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 средств управления, ограничивающих распространение прав на доступ	1.1.1.5
	Проверка наличия механизма, претворяющего в жизнь дискреционные ПРД, как для явных, так и для скрытых действий пользователя	1.1.1.6
	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	1.1.2.2

№ п/п	Наименование испытаний (проверок)	Пункт методики
	данных в систему	
	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 функции установки мандатной метки автовхода.	1.1.2.6
2	**Проверка очистки памяти**	1.2
	Проверка возможности очистки внешней памяти	1.2.1
	Проверка возможности 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 (в идентифицированном СЗИ «Блокхост-Сеть 3»), 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

№ п/п	Наименование испытаний (проверок)	Пункт методики
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
	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 выполнения программ в отдельной части оперативной памяти	1.10.2

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 файла. Остальные действия невозможны, например, нельзя прочитать содержимое каталога (подкаталоги и файлы), при этом все его содержимое также имеет запрет по чтению.

Использование одновременно разрешения чтения и записи дает полный доступ к объекту: чтение и изменение содержимого, переименование, перемещение и удаление файла (таблица П4.2).

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

Разрешения для субъекта доступа (пользователя)		**Перечень разрешенных операций по отношению к объекту доступа**				
Чтение	Запись	Чтение содержимого	Запись (изменение содержимого)	Переимено-вание	Перемещение	Удаление
+	-	+	-	-	-	-
-	+	-	+	-	-	-
+	+	+	+	+	+	+
-	-	-	-	-	-	-

Действия

Перечень действий для проверки выполнения контроля доступа и ожидаемый результат после выполнения каждого действия представлен в таблицах П4.3 и П4.4.

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

№ п/п	**Действия**	**Результат**
1	**Создание матрицы доступа и тестовых объектов файловой системы**	

<table>
<tr><th>№ п/п</th><th>Действия</th><th>Результат</th></tr>
<tr><td></td><td>Создать матрицу разграничения доступа</td><td>
<table>
<tr><td></td><td>D:\D1</td><td>D:\D2</td><td>D:\D3</td><td>D:\D4</td></tr>
<tr><td>User1</td><td>RW</td><td>RW</td><td>RW</td><td>RW</td></tr>
<tr><td>User2</td><td>W</td><td>W</td><td>W</td><td>W</td></tr>
<tr><td>User3</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>User4</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td></td><td>D:\D5</td><td>D:\D6</td><td>D:\read.txt</td><td>D:\copy.txt</td></tr>
<tr><td>User1</td><td>RW</td><td>RW</td><td>RW</td><td>RW</td></tr>
<tr><td>User2</td><td>W</td><td>W</td><td>W</td><td>W</td></tr>
<tr><td>User3</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>User4</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td></td><td>D:\ren.txt</td><td>D:\modify.txt</td><td>D:\move.txt</td><td>D:\del.txt</td></tr>
<tr><td>User1</td><td>RW</td><td>RW</td><td>RW</td><td>RW</td></tr>
<tr><td>User2</td><td>W</td><td>W</td><td>W</td><td>W</td></tr>
<tr><td>User3</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>User4</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
</table>
</td></tr>
<tr><td></td><td>Создать объекты файловой системы для проверки ПРД к каталогам:
D:\D1,
D:\D2,
D:\D3,
D:\D4,
D:\D5,
D:\D6,
каждый из которых содержат 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,</td><td>Успешное создание указанных директорий и файлов</td></tr>
</table>

№ п/п	Действия	Результат
	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 СЗИ
	В окне «Список машин» выбрать рабочую станцию, 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 гарантированное удаление и 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 гарантированное удаление и 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**
	Задать дискреционные ПРД для пользователя **User3** в соответствии с матрицей разграничения доступа, включить для всех объектов	Отображение произведенных настроек в **Основной панели настроек клиента**

№ п/п	Действия		Результат
	гарантированное удаление и аудит		
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** в соответствии с матрицей РД, включив для всех объектов аудит		Отображение произведенных настроек в **Основной панели настроек клиента**
	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***		Настройки сохранены
3	**Просмотр событий**		
	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***		Появление сообщений, фиксирующих произведенное изменение настроек на выбранной рабочей станции
	Завершить работу с консолью администрирования СЗИ		Закрытие окна консоли администрирования
4	**Проверка действующих политик разграничения доступа к файловой системе NTFS**		
	На выбранной рабочей станции 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
5	**Проверка дискреционного механизма разграничения доступа для заданных пользователям ПРД**		
5.1	Осуществить вход на выбранную рабочую станцию от имени и с правами пользователя **User1** 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	Успешно

№ п/п	Действия		Результат
		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 на выбранную рабочую станцию 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

№ п/п	Действия		Результат
	Удаление	D:\D6	Неудачно
		D:\del.txt	Неудачно
	Восстановить объекты файловой системы. Завершить сеанс работы пользователя User2		Появление приглашения для входа в систему
5.3	Осуществить вход на выбранную рабочую станцию 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
	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
5.4	Осуществить вход на выбранную рабочую станцию от имени и с правами пользователя **User4** и выполнить следующие действия		
	Чтение	D:\D1	Неудачно

№ п/п	Действия		Результат
		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
6	**Просмотр событий аудита**		
	Запустить консоль «Системы развертывания и аудита»		Запуск консоли Системы развертывания и аудита
	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***		Появление сообщений, фиксирующих санкционированные и несанкционированные попытки доступа пользователей к объектам файловой структуры.
7	**Удаление настроек дискреционных ПРД**		
	В окне «Настройки машины» раскрыть дерево *Список пользователей →User1*. Выбрать параметр *Дискреционный*		В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User1**
	Удалить клавишей **<Del>** из области настроек объекты файловой системы, стоящие на контроле		Область настроек для дискреционных ПРД пользователя **User1** очистится
	В окне «Настройки машины» раскрыть дерево *Список пользователей*		В **Основной панели настроек клиента** открылись

№ п/п	Действия	Результат
	→*User2*. Выбрать параметр *Дискреционный*	настройки механизма дискреционных ПРД для **User2**
	Удалить клавишей **<Del>** из области настроек объекты файловой системы, стоящие на контроле	Область настроек для дискреционных ПРД пользователя **User2** очистится
	В окне «Настройки машины» раскрыть дерево *Список пользователей* →*User3*. Выбрать параметр *Дискреционный*	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User3**
	Удалить клавишей **<Del>** из области настроек объекты файловой системы, стоящие на контроле	Область настроек для дискреционных ПРД пользователя **User3** очистится
	В окне «Настройки машины» раскрыть дерево *Список пользователей* →*User4*. Выбрать параметр *Дискреционный*	В **Основной панели настроек клиента** открылись настройки механизма дискреционных ПРД для **User4**
	Удалить клавишей **<Del>** из области настроек объекты файловой системы, стоящие на контроле	Область настроек для дискреционных ПРД пользователя **User4** очистится
	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Сохранение настроек
8	**Просмотр событий аудита**	
	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих произведенные изменения настроек на выбранной рабочей станции

Таблица П4.4 – Перечень действий при проверке контроля запуска на исполнение исполняемых объектов наименованными субъектами

№ п/п	Действия	Ожидаемый результат
1	Запустить консоль администрирования СЗИ «Блокхост-Сеть 3»	Консоль администрирования СЗИ запущена
2	В окне «Список машин» выбрать рабочую станцию	В Основной панели настроек клиентов отобразились настройки механизмов СЗИ на выбранной рабочей станции
3	В окне «Настройки машины» раскрыть дерево Список пользователей → User1. Выбрать параметр Контроль процессов	В Основной панели настроек клиентов отобразился механизм настройки контроля процессов

№ п/п	Действия	Ожидаемый результат
4	В **Основной панели настроек клиентов** перенести все процессы из списков «Запущенные процессы» и «Установленные процессы» в верхнее поле окна – «Разрешенные процессы»	В **Основной панели настроек клиентов** отобразился полный список разрешенных процессов.
5	Удалить из списка разрешенных процессов файл «Far.exe»	Файл «Far.exe» появился в списке запрещенных
6	Активировать аудит, для чего необходимо отметить параметр Аудит, распложенный справа от выбранного процесса	Параметр ***Аудит*** установлен
7	Активировать режим замкнутой среды, для чего необходимо отметить параметр ***Контролировать***, расположенный в верхней части вкладки.	Параметр ***Контролировать*** установлен
8	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	Настройки сохранены
9	Войти в ОС рабочей станции от имени пользователя User1	Загрузка рабочего стола
10	Попытаться запустить на исполнение файл «Far.exe»	Отказ доступа
11	Войти в ОС рабочей станции от имени пользователя Admin	Загрузка рабочего стола
12	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих санкционированные и несанкционированные попытки доступа

Результаты тестирования

Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) 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 РД осуществляется с использованием механизма копирования индивидуальных настроек разграничения доступа и механизма объединения пользователей (индивидов) в группы. Копирование настроек СЗИ «Блокхост-Сеть 3» позволяет применить созданные правила к разным пользователям, что существенно упрощает процесс настройки ПРД пользователей. Администратор безопасности с помощью процедуры копирования настроек СЗИ «Блокхост-Сеть 3» может осуществить репликацию настроек разных пользователей. Использование репликации настроек 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 П4.5.

Таблица П4.5 – 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
3	Загрузить консоль администрирования СЗИ	Запуск консоли администрирования СЗИ
4	В окне **«Список машин»** выбрать рабочую станцию 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***	Сохранение настроек
7	В окне «Настройки машины» раскрыть дерево *Список пользователей →User1*. Выбрать параметр	Появление в **Основной панели настроек клиента** настроек

№ п/п	Действия	Ожидаемый результат
	Дискреционный	дискреционного механизма СЗИ
8	Выбрать пункт меню Главная →Копировать	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***	Сохранение настроек
12	Убедиться в правильности применения настроек пользователя **User1** к пользователю **User2**	Правильное применение настроек пользователя **User1** к пользователю **User2**

Проверка выполнения заданных параметров выполняется на основе действий, указанных в п. 1.1.1.1.

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 пользователи не имеют прав на запуск консоли администрирования, что позволяет исключить непреднамеренный доступ пользователей к администрированию СЗИ.

Действия

Для выполнения проверки пользователю **User1** необходимо присвоить права администратора локальной рабочей станции. Выполняемые при проверке действия указаны в таблице П4.6.

Таблица П4.6 – Проверка возможности санкционированного изменения ПРД

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
2	Попытаться запустить консоль администрирования СЗИ	Появление сообщения *Вам не разрешено запускать консоль администратора*
3	Выполнить вход в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
4	Запуск консоли администрирования СЗИ	Появление консоли администрирования СЗИ
5	Войти в консоль администрирования СЗИ. Выбрать рабочую станцию. Изменить ПРД для конкретного пользователя	Успешно
6	Сохранить произведенные настройки, выбрав пункт меню *Главная →Сохранить*	Сохранение настроек
7	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку *Выполнить запрос*.	Появление сообщений об изменениях ПРД

Результаты тестирования

Проверка считается успешной, если администратор СЗИ успешно изменил ПРД пользователя, а пользователь не смог осуществить изменение ПРД из-за недоступности серверной консоли администрирования.

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 П4.7.

Таблица П4.7 – Проверка предоставления прав изменения ПРД выделенным субъектам

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени встроенного локального администратора	Загрузка рабочего стола
2	Загрузить консоль администрирования СЗИ, в окне «Список машин» выбрать рабочую станцию	Появление консоли администрирования
3	В окне «Настройки машины» раскрыть дерево *Список пользователей →User1*. Выбрать параметр *Полномочия*	Появление в Основной панели настроек клиента настроек разграничения доступа пользователей к администрированию СЗИ
4	Предоставить все полномочия по администрированию СЗИ для пользователя User1, установив в Основной панели настроек клиента параметр *Запуск консоли СЗИ*	Успешно
5	Сохранить произведенные настройки, выбрав пункт меню *Главная →Сохранить*	Сохранение настроек
6	Выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
7	Войти в консоль администрирования СЗИ, в окне «Список машин» выбрать рабочую станцию. Изменить настройки всех механизмов СЗИ.	Успешно
8	Сохранить произведенные настройки, выбрав пункт меню *Главная →Сохранить*	Сохранение настроек
9	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку *Выполнить запрос*.	Появление сообщений об успешном изменении настроек СЗИ пользователем User1

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 средств управления, ограничивающих распространение прав на доступ

Описание функции

В СЗИ «Блокхост-Сеть 3» должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Механизм, предусматривающий ограничение распространения прав на доступ, может быть полезен в случае, когда администратору безопасности необходимо разделить

функциональные обязанности с другими пользователями.

Действия

Действия при проверке данного пункта указаны в таблице П4.8.

Таблица П4.8 – Действия при проверке наличия средств управления, ограничивающих распространение прав на доступ

№ п/п	Действия	Ожидаемый результат
1	**Создание субъектов доступа для администрирования СЗИ**	
	Загрузить серверную консоль администрирования СЗИ, в окне **«Список машин»** выбрать ЭВМ1	Запуск консоли администрирования
	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 **User1** установить полномочия Аудитор	Для **User1** 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.

Результаты тестирования

Проверка считается успешной, если в СЗИ предусмотрены средства, ограничивающие распространение прав на доступ.

1.1.1.6 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 П4.9.

Таблица П4.9 – Этапы проверки механизма ПРД

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени пользователя User3	Загрузка рабочего стола
2	Открыть D:\D1\read1.txt	Успешно
3	Изменить файл D:\D1\read1.txt и попытаться сохранить	Неудачно
4	Открыть 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 от имени и с правами	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
	пользователя Admin	
12	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос.	Появление сообщений о попытках доступа к контролируемым объектам

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.

1.1.2 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 П4.10.

Таблица П4.10 – Матрица разграничения доступа

СУБЪЕКТЫ	**ОБЪЕКТЫ**		
	D:\M1 (мандатная метка = **1,Public**)	*D:\M2* (мандатная метка = **2,Public,Work**)	*D:\M3* (мандатная метка = **3,Public,Work,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

Действия

Действия, выполняемые при проверке, приведены в таблице П4.11.

Таблица П4.11 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	**Действия**	**Ожидаемый результат**
1	Войти в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Запустить консоль администрирования СЗИ «Блокхост-Сеть 3». В окне **«Список машин»** выбрать рабочую станцию	Появление консоли администрирования СЗИ. Отображение в **Основной панели настроек клиентов** настроек механизмов СЗИ ЭВМ1.
3	**Создание объектов файловой системы**	
3.1	Создать каталоги *D:\M1*, *D:\M2*, *D:\M3*	Созданы каталоги *D:\M1*, *D:\M2*, *D:\M3*

№ п/п	Действия	Ожидаемый результат
3.2	Создать файлы: 1) D:\M1\read_1.txt; 2) D:\M2\read_2.txt; 3) D:\M3\read_3.txt	Созданы файлы *D:\M1\read_1.txt*, *D:\M2\read_2.txt*, *D:\M3\read_3.txt*
4	**Задание классификационных уровней (меток) объектам доступа**	
4.1	В консоли администрирования СЗИ в окне **«Настройки машины»** выбрать пункт ***Мандатный механизм***. 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

№ п/п	Действия	Ожидаемый результат
5.2	Перетащить мышью папку D:\M1 из Списка объектов файловой системы рабочей станции 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 список ресурсов, 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* включить аудит событий, связанных с попытками доступа к контролируемым ресурсам	В области *Список правил мандатной метки или категории* отображается список ресурсов, сопоставленных данной 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 рабочей станции 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 список ресурсов, сопоставленных 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 и D:\M3 из Списка объектов файловой системы рабочей станции 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 список ресурсов, сопоставленных данной категории. Параметр ***Аудит*** установлен.
5.9	В **Основной панели настроек клиентов** в области *Мандатные метки и категории*	В области *Список правил мандатной метки или категории* отображается пустой список

№ п/п	Действия	Ожидаемый результат
	выделить категорию с именем ***Work***	ресурсов, сопоставленных данной категории
5.10	Перетащить мышью папки D:\M2 и D:\M3 из Списка объектов файловой системы рабочей станции 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 список ресурсов, сопоставленных 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 папку D:\M3 из Списка объектов файловой системы рабочей станции 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 список ресурсов, сопоставленных данной категории. Параметр ***Аудит*** установлен.
5.13	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Настройки сохранены
6	**Задание классификационных меток субъектам доступа**	
6.1	В окне **«Настройки машины»** выбрать пункт ***Список пользователей***. Проверить значения классификационных уровней пользователей в соответствии с таблицей П4.10. Для пользователей **User1**, **User2** и **User3** выполнить редактирование значений мандатной метки и категорий, изменив их значение, соответственно, в поле ***Мандатная метка*** и ***Категории*** окна **«Изменение пользователя»** (для вызова этого окна выделить в **Основной панели настроек клиентов** редактируемого пользователя и выбрать пункт меню ***Управление пользователями →Изменение пользователя***)	Присвоены соответствующие мандатные метки и категории пользователям
7	**Просмотр событий аудита**	
7.1	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку	Появление сообщений, фиксирующих произведенные изменения настроек

№ п/п	Действия		Ожидаемый результат
	Выполнить запрос.		
7.2	Перезагрузить рабочую станцию		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\read_1.txt	Успешно
		D:\M2\read_2.txt	Неудачно
		D:\M3\read_3.txt	Неудачно
8.3	Запись файлов	D:\M1\read_1.txt в D:\M1	Успешно. Создана копия файла
		D:\M1\read_1.txt в D:\M2	Неудачно
		D:\M1\read_1.txt в D:\M3	Неудачно
8.4	Перезагрузить сервер безопасности		Появление окна аутентификации СЗИ
8.5	Выполнить вход в систему от имени и с правами пользователя **User2** и значением мандатной метки ***2,Public,Work***		
8.6	Чтение файлов	D:\M1\read_1.txt	Успешно
		D:\M2\read_2.txt.	Успешно
		D:\M3\read_3.txt	Неудачно
	Запись файлов	D:\M2\read_2.txt в D:\M1	Неудачно
		D:\M2\read_2.txt в D:\M2	Успешно. Создана копия файла
		D:\M2\read_2.txt в D:\M3	Неудачно
8.7	Перезагрузить сервер безопасности		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\read_1.txt	Успешно
		D:\M2\read_2.txt	Успешно
		D:\M3\read_3.txt	Успешно
	Запись файлов	D:\M3\read_3.txt в D:\M1	Неудачно
		D:\M3\read_3.txt в D:\M2	Неудачно
		D:\M3\read_3.txt в D:\M3	Успешно. Создана копия файла

№ п/п	Действия	Ожидаемый результат
8.10	Перезагрузить рабочую станцию	Появление окна аутентификации СЗИ
9	**Просмотр событий аудита**	
9.1	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***.	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

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);
- 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 П4.12.

Таблица П4.12 – Действия при проверке запроса и получения классификационных меток при вводе новых данных в систему

№ 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 рабочую станцию, 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
6	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	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	Сохранение настроек

№ п/п	Действия	Ожидаемый результат
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	Сохранение настроек
8	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос	Появление сообщений, фиксирующих произведенное в СЗИ изменение параметров учетной записи пользователя

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 П4.13.

Таблица П4.13 – 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 систему 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

№ п/п	Действия	Ожидаемый результат
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 рабочую станцию, нажать кнопку Выполнить запрос.	Наличие записей о доступе к объектам

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 П4.14.

Таблица П4.14 – Действия при проверке возможности сопровождения (изменения) классификационных уровней субъектов и объектов специально выделенными субъектами

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в ОС от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Запуск консоли администрирования СЗИ. В окне **«Список машин»** выбрать рабочую станцию	В **Основной панели настроек клиентов** отобразились настройки механизмов СЗИ для рабочей станции

№ п/п	Действия	Ожидаемый результат
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** возможность управления настройками СЗИ (отметить пункт ***Запуск консоли СЗИ***)	Отображение в **Основной панели настроек клиента** установленных пользователю **User1** параметров администрирования СЗИ
5	Перезагрузить рабочую станцию	Появление интерфейса аутентификации в СЗИ
6	Выполнить вход в систему от имени и с правами пользователя **User1**	Загрузка рабочего стола
7	Запуск консоли администрирования СЗИ	Успешно
8	Изменить каталогу *D:\M1* мандатную метку с ***1*** на ***2***	Успешное изменение мандатной метки
9	Добавить каталог *D:\M1* в список объектов мандатной категории ***Work***	Успешное изменение мандатной категории
10	Сохранить произведенные настройки, выбрав пункт ***Сохранить*** в меню ***Файл***	Сохранение настроек
11	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих произведенное изменение настроек

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.

Согласно схеме общей архитектуры СЗИ (рис. 1.3 – Руководство администратора безопасности) диспетчер доступа реализован в модуле «Модуль диспетчера доступа и гарантированного удаления». По умолчанию всем объектам присвоена иерархическая мандатная метка ***Документы общего доступа***, равная ***1*** и не назначены неиерархические категории.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.2.1 согласно таблице П4.15.

Таблица П4.15 – Действия при проверке реализации диспетчера доступа

№ п/п	Действия	Ожидаемый результат
1	Выполнить вход в систему от имени и с правами пользователя **Admin**	Загрузка рабочего стола
2	Создать файлы: - D:\M1\test1.txt; - D:\M1\test2.txt; - D:\M2\test3.txt; - D:\M2\test4.txt; - D:\M3\test5.txt; - D:\M3\test6.txt	Успешное создание указанных файлов
3	Запустить консоль администрирования СЗИ, в окне **«Список машин»** выбрать рабочую станцию 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	Неудачно

№ п/п	Действия	Ожидаемый результат
	изменения в файл и попытаться сохранить	
8	Сохранить измененный файл *D:\M1\test2.txt* в *D:\M2*	Сохранение файла
9	Перезагрузить рабочую станцию, выполнить вход в систему 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	Выполнить вход в систему от имени и с правами пользователя **User2** и мандатной меткой ***2,Public,Work***	Загрузка рабочего стола
14	Попытаться прочитать файлы D:\M3\test5.txt и D:\M3\test6.txt	Неудачно
15	Перезагрузить рабочую станцию, выполнить вход в систему от имени и с правами пользователя **Admin**, запустить консоль администрирования СЗИ	Загрузка рабочего стола и открытие консоли администрирования СЗИ
16	Установить дискреционные права доступа на директорию *D:\M3* для пользователя **User2**: D:\M3\ = **R/W**	Отображение установленных прав доступа
17	Перезагрузить ЭВМ1, вход в систему от имени и с правами пользователя **User2** и мандатной меткой ***2,Public,Work***	Загрузка рабочего стола
18	Прочитать файл D:\M3\test5.txt	Успешно
19	Прочитать файл D:\M3\test6.txt	Успешно
20	Скопировать файлы D:\M3\test5.txt и D:\M3\test6.txt в D:\M2	Успешно
21	Перезагрузить рабочую станцию, выполнить вход в систему от имени и с правами пользователя **Admin**, запустить консоль администрирования СЗИ	Загрузка рабочего стола и открытие консоли администрирования СЗИ
22	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»**	Появление сообщений, фиксирующих произведенные изменения настроек и попытки

№ п/п	Действия	Ожидаемый результат
	выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	доступа к контролируемым объектам

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 функции установки мандатной метки автовхода

Описание функции

Для упрощения процесса эксплуатации СЗИ, в состав механизмов внесена функция установки иерархической мандатной метки автовхода пользователя в ОС (без неиерархических категорий). При использовании в СВТ автовхода пользователя в операционную систему сеансу пользователя присваивается не наименьшая иерархическая метка, а та, которую установит администратор.

Действия

Проверка выполняется на основе действий, выполненных в п. 1.1.2.1 (см. таблицу П4.11).

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

Таблица П4.16 – Действия при проверке функции установки мандатной метки автовхода пользователя в ОС.

№ п/п	Действия	Ожидаемый результат
	Выполнить вход в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
	Удалить из списка объектов мандатной категории Secret директорию D:\M3\	Успешное удаление D:\M3\ из списка объектов мандатной категории Secret
	Удалить из списка объектов мандатной категории Work директории D:\M2\ и D:\M3\	Успешное удаление D:\M2\ и D:\M3\ из списка объектов мандатной категории Work
	Удалить из списка объектов мандатной категории Public директории D:\M1\, D:\M2\ и D:\M3\	Успешное удаление D:\M1\, D:\M2\ и D:\M3\ из списка объектов мандатной категории Public
	Настроить функцию Автовход для пользователя User1 с мандатной меткой 1	

№ п/п	Действия	Ожидаемый результат
	Запуск консоли администрирования СЗИ	Открытие окна консоли администрирования СЗИ
	В окне «Список машин» выбрать рабочую станцию, в окне «Настройки машины» выделить параметр Параметры	В Основной панели настроек клиентов отображены системные настройки выбранного клиента СЗИ
	Отметить поле Параметры автовхода	В Основной панели настроек клиентов появились поля ввода идентификационных данных пользователя СЗИ
	Заполнить открывшиеся поля ввода идентификационными данными пользователя User1. Сохранить настройки, нажав кнопку Сохранить параметры.	Открытие информационного окна с сообщением об успешном сохранении настроек.
	Вызвать процедуру перезагрузки ОС	Загрузка операционной системы под именем User1 с мандатной меткой 1
	Открыть папку D:\M1	Успешно
	Прочитать файл D:\M1\test1.txt	Успешно
	Внести изменения в файл D:\M1\test1.txt и попытаться сохранить его в папки D:\M2 и D:\M3	Неудачно
	Открыть папки: D:\M2 D:\M3	Нет доступа
	Выполнить вход в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
	В соответствии с действиями, описанными в п.5, настроить функцию Автовход для пользователя User2 с иерархической мандатной меткой 2	Успешное сохранение настроек
	Вызвать процедуру перезагрузки ОС	Загрузка операционной системы и вход в нее под именем User2 с мандатной меткой 2
	Открыть папку D:\M1	Успешно
	Прочитать файл D:\M1\test1.txt	Успешно
	Внести изменения в файл D:\M1\test1.txt и попытаться сохранить его в папки D:\M1 и D:\M3	Неудачно
	Сохранить измененный файл D:\M1\test1.txt в папку D:\M2	Успешно
	Открыть папку D:\M3	Нет доступа

№ п/п	Действия	Ожидаемый результат
	Выполнить вход в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
	В соответствии с действиями, описанными в п.5, настроить функцию Автовход для пользователя User3 с мандатной меткой 3	Успешное сохранение настроек
	Вызвать процедуру перезагрузки ОС	Загрузка операционной системы под именем User3 с мандатной меткой 3
	Открыть папку D:\M1	Успешно
	Прочитать файл D:\M1\test1.txt	Успешно
	Внести изменения в файл D:\M1\test1.txt и попытаться сохранить его в папки D:\M1 и D:\M2	Нет доступа
	Сохранить измененный файл D:\M1\test1.txt в папку D:\M3	Успешно

Критерии оценки

Положительные результаты при проверке настоящего пункта методики являются достаточным признаком для принятия решения о соответствии реализации проверяемого механизма требованиям руководящего документа и документации на СЗИ.

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. 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 П4.17.

Таблица П4.17 – Действия при проверке очистки внешней памяти

№ п/п	Действия	Ожидаемый результат
1	Войти в систему 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	Запустить консоль администрирования СЗИ»	Открытие консоли администрирования СЗИ
5	Для рабочей станции в окне «Настройки машины» раскрыть дерево Список пользователей →User1→Дискреционный. Добавить в ПРД файл D:\TestDel.txt, установить атрибут его гарантированного удаления и аудит.	Файл добавлен, атрибут гарантированного удаления и аудит установлены
6	Перезагрузить рабочую станцию, 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>	Файл удален. «Корзина» пуста
10	Выполнить с помощью программного средства «TERRIER 3.0» (WinHex) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность не найдена
11	Перегрузить рабