнитных дисках, CD/DVD-накопитель, последовательный порт, USB-устройство) по именам;
- средства СЗИ позволяют задавать явные права на доступ для каждой пары «пользователь - устройство доступа» (формировать матрицу доступа к устройствам).

1.6 Проверка механизма идентификации и аутентификации пользователей

1.6.1 Проверка требования от пользователей идентифицировать себя при запросах на доступ и проверка подлинности идентификатора субъекта (аутентификации)

Описание функции

Идентификация и аутентификация пользователя при его доступе в систему предназначена для защиты ЭВМ от загрузки ОС Microsoft Windows незарегистрированным пользователем. Данный механизм предполагает наличие у пользователя уникального регистрационного имени, пароля, ключевого носителя и PIN-кода ключевого носителя. Дополнительно пользователь во время процедуры идентификации и аутентификации вводит классификационный уровень доступа к информации – комбинацию иерархической метки (целое число в диапазоне от 1=низший уровень до 255=высший уровень) и неиерархических категорий.

В СЗИ ведется список разрешенных пользователей для входа в систему, который может быть изменен администратором безопасности. Идентификация и аутентификация пользователей осуществляются только после инициализации механизмов защиты СЗИ. При этом отключена возможность загрузки ОС в защищенном режиме для всех пользователей, за исключением администратора безопасности.

Для идентификации и аутентификации пользователя при его доступе в систему реализованы два способа парольной защиты:

- вход в систему по паролю, вводимому пользователем с клавиатуры;
- вход в систему по ключевому носителю с паролем (пароль в зашифрованном виде хранится на ключевом носителе).

Дополнительно СЗИ обеспечивает возможность двухфакторной аутентификации пользователей средствами СЗИ, при входе в домен Microsoft Active Directory с использованием цифровых сертификатов пользователей, выработанных, в том числе, с использованием российских криптографических алгоритмов (ГОСТ). Сертификаты могут храниться на персональных электронных идентификаторах (ключевых носителях).

Действия

С помощью консоли администрирования в базе данных СЗИ регистрируется группа пользователей с указанной ниже Политикой аутентификации учетных записей, и выполняется последовательность действий, указанных в таблицах П4.37, П4.38, П4.39, для проверки описанных требований.

Таблица П4.37 – Управление учетными записями пользователей в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	**Проверка возможности добавления учетных записей пользователей**	
1.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
1.2	В окне **«Список машин»** выбрать ЭВМ2. В окне **«Настройки машины»** выбрать пункт «**Политика аутентификации»** и установить параметры: Минимальная длина – 8 знаков Пароль должен отвечать требованиям сложности Максимальный срок действия пароля 30 дней Требование изменять минимум 2 знак(ов) при создании новых паролей Запретить использование 2 последних сохраненных паролей Максимальное количество неудачных попыток входа – 3 Блокировать пользователя на 10 минут при превышении максимального количества неудачных попыток входа. Выбрать пункт главного меню «Главная» → **«Сохранить все»**	Успешная настройка **Политики аутентификации**
1.3	В окне **«Настройки машины»** выбрать пункт «**Список пользователей».** Выбрать пункт главного меню «**Управление пользователями»** → **«Добавление пользователей»**.	Появление окна **«Добавление пользователей»**
1.4	Добавить пользователя **User7**, задать пароль пользователя длиной 8 символов и удовлетворяющий требованиям сложности. Добавить пользователя в Список пользователей СЗИ	Успешное добавление пользователя **User7**
1.5	В окне **«Основные настройки клиента»** изменить иерархическую мандатную метку пользователя **User7** на мандатную метку **2**	Успешное изменение иерархической мандатной метки пользователя **User7**.

№ п/п	Действия	Ожидаемый результат
1.6	Добавить пользователя **User8** (мандатная метка **1**). Попытаться задать пароль пользователя длиной 7 символов. Задать пароль длиной 8 символов, удовлетворяющий требованию сложности пароля	Успешное добавление пользователя **User8**, пароль длиной 7 символов не задан. Пароль длиной 8 символов задан.
1.7	Добавить пользователя **User10** (мандатная метка входа **1**). Задать пароль пользователя длиной 9 символов	Успешное добавление пользователя **User10**, пароль задан.
1.8	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»	Сохранение настроек
2	**Проверка возможности изменения имени учетной записи пользователя**	
2.1	В окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. В «**Основной панели настроек клиента»** выделить пользователя **User7** и выбрать пункт меню «**Управление пользователями»** → **«Изменение пользователя»**	Появление окна **«Изменение пользователя»**
2.2	Изменить имя пользователя **User7** на **User8**	Предупреждение о существовании пользователя с именем **User8** в СЗИ – имя пользователя не изменяется
2.3	Изменить имя пользователя на **User9**	Успешное изменение имени пользователя User9.
2.4	Сохранить произведенные настройки, выбрав пункт меню **Главная** →**Сохранить все**	Сохранение настроек
3	**Проверка назначения пользователю ключевого носителя (токена)**	
3.1	Подключить к рабочей станции ЭВМ2 ключевой носитель. В окне **«Список машин»** выбрать ЭВМ2	Отображение ключевого носителя в окне **Токены**
3.2	В окне **«Настройки машины»** выбрать пункт «**Список пользователей»**. В «**Основной панели настроек клиента»** выделить пользователя **User8** и выбрать пункт меню «**Управление пользователями»** → **«Управление носителями».**	Появление окна **«Управление носителями»**
3.3	В окне **«Управление носителями»** выбрать ключевой носитель, ввести PIN-код и сохранить.	Успешное назначение ключевого носителя пользователю
3.4	В окне **«Настройки машины»** выбрать Список пользователей → User8 → Аутентификация и установить «**Вход с токеном».** **Сохранить** произведенные настройки, выбрав пункт меню «**Главная**» → **«Сохранить все»**	Установка Вход с токеном
3.5.	Повторить указанные в п. 3.1 - 3.4. для привилегированной учетной записи (с правами администратор)	Установка Вход с токеном
4	**Проверка событий аудита, фиксирующих изменение настроек СЗИ**	
4.1	Запустить консоль «Системы развертывания и аудита». Выбрать **«Мониторинг»** Выбрать ЭВМ1→ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений аудита, фиксирующих изменение параметров работы СЗИ.

№ п/п	Действия	Ожидаемый результат
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях под управлением всех остальных поддерживаемых операционных систем и с использованием устройств идентификации, приведенных в таблице 6.3.	Совпадение полученных результатов с приведенными выше результатами

Таблица П4.38 – Проверка корректности идентификации и аутентификации пользователя при входе в систему

№ п/п	Действия	Ожидаемый результат
1	**Проверка идентификации и аутентификации пользователей**	
1.1	Выполнить попытку входа в систему ЭВМ2 от имени и с правами несанкционированного пользователя **User11**	Запрет входа в систему
1.2	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: **1) неверный пароль;** 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; 4) верную мандатную метку входа	Запрет входа в систему
1.3	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: 1) верный пароль; **2) неверный идентификатор входа;** 3) верный PIN-код идентификатора входа, зарегистрированного в базе данных СЗИ для данного пользователя; 4) верную мандатную метку входа	Запрет входа в систему
1.4	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: 1) верный пароль; 2) верный идентификатор входа; 3) **неверный** PIN-код идентификатора входа; 4) верную мандатную метку входа	Запрет входа в систему. Ожидание 10 мин.
1.5	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: 1) верный пароль; 2) верный идентификатор входа; **3)** верный PIN-код идентификатора входа; 4) верную мандатную метку входа	Запрет входа в систему

№ п/п	Действия	Ожидаемый результат
1.6	Подождать 10 минут. Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: 1) верный пароль; 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; **4) неверную мандатную метку входа**	Запрет входа в систему
1.7	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User8**. Указать: 1) верный пароль; 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; 4) **верную** мандатную метку входа	Вход в систему
1.8	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
1.9	Выполнить попытку входа в систему ЭВМ2 с правами санкционированного пользователя **User9**. Указать: верный пароль;	Вход в систему
1.10	Назначить User9 ключевой носитель и установить настройку Вход с токеном	Успешное назначение ключевого носителя и установка параметра вход с токеном пользователю User9
1.11	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
1.12	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User9**. Указать: 1) верный пароль; 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; 4) верную **мандатную метку** входа, равную **2**	Вход в систему
1.13	Выполнить попытку входа в систему ЭВМ2 от имени и с правами санкционированного пользователя **User9**. Указать: 1) верный пароль; 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; 4) неверную **мандатную метку** входа, равную **3**	Запрет входа в систему
1.13.1	Выполнить действия, указанные в п. 1.12 для **привилегированной** учетной записи (с правами администратора)	Вход в систему
1.14	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования сервера СЗИ	Открытие консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1.15	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
1.16	Выполнить указанные в пунктах 1.1 – 1.15 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
2	**Проверка возможности изменения пароля пользователями без привлечения администратора безопасности СЗИ**	
2.1	Войти в систему ЭВМ2 от имени и с правами пользователя **User9** на рабочей станции ЭВМ2	Загрузка рабочего стола
2.2	Нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**	Появление диалога выбора действий ОС Windows
2.3	Нажать ссылку «**Сменить пароль»**.	Появление диалога **«Смена пароля»**
2.4	Заполнить поля диалога: - в поле ввода «**Старый пароль»** ввести текущий пароль; - в поле ввода «**Новый пароль»** ввести новый пароль (длиной 7 символов); - повторить ввод нового пароля в поле ввода «**Подтвердите пароль»**; - в поле ввода **PIN-код** ввести PIN-код доступа к ключевому носителю. Нажать кнопку «**Применить»** для запуска процедуры изменения пароля.	Появление сообщения с описанием ошибки смены пароля.
2.5	Нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**	Появление диалога выбора действий ОС Windows
2.6	Нажать ссылку «**Сменить пароль»**.	Появление диалога **«Смена пароля»**
2.7	Заполнить поля диалога: - в поле ввода «**Старый пароль»** ввести текущий пароль; - в поле ввода «**Новый пароль»** ввести новый пароль (длиной 8 символов, но не удовлетворяющий сложности пароля: Буквы\цифры\спец символы); - повторить ввод нового пароля в поле ввода «**Подтвердите пароль»**; - в поле ввода **PIN-код** ввести PIN-код доступа к ключевому носителю. Нажать кнопку «**Применить»** для запуска процедуры изменения пароля.	Появление сообщения с описанием ошибки смены пароля.
2.8	Заполнить поля диалога: - в поле ввода «**Старый пароль»** ввести текущий пароль; - в поле ввода «**Новый пароль»** ввести новый пароль (длиной 8 символов и удовлетворяющий сложности пароля);	Пароль изменен. Загрузка рабочего стола.

№ п/п	Действия	Ожидаемый результат
	- повторить ввод нового пароля в поле ввода «**Подтвердите пароль»**; - в поле ввода **PIN-код** ввести PIN-код доступа к ключевому носителю. Нажать кнопку «**Применить»** для запуска процедуры изменения пароля.	
2.9	Нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**	Появление диалога выбора действий ОС Windows
2.10	Нажать ссылку «**Сменить пароль»**.	Появление диалогового окна **«Смена пароля»**
2.11	Заполнить поля диалога: - в поле ввода «**Старый пароль»** ввести текущий пароль - в поле ввода «**Новый пароль»** ввести новый пароль (длиной 9 символов и удовлетворяющий сложности пароля); - повторить ввод нового пароля в поле ввода «**Подтвердите пароль»**; - в поле ввода **PIN-код** ввести PIN-код доступа к ключевому носителю. Нажать кнопку «**Применить»** для запуска процедуры изменения пароля.	Пароль изменен. Загрузка рабочего стола.
2.12	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
2.13	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием пароля длиной 7 символов	Вход в систему невозможен
2.14	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием старого пароля длиной 8 символов	Вход в систему невозможен
2.15	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием нового пароля длиной 9 символов (измененного через диалог **«Смена пароля»**)	Успешный вход пользователя в систему
2.16	Перезагрузить ЭВМ1	Перезагрузка ЭВМ1
2.17	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования сервера СЗИ	Открытие консоли администрирования СЗИ
2.18	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
2.19	Выполнить указанные в пунктах 2.1 – 2.18 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
3	**Проверка возможности изменения пароля пользователя администратором безопасности СЗИ**	
3.1	В консоли администрирования СЗИ в окне	В **Основной панели настроек клиентов**

№ п/п	Действия	Ожидаемый результат
	«Настройки машины» выбрать пункт «**Список пользователей»**	отображается список пользователей СЗИ
3.2	В «**Основной панели настроек клиентов»** выделить пользователя **User10**, в главном меню выбрать пункт «**Управление пользователями»** → **«Изменение пароля»**.	Появление окна **«Изменение пароля пользователя»**
3.3	В появившемся окне **«Изменение пароля пользователя»** ввести новый пароль его и подтверждение, нажать кнопку «**Изменить»**	Пароль пользователя изменен
3.4	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
3.5	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
3.6	Попытаться войти в систему ЭВМ2 от имени и с правами пользователя **User10** с указанием старого пароля	Вход в систему невозможен
3.7	Попытаться войти в систему ЭВМ2 от имени и с правами пользователя **User10** с указанием нового пароля (измененного через диалоговое окно серверной консоли СЗИ **«Изменение пароля пользователя»**)	Успешный вход пользователя в систему
3.8	Перезагрузить ЭВМ1	Перезагрузка ЭВМ1
3.9	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования сервера СЗИ	Открытие консоли администрирования СЗИ
3.10	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «Выполнить запрос**».**	Появление сообщений, фиксирующих смену PIN-кода и входа в систему
3.11	Выполнить указанные в пунктах 3.1 – 3.10 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
4	**Проверка возможности изменения PIN-кода идентификаторов входа пользователей администратором безопасности СЗИ**	
4.1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
4.2	Подключить ключевой носитель пользователя к ЭВМ2	Идентификация ключевого носителя средствами ОС ЭВМ1
4.3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ1, в окне **«Токены»** раскрыть дерево типа ключевого носителя и выбрать необходимый ключевой носитель.	Появление окна ввода PIN-кода носителя
4.4	В окно ввода PIN-кода ввести текущий PIN-код доступа к ключевому носителю и нажать кнопку **Вход**.	В **Основной панели настроек клиентов** отображаются параметры идентификатора входа
4.5	Для смены PIN-кода нажать кнопку «**Сменить PIN-код»**, в открывшемся окне смены PIN-кода вести	Успешная смена PIN-кода

№ п/п	Действия	Ожидаемый результат
	новый PIN-код и нажать кнопку «**Изменить**»	
4.6	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»	Сохранение настроек
4.7	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
4.8	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием старого PIN-кода	Вход в систему невозможен
4.9	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием нового PIN-кода	Успешный вход пользователя в систему
4.10	Перезагрузить ЭВМ1	Перезагрузка ЭВМ1
4.11	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования сервера СЗИ	Открытие консоли администрирования СЗИ
4.12	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «Выполнить запрос**».**	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
4.13	Повторить пункты 4.1 – 4.12 для всех поддерживаемых в СЗИ идентификаторов входа	Совпадение полученных результатов с приведенными выше результатами
4.14	Выполнить указанные в пунктах 4.1 – 4.13 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
5	**Проверка возможности изменения PIN-кода идентификаторов входа пользователей при входе в систему с включенными политиками PIN-кода**	
5.1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
5.2	Подключить ключевой носитель пользователя к ЭВМ2	Идентификация ключевого носителя средствами ОС ЭВМ1
5.3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ1, в окне **«Токены»** раскрыть дерево типа ключевого носителя и выбрать необходимый ключевой носитель.	Появление окна ввода PIN-кода носителя
5.4	В окно ввода PIN-кода ввести текущий PIN-код доступа к ключевому носителю и нажать кнопку «**Вход**».	В **Основной панели настроек клиентов** отображаются параметры идентификатора входа
5.5	Установить галочку на параметре **Принудительная смена PIN-кода**	Параметр смены PIN-кода установлен
5.6	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Политика аутентификации»** и установить политику PIN-кода: Минимальная длина – 8 знаков Пароль должен отвечать требованиям сложности	Успешная настройка **Политики аутентификации**
5.7	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → «**Сохранить все**»	Сохранение настроек

№ п/п	Действия	Ожидаемый результат
5.8	Повторить пункты 5.2 – 5.6 для всех поддерживаемых в СЗИ идентификаторов входа	Совпадение полученных результатов с приведенными выше результатами
5.9	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
5.10	Попытаться войти в систему на ЭВМ2 от имени и с правами пользователя **User9** с указанием правильного PIN-кода	Появление сообщения о необходимости смены PIN-кода
5.11	Заполнить поля диалога: Правильный старый PIN код Новый и его подтверждение не удовлетворяющий политикам PIN-кода	Появление сообщения с описанием ошибки смены PIN-кода
5.12	Заполнить поля диалога: Правильный старый PIN код, новый, удовлетворяющий политикам, и его подтверждение	Смена PIN-кода и вход в систему
5.13	Запустить на ЭВМ1 консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «Выполнить запрос**».**	Появление сообщений, фиксирующих смену PIN-кода и входа в систему
6	**Проверка возможности удаления учетной записи пользователя**	
6.1	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
6.2	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Список пользователей»**	В «**Основной панели настроек клиентов»** отображается список пользователей СЗИ
6.3	В «**Основной панели настроек клиентов»** в списке пользователей выделить пользователя **User10**, в главном меню выбрать пункт «**Управление пользователями» → «Удаление из настроек»**	Появление сообщения подтверждения удаления пользователя из СЗИ
6.4	Подтвердить удаление пользователя	Пользователь удален из СЗИ
6.5	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранит все»**	Сохранение настроек
6.6	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
6.7	Попытаться войти в систему ЭВМ2 от имени и с правами пользователя **User10**	Вход в систему невозможен
6.8	Перезагрузить ЭВМ1	Перезагрузка ЭВМ1
6.9	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
6.10	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
7	**Проверка возможности временного ограничения на вход пользователей в систему**	

№ п/п	Действия	Ожидаемый результат
7.1	В консоли администрирования СЗИ в окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User9** выбрать пункт «**Ограничение по времени»**.	В «**Основной панели настроек клиентов»** отображаются настройки механизма временного контроля
7.2	Установить параметры «**Включить временные ограничения»**, **«Вести аудит временных разрешений»** и установить разрешение на работу в текущий день недели с 08:00 до текущего часа	Успешное задание настроек
7.3	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
7.4	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
7.5	Попытаться войти в систему от имени и с правами пользователя **User9**	Вход в систему невозможен
7.6	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
7.7	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User9** выбрать пункт «**Ограничение по времени»**.	В «**Основной панели настроек клиентов»** отображаются настройки механизма «**Ограничение по времени»**
7.8	Установить разрешение на работу по средам с 08:00 до 20:00	Успешное изменение настроек
7.9	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
7.10	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
7.11	Попытаться войти в систему ЭВМ2 от имени и с правами пользователя **User9**	Успешный вход пользователя в систему
7.12	Перезагрузить ЭВМ1	Перезагрузка ЭВМ1
7.13	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
7.14	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2, нажать кнопку «**Выполнить запрос».**	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
7.15	Выполнить указанные в пунктах 7.1 – 7.14 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами
8.	**Проверка входа в систему пользователем используя группы AD**	
8.1	Войти в систему ЭВМ2 пользователем домена	Вход в систему невозможен
8.2	Войти в систему ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
8.3	Добавить группу AD Пользователи домена (Domain	Группа AD добавлена

№ п/п	Действия	Ожидаемый результат
	Users)	
8.4	Перезагрузить ЭВМ2	Перезагрузка ЭВМ2
8.5	Войти в систему ЭВМ2 пользователем домена	Успешный вход пользователя в систему
8.6	Запустить на ЭВМ1 консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2, нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих попытки входа в систему
8.7	Выполнить указанные в пунктах 8.1 – 8.6 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Таблица П4.39 – Проверка возможности аутентификации пользователей с использованием цифровых сертификатов

№ п/п	Действия	Ожидаемый результат
1	**Настройка центра сертификации**	
1.1	ЦС настраивается в соответствии с п. 1.4	Доступа веб-страница ЦС http://ser2008ad/certsrv
2	**Получение сертификата пользователя**	
2.1.	Войти в систему ЭВМ 2 от имени и с правами пользователя User1 в домен GIS.LAN	Рабочий стол загружен
2.2	Запросить сертификат http://ser2008ad/certsrv и загрузить его в идентификатор	Сертификат пользователя загружен в идентификатор
2.3	Выйти из ОС	
3	**Установка варианта аутентификации пользователя**	
3.1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
3.2	В консоли администрирования выполнить следующие действия: 1) В окне списка машин выбрать ЭВМ2; 2) В списке пользователей выбрать пользователя User1; 3) Перейти в меню «Аутентификация»; 4) Установить параметр «Вход с токеном»; 5) Нажать кнопку «Сохранить все».	Вариант аутентификации «Вход с токеном» пользователю User1 установлен
4	**Авторизация пользователя с использованием цифрового сертификата**	
4.1	Войти в систему ЭВМ 2 от имени и с правами пользователя User1 в домен GIS.LAN	Рабочий стол загружен
4.2.	Выйти из ОС	
5	**Отзыв сертификата пользователя**	
5.1.	Войти в систему ЭВМ 1 от имени и с правами пользователя Admin в сервер контролера домена GIS.LAN	Рабочий стол загружен

№ п/п	Действия	Ожидаемый результат
5.2.	Загрузить «Центр сертификации» перейдя по ветке «Пуск» - «Все программы» – «Администрирование» – «Центр сертификации»	Оснастка «Центра сертификации» загружена
5.3.	Выбрать сертификат пользователя User1 перейдя по ветке «Центр сертификации» - «GIS-SER2008AD-CA» - «Выданные сертификаты»	Сертификат пользователя User1 выбран
5.4.	Через контекстное меню выбрать команды «Все задачи» - «Отзыв сертификата»	Сертификат пользователя User1 отозван
6	**Авторизация пользователя с использованием цифрового сертификат отозванного в ЦС**	
6.1.	Войти в систему ЭВМ 2 от имени и с правами пользователя User1 в домен GIS.LAN	Отказ в доступе
7	**Проверка регистрации событий безопасности**	
7.1.	Войти в систему ЭВМ1 пользователем домена	Успешный вход пользователя в систему
7.2.	Запустить на ЭВМ1 консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2, нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих попытки входа в систему
7.3.	Выполнить указанные в пунктах 1 – 7 действия на рабочих станциях ЭВМ 2 – ЭВМ 5 для всех установленных операционных систем и с идентификаторами, указанными в таблице 6.3	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Результаты проверки считаются положительным, если:

- при вводе верного имени пользователя, зарегистрированного в системе, предъявлении назначенного ключевого носителя, верного пароля и мандатной метки осуществляется вход в систему;
- при вводе незарегистрированного имени пользователя, при предъявлении незарегистрированного ключевого носителя или ввода неверного пароля появляется приглашение вновь предъявить права на вход в систему, а в случае превышения максимального количества попыток входа, установленного в политике аутентификации, вход в систему для пользователя блокируется, и система перезагружается;
- СЗИ блокирует возможности обхода процедуры идентификации;
- СЗИ обеспечивает надежную регистрацию всех событий, связанных с попытками идентификации и аутентификации;
- СЗИ предоставляет пользователю сменить пароль или PIN-код к персональному идентификатору самостоятельно, при установке такого требования администратором безопасности;
- администратор безопасности может установить временное ограничение на вход пользователя в систему;
- СЗИ блокирует возможность задания пароля пользователя длиной менее установленной в политике безопасности;

- СЗИ обеспечивает возможность двухфакторной аутентификации пользователей средствами СЗИ при входе в ОС Windows с использованием цифровых сертификатов пользователей. Сертификаты могут храниться на персональных электронных идентификаторах eToken, SafeNet eToken, ruToken, JaCarta, ESMART Token и Avest Token;

1.6.2 Проверка возможности надежно связывать полученную идентификацию со всеми действиями данного пользователя

Описание функции

СЗИ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

Действия

Проверка выполняется на основании действий, выполняемых в п.п. 1.1.1.1, 1.1.2.1 и 1.6.1 и проверки содержания необходимой информации о действиях пользователя.

Результаты тестирования

Проверка считается успешной, если СЗИ обладает способностью надежно связывать полученную идентификацию со всеми действиями пользователя.

1.7 Проверка механизма регистрации событий

1.7.1 Проверка регистрации событий использования идентификационного и аутентификационного механизмов

Описание функции

Регистрация использования идентификационного и аутентификационного механизма включает внесение в журнал всех событий, связанных с попытками аутентификации.

Действия

Проверка выполняется на основании действий, выполненных в п. 1.6.1 и путем проверки журнала, содержащего информацию об идентификации и аутентификации пользователей (дата и время, субъект, тип события, успешно ли осуществилось событие).

Результаты тестирования

Результаты проверки считаются положительными, если СЗИ обеспечивает надежную регистрацию всех событий, связанных с попытками аутентификации, в том числе должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события;

- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

1.7.2 Проверка регистрации запроса на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)

Описание функции

СЗИ «Блокхост-Сеть 3» должна регистрировать все запросы на доступ к защищаемому ресурсу.

Действия

Проверка выполняется после совокупности выполненных действий, описанных в испытаниях:

- проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа (п. 1.1.1.1)
- проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта (п. 1.1.2.1).

Дальнейшие действия проверки и ожидаемые результаты приведены в таблице П4.40.

Таблица П4.40 – Действия при проверке регистрации запроса на доступ к защищаемому ресурсу

№ п/п	Действия	Ожидаемый результат
1	Войти в систему ЭВМ 1 от имени и с правами пользователя **Admin** с ролью в СЗИ «Администратор» и «Аудитор»	Загрузка рабочего стола
2	Запустить «Консоль сервера Блокхост-Сеть 3».	Консоль запущена
3	В консоли «Система развертывания и аудита» выполнить действия: 1) Перейти в раздел «Мониторинг», 2) Выбрать ЭВМ 2, 3) Нажать кнопку «Выполнить запрос»	Информация о событиях безопасности загружена
4	Выбрать события по категории «Дискреционное управление доступом» и нажать кнопку «Выполнить запрос»	Журнал регистрации событий безопасности содержит информацию о запросах на доступ к защищаемому ресурсу
5	Выполнить указанные в пунктах 1–4 действия для остальных поддерживаемых ОС на рабочих станциях в виртуальной сети	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Результаты проверки считаются положительными, если:

- журнал регистрации событий безопасности содержит информацию о запросах на доступ к защищаемому ресурсу;
- в зарегистрированных событиях регистрируется следующая информация:

– дата и время;
– субъект, осуществляющий регистрируемое действие;
– тип события;
– успешно ли осуществилось событие (обслужен запрос на доступ или нет).

1.7.3 Проверка регистрации создания и уничтожения объекта

Описание функции

СЗИ «Блокхост-Сеть 3» должна обеспечивать регистрацию создания и уничтожения объектов.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.41.

Таблица П4.41 – Действия при проверке регистрации создания и уничтожения объекта

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС ЭВМ1 от имени и с правами пользователя **Admin**	Появление рабочего стола
2	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
3	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** раскрыть дерево «**Список пользователей»** → **User1** выбрать пункт «**Дискреционный**.» Добавить в список контролируемых объектов диск D:\, если он в нем отсутствует, разрешив полный доступ к объекту и аудит.	В «**Основной панели настроек клиентов»** установлены настройки дискреционного механизма для пользователя **User1**
4	В окне **«Настройки машины»** выбрать пункт «**Мандатный механизм»**. В «**Основной панели настроек клиентов»** выделить мандатную метку «**Документы общего пользования».** Присвоить мандатную метку **1** объекту D:\	В «**Основной панели настроек клиентов»** установлены настройки мандатного механизма
5	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Сохранение настроек
6	Войти в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
7	Создать новый объект доступа D:\НОВЫЙ ТЕКСТОВЫЙ ДОКУМЕНТ.txt	Создание объекта доступа
8	Переименовать объект доступа из D:\НОВЫЙ ТЕКСТОВЫЙ ДОКУМЕНТ.txt в D:\11.txt	Переименование объекта доступа
9	Удалить объект доступа D:\11.txt	Удаление объекта доступа
10	Перезагрузить ЭВМ	Перезагрузка ЭВМ
11	Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита»
12	В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Наличие информации о действиях с объектом доступа

№ п/п	Действия	Ожидаемый результат
13	Выполнить указанные в пунктах 1 – 12 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Результаты проверки считаются положительными, если СЗИ обеспечивает надежную регистрацию всех событий, связанных с созданием и уничтожением объектов, в том числе должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события;
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

1.7.4 Проверка регистрации действий по изменению ПРД

Описание функции

СЗИ «Блокхост-Сеть 3» должна обеспечивать регистрацию действий по изменению ПРД.

Действия

Проверка выполняется согласно действиям, выполняемым в п. 1.1.1.1.

Журнал содержит информацию о действиях по изменению ПРД (дата и время, субъект, тип события, успешно ли осуществилось событие)

Результаты тестирования

Результаты проверки считаются положительными, если СЗИ обеспечивает надежную регистрацию всех событий, связанных с изменением ПРД, в том числе должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события;
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

1.7.5 Проверка наличия средств выборочного ознакомления с регистрационной информацией

Описание функции

СЗИ «Блокхост-Сеть 3» реализован механизм фильтрации событий в журнале аудита.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.42.

Таблица П4.42 – Действия при проверке наличия средств выборочного ознакомления с регистрационной информацией

№ п/п	Действия	Ожидаемый результат
1	Войти в систему от имени и с правами пользователя **Admin**	Появление рабочего стола
2	Запустить консоль «Системы развертывания и аудита»	Открытие консоли Системы развертывания и аудита
3	В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Отображение сообщений аудита о работе модулей СЗИ.
4	В окне события аудита выбрать пункты и критерии, согласно которым будет выполнена фильтрация. Нажать кнопку «**Выполнить запрос».**	В «**Основной панели настроек клиентов»** будут отображены только сообщения, которые отвечают критериям фильтра
5	Выполнить указанные в пунктах 1–4 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Результаты проверки считаются положительными, если в СЗИ функционируют средства для выборочного ознакомления с регистрационной информацией.

1.7.6 Проверка регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.)

Описание функции

СЗИ «Блокхост-Сеть 3» должна регистрировать все попытки доступа, все действия оператора и выделенных пользователей.

Действия

Проверка выполняется согласно действиям, выполняемым в п. 1.1.1.1, 1.1.2.1 и 1.6.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.43.

Таблица П4.43 – Действия при проверке регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.)

№ п/п	Действия	Ожидаемый результат
1	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Создать директорию C:\LogTest. Создать файлы: -C:\LogTest\test1.txt; -C:\LogTest\test2.txt	Появление в проводнике папки и файлов

№ п/п	Действия	Ожидаемый результат
3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Мандатный механизм»**. Назначить иерархические мандатные метки с ведением аудита для файлов: - C:\LogTest\test1.txt – мандатную метку **1**; - C:\LogTest\test2.txt – мандатную метку **2**	Правила разграничения доступа для мандатного механизма заданы
4	В окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → User1 → «Дискреционный».** Задать дискреционные ПРД с аудитом: -C:\LogTest\test1.txt – **R/W**; -C:\LogTest\test2.txt – **R/W**. в окне **«Настройки машины»** раскрыть дерево «**Список пользователей» → User2 → «Дискреционный».** Задать дискреционные ПРД с аудитом: -C:\LogTest\test1.txt – **R/W**; -C:\LogTest\test2.txt – **-/-**.	Правила разграничения доступа для дискреционного доступа заданы
5	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Сохранение настроек
6	Перезагрузить ЭВМ2	Появление интерфейса СЗИ «Блокхост-Сеть 3»
7	Войти в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
8	Открыть файл C:\LogTest\test1.txt	Открытие файла
9	Открыть файл C:\LogTest\test2.txt	Отказано в доступе
10	Выйти из системы или перезагрузить ЭВМ2	Появление интерфейса СЗИ «Блокхост-Сеть 3»
11	Войти в систему от имени и с правами **User2**	Загрузка рабочего стола
12	Открыть файл C:\LogTest\test1.txt	Открытие файла
13	Открыть файл C:\LogTest\test2.txt.	Отказано в доступе
14	Выйти из системы или перезагрузить ЭВМ2	Появление интерфейса СЗИ «Блокхост-Сеть 3».
15	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
16	Запустить консоль Системы развертывания и аудита	Открытие консоли Системы развертывания и аудита
17	В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Отображены сведения обо всех действиях пользователей и для каждого события содержит дату и время, субъект, тип, статус
18	Выполнить указанные в пунктах 1–17 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Результаты проверки считаются положительными, если СЗИ регистрирует все попытки доступа, все действия оператора и выделенных пользователей**.**

1.8 Проверка взаимодействия пользователя с СЗИ «Блокхост-Сеть 3»

1.8.1 Проверка наличия модульной структуры СЗИ «Блокхост-Сеть 3» для обеспечения возможности изучения, анализа, верификации и модификации

Описание функции

Для удобного взаимодействия с администратором безопасности и пользователями СЗИ «Блокхост-Сеть 3» структурирована и имеет интуитивно понятный интерфейс (см. п. 3.2. настоящего руководства), что обеспечивает возможность правильной настройки СЗИ на контролируемых рабочих станциях со стороны администратора безопасности.

Взаимодействие пользователя с СЗИ должно обеспечивать настройку его параметров работы. Параметры СЗИ делятся на системные, которые задают правила доступа всех пользователей и индивидуальные, которые относятся к правилам доступа конкретных пользователей.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.44.

Таблица П4.44 – Действия при проверке наличия модульной структуры СЗИ «Блокхост-Сеть 3» для обеспечения возможности изучения, анализа, верификации и модификации

№ п/п	Действия	Ожидаемый результат
1	Используя руководство администратора (см. п. 1.6. «Общая архитектура СЗИ «Блокхост-Сеть 3»), убедиться в модульной структуре построения СЗИ	Описание модулей в руководстве администратора
2	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
3	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
4	В окне **«Список машин»** выбрать ЭВМ2, в окне **«Настройки машины»** выбрать пункт «**Список пользователей»**	Появление в «**Основной панели настроек клиентов»** списка пользователей
5	В окне **«Список машин»**, раскрыв список пользователей СЗИ выделить любого пользователя	Появление в «**Основной панели настроек клиентов»** индивидуальных настроек пользователя, распределенных по механизмам СЗИ
6	В окне **«Настройки машины»** выбрать пункт «**Общие сведения»**	В «**Основной панели настроек клиентов»** отобразились настройки механизмов СЗИ

№ п/п	Действия	Ожидаемый результат
		выбранной ЭВМ
7	Выполнить указанные в пунктах 1 – 6 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания механизма взаимодействия пользователя с КСЗ считаются успешными, если СЗИ «Блокхост-Сеть 3» структурирована, а ее структура является модульной.

1.8.2 Проверка наличия стандартизированного интерфейса пользователя

Описание функции

Интерфейс пользователя определен согласно руководству администратора (см. п. 4.1 «Вход в систему» и п. 3.2 «Консоль администрирования СЗИ «Блокхост-Сеть 3»).

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.45.

Таблица П4.45 – Действия при проверке наличия стандартизированного интерфейса пользователя

№ п/п	Действия	Ожидаемый результат
1	Включить ЭВМ1	Появление интерфейса СЗИ «Блокхост-Сеть 3»
2	Убедиться, что интерфейс процесса аутентификации пользователя СЗИ соответствует указанному в документации (п. 4.1 «Вход в систему» руководства администратора).	Соответствует
3	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
4	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
5	Убедиться, что интерфейс консоли администрирования СЗИ соответствует указанному в документации (п. 3.2 «Консоль администрирования СЗИ «Блокхост-Сеть 3» руководства администратора).	Соответствует
6	Выполнить указанные в пунктах 1 – 5 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если интерфейс аутентификации пользователя и интерфейс консоли администрирования СЗИ определены и являются неизменными.

1.8.3 Проверка обеспечения надежности интерфейса

Описание функции

Взаимодействие с пользователем обеспечивает интерфейс пользователя и консоли администрирования. При указанном взаимодействии должна обеспечиваться надежность интерфейса.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.46.

Таблица П4.46 – Действия при проверке обеспечения надежности интерфейса

№ п/п	Действия	Ожидаемый результат
1	Включить ЭВМ1	Появление интерфейса СЗИ «Блокхост-Сеть 3»
2	Повторить десять раз следующую последовательность действий: - войти в систему от имени и с правами пользователя **Admin**; - открыть консоль администрирования СЗИ; - закрыть консоль администрирования СЗИ; - выйти из системы	Появление рабочего стола. Неизменность интерфейса СЗИ
3	Повторить десять раз следующую последовательность действий: - включить ЭВМ1; - войти в систему от имени и с правами пользователя **Admin**; - открыть консоль администрирования СЗИ; - обеспечить аварийное завершение, путем симуляции сбоя по питанию	Появление интерфейса СЗИ «Блокхост-Сеть 3»
4	Включить ЭВМ1	Появление интерфейса СЗИ «Блокхост-Сеть 3»
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Испытания надежности интерфейса считаются успешными, если при неоднократном к нему обращении интерфейс СЗИ остается стабильно рабочим. Аварийные завершения работы не сказываются на его надежности.

1.8.4 Проверка логического изолирования интерфейса пользователя и СЗИ от других таких же интерфейсов

Описание функции

Каждый интерфейс пользователя и СЗИ должен быть логически изолирован от других таких же интерфейсов.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.47.

Таблица П4.47 – Действия при проверке логического изолирования интерфейса пользователя и СЗИ от других таких же интерфейсов

№ п/п	Действия	Ожидаемый результат
1	Включить ЭВМ1	Появление интерфейса СЗИ «Блокхост-Сеть 3».
2	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
3	Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
4	В окне **«Настройки машины»** выбрать не менее 5 вариантов изменения настроек основных механизмов СЗИ «Блокхост-Сеть 3»	Каждому механизму соответствует своя область настроек.
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается, успешной если каждый интерфейс пользователя и СЗИ «Блокхост-Сеть 3» логически изолирован от других таких же интерфейсов.

1.9 Проверка надежного восстановления

1.9.1 Проверка полного восстановления свойств СЗИ «Блокхост-Сеть 3» после сбоев и отказов оборудования при использовании процедур восстановления

Описание функции

Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств СЗИ.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.48.

Таблица П4.48 – Действия при проверке полного восстановления свойств СЗИ «Блокхост-Сеть 3» после сбоев и отказов оборудования при использовании процедур восстановления

№ п/п	Действия	Ожидаемый результат
1	Включение ЭВМ1	Появление интерфейса СЗИ

№ п/п	Действия	Ожидаемый результат
2	Войти в систему от имени и с правами **Admin**	Загрузка рабочего стола
3	Проверить работоспособность СЗИ	Механизмы защиты СЗИ функционируют
4	Выключение питания ЭВМ1 и включение ее вновь для имитирования отказа оборудования	Появление интерфейса СЗИ
5	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
6	Проверить работоспособность СЗИ	Механизмы защиты СЗИ функционируют
7	Выполнить указанные в пунктах 1 – 6 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка процедуры надежного восстановления считается успешной, если в результате ее применения произошло полное восстановление свойств СЗИ.

1.10 Проверка целостности СЗИ «Блокхост-Сеть 3»

1.10.1 Проверка наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3»

Описание функции

Контроль целостности должен осуществляться по алгоритму CRC-32 и при обнаружении изменений в файле должно происходить его восстановление. Этот механизм используется для контроля целостности и надежного восстановления свойств средства защиты информации после сбоев и отказов оборудования.

При инсталляции средства защиты автоматически создаются резервные копии всех программных модулей СЗИ вместе с их контрольными суммами. Проверка целостности осуществляется периодически в процессе работы системы. При обнаружении ошибки выполняется перезагрузка системы с восстановлением модулей из резервных копий.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.49.

Таблица П4.49 – Действия при проверке наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
	Периодический контроль целостности СЗИ после перезагрузки ОС	
1	Войти в систему от имени и с правами **Admin**	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
2	Создать документ C:\test.txt с произвольным содержимым	Документ создан и сохранен на диск
3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ 2. В окне **«Настройки машины»** выбрать параметр «**Контроль целостности файлов»**.	В **Основной панели настроек клиента** отобразились настройки механизма контроля целостности файлов.
4	В **Основной панели настроек клиента**: - отметить параметр **«Включить контроль целостности»**; - в поле «**Периодичность контроля (чч:мм:сс)»** установить интервал 5 **мин**.	Механизм контроля целостности включен и установлена периодичность контроля равная 5 мин.
5	В окне **«Настройки машины»** выбрать параметр «**Контроль целостности»**. Добавить следующие файлы (объекты) на контроль и отметить для каждого из них параметр **Аудит**: - blockpostMF.sys; - GIS.BlockPost.Client.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe И установить атрибут **Восстанавливать**	Файлы поставлены на контроль. Пункт **Аудит** у каждого объекта активирован
6	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Изменения сохранены
7	Перезагрузить ЭВМ 2	Загрузка операционной системы
8	С помощью программы **WinHEX** внести изменение в файлы: - blockpostMF.sys; - GIS.BlockPost.Client.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe и сохранить	Изменения внесены и сохранены
9	Перезагрузить ЭВМ2	Загрузка операционной системы
10	Открыть фалы - blockpostMF.sys; - GIS.BlockPost.Client.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe программой **WinHEX** и убедиться, что файл восстановлен к исходному состоянию	В файле не содержится внесенных изменений
	Периодический контроль целостности СЗИ во время сеанса работы	
11	Войти в систему с от имени и справами пользователя User1	Загрузка рабочего стола
12	Выполнить следующие действия 1) Внести изменения в файл blockpostMF.sys, 2) Ожидание установленного времени «Периодичности контроля» равное 5 минутам.	Изменения внесены и сохранены

№ п/п	Действия	Ожидаемый результат
	3) Открыть файл blockpostMF.sys и убедиться, что файл восстановлен	В файле не содержится внесенных изменений
13	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ 2. Нажать кнопку «**Выполнить запрос».**	Наличие записей об успешном восстановлении файлов, поставленных на контроль
14	Выполнить указанные в пунктах 1 – 14 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Результаты тестирования

Проверка считается успешной, если:

- обеспечивается контроль целостности программной и информационной частей СЗИ и полное восстановление свойств СЗИ при нарушении целостности;
- при нарушении целостности файлов, обеспечивается их полное восстановление;
- в журнале аудита фиксируются сообщения о нарушении целостности файлов, поставленных на контроль.

1.10.2 Проверка наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3» с блокировкой доступа пользователя при нарушении целостности

Описание функции

В СЗИ должна осуществляется проверка целостности периодически в процессе работы системы. При обнаружении нарушений целостности, установленных на контроль объектов, должна осуществляться блокировка доступа пользователей в систему, а также возможно прерывание сеанса работы пользователя.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.50.

Таблица П4.50 – Действия при проверке наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3» с блокировкой доступа пользователя при нарушении целостности

№ п/п	Действия	Ожидаемый результат
	Периодический контроль целостности СЗИ с блокировкой пользователя после перезагрузки ОС	
1	Войти в систему ЭВМ1 от имени и с правами **Admin**	Загрузка рабочего стола
2	Создать документ C:\test.txt с произвольным содержимым	Документ создан и сохранен на диск
3	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ 2. В окне **«Настройки машины»** выбрать	В **Основной панели настроек клиента** отобразились настройки

№ п/п	Действия	Ожидаемый результат
	параметр «**Контроль целостности файлов»** и «**Блокировать доступ пользователей в систему при нарушении целостности файлов»**	механизма контроля целостности файлов.
4	В **Основной панели настроек клиента**: - отметить параметр **«Включить контроль целостности»**; - в поле «**Периодичность контроля (чч:мм:сс)»** установить интервал 5 **мин**.	Механизм контроля целостности включен и установлена периодичность контроля равная 5 мин.
5	В окне **«Настройки машины»** выбрать параметр **Контроль целостности**. Добавить следующие файлы (объекты) на контроль и отметить для каждого из них параметр **Аудит**: - blockpostMF.sys; - GIS.BlockPost.Client.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe Атрибут «**Восстанавливать»** отключить, если он включен	Файлы поставлены на контроль. Пункт **Аудит** у каждого объекта активирован
6	Сохранить произведенные настройки, выбрав пункт меню «**Главная»** → **«Сохранить все»**	Изменения сохранены
7	Перезагрузить ЭВМ2	Загрузка операционной системы
8	С помощью программы **WinHEX** внести изменение в файлы: - blockpostMF.sys; - GIS.BlockPost.Client.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe и сохранить	Изменения внесены и сохранены
9	Перезагрузить ЭВМ 1	Загрузка операционной системы
10	Попытка входа в систему ЭВМ 1 пользователем	Вход в систему заблокирован, нарушена целостность файла
11	Войти в систему ЭВМ 1 от имени и с правами **Admin**	Загрузка рабочего стола
	Периодический контроль целостности СЗИ с блокировкой пользователя во время сеанса работы	
12	Войти в систему с от имени и справами пользователя Admin	Загрузка рабочего стола
13	С помощью программы **WinHEX** внести изменение в файл blockpostMF.sys.	Изменения внесены и сохранены
14	Ожидание установленного времени Периодичности контроля равное 5 минутам	Сеанс работы пользователя прерывается.
15	Попытка входа в систему ЭВМ 2 пользователем User1	Вход в систему заблокирован, нарушена целостность файла
16	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ2. Нажать кнопку «**Выполнить запрос».**	Наличие записей о нарушении целостности файлов, поставленных на контроль и блокировании пользователя.
17	Выполнить указанные в пунктах 1 – 16 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных	Совпадение полученных результатов с приведенными

№ п/п	Действия	Ожидаемый результат
	установленных операционных систем	выше результатами

Критерии оценки

Проверка считается успешной, если:

- при нарушении целостности файлов, установленных на контроль, вход пользователя в систему заблокирован;
- при нарушении целостности файлов, установленных на контроль, сеанс работы пользователя прерван;
- в журнале аудита фиксируются сообщения о нарушении целостности файлов, поставленных на контроль.

1.10.3 Проверка регистрации событий, связанных с изменением целостности среды

Описание функции

В СЗИ «Блокхост-Сеть 3» должна производиться регистрация событий, связанных с целостности среды (установленных программ, служб, драйверов, перечня каталогов общего доступа) с целью обнаружения модификации ресурсов системы.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.51.

Таблица П4.51 – Проверка контроля целостности среды

№ п/п	Действия	Ожидаемый результат
1	**Настройки целостности среды**	
1.1	Войти в систему от имени и с правами **Admin**	Загрузка рабочего стола
1.2	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ 1. В окне **«Настройки машины»** выбрать параметр **Контроль целостности среды**	В **Основной панели настроек клиента** отобразились настройки механизма контроля целостности среды.
1.3	Установить параметры: **Контроль установки\удаления программ;** **Контроль установки\удаления служб;** **Контроль установки\удаления драйверов;** **Контроль изменения перечня каталогов общего доступа.**	Для ЭВМ1 настроен **Контроль целостности среды**
1.4	Сохранить произведенные настройки, выбрав пункт меню «**Главная**» → **«Сохранить все»**	Изменения сохранены
2	**Проверка регистрации событий безопасности**	
2.1	Перезагрузить ЭВМ 1	Загрузка операционной системы
2.2	Войти в систему от имени и с правами **Admin** и установить	Клиент eToken установлен

	PKIClient eToken	
2.3	Создать папку общего доступа	Папка общего доступа создана
2.4	Удалить клиента eToken	Клиент eToken удален
2.5	Отключить папку общего доступа	Клиент RuToken установлен
2.5	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, об установке и удалении приложения, а также об изменения перечня каталогов общего доступа
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки

Проверка считается успешной, если при отслеживании изменений целостности среды появляются сообщения, фиксирующие изменения целостности установленных на контроль объектов.

1.10.4 Проверка регистрации событий, связанных с изменением аппаратной среды

Описание функции

СЗИ «Блокхост-Сеть 3» должно регистрировать события, связанные с изменения следующих устройств аппаратной среды: процессор, жесткий диск, CDROM, сетевой адаптер, материнская плата, видеокарта.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.52.

Таблица П4.52 – Проверка контроля аппаратной среды

№ п/п	Действия	Ожидаемый результат
1	**Настройки целостности среды**	
1.1	Войти в систему от имени и с правами **Admin**	Загрузка рабочего стола
1.2	В консоли администрирования СЗИ в окне **«Список машин»** выбрать ЭВМ 1. В окне **«Настройки машины»** выбрать параметр «**Контроль целостности среды»**	В **Основной панели настроек клиента** отобразились настройки механизма контроля целостности среды.
1.3	Установить параметры: **«Контроль аппаратной среды.»**	Для ЭВМ1 настроен **Контроль аппаратной среды**
1.4	Сохранить произведенные настройки, выбрав пункт меню «**Главная» → «Сохранить все»**	Изменения сохранены
2	**Проверка**	
2.1	Перезагрузить ЭВМ 1, после перезагрузки отключить станцию ЭВМ1	ЭВМ1 отключена
2.2	Подключить в ЭВМ 1 новый CD-Rom	Новое устройство подключено
2.3	Запустить ЭВМ1 и войти в систему пользователем	ЭВМ включена, загрузка ОС

2.4	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать ЭВМ1. Нажать кнопку «**Выполнить запрос».**	Появление сообщений, фиксирующих о целостности аппаратной среды
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ 1 – ЭВМ 5 для всех остальных установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки

Проверка считается успешной, если при отслеживании конфигурации устройств компьютера фиксируются сообщения об обнаружении модификации ресурсов системы.

1.10.5 Проверка выполнения программ в отдельной части оперативной памяти

Описание функции

Программы (модули) СЗИ должны выполняться в отдельной части оперативной памяти.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.53.

Таблица П4.53 – Выполнения программ в отдельной части оперативной памяти

№ п/п	Действия	Ожидаемый результат
1	Войти в систему от имени и с правами **Admin**	Загрузка рабочего стола
2	Запускаем утилиту RamMap	Утилита запущена
3	Поиск адресов в оперативной памяти	
4	В запущенной утилите RamMap перейти в вкладку «File Details» и отсортировать по столбцу «Path»	Процессы, запущенные в оперативной памяти отсортированы
5	**Поиск занятых ячеек памяти модуля СЗИ consolelauncher.exe**	
5.1	Выбрать и раскрыть список занимаемых адресов C:\blockhost\bpshell\consolelauncher.exe	Список адресов раскрыт
5.2	В столбце «PhysicalAddress» выбрать произвольное значение физической ячейки	Адрес ячейки выбран
5.3	Нажать сочетание клавиш CTRL + F	Открыто окно поиска
5.4	Внести адрес выбранной ячейки и последовательно произвести поиск установив параметр «Вверх», «Вниз»	Совпадений не найдено
6	**Поиск занятых ячеек памяти модуля СЗИ gis.blockpost.exe**	
6.1	Выбрать и раскрыть список занимаемых адресов C:\blockhost\bpshell\gis.blockpost.exe	Список адресов раскрыт
6.2	В столбце «PhysicalAddress» выбрать произвольное значение физической ячейки	Адрес ячейки выбран
6.3	Нажать сочетание клавиш CTRL + F	Открыто окно поиска

№ п/п	Действия	Ожидаемый результат
6.4	Внести адрес выбранной ячейки и последовательно произвести поиск установив параметр «Вверх», «Вниз»	Совпадений не найдено
7	**Поиск занятых ячеек памяти модуля СЗИ gis.client.settingsdispatcher.exe**	
7.1	Выбрать и раскрыть список занимаемых адресов C:\blockhost\system32\gis.client.settingsdispatcher.exe	Список адресов раскрыт
7.2	В столбце «PhysicalAddress» выбрать произвольное значение физической ячейки	Адрес ячейки выбран
7.3	Нажать сочетание клавиш CTRL + F	Открыто окно поиска
7.4	Внести адрес выбранной ячейки и последовательно произвести поиск установив параметр «Вверх», «Вниз»	Совпадений не найдено

Результаты тестирования

Проверка считается успешной, если не найдено совпадений адресов занятыми модулями СЗИ в оперативной памяти ЭВМ.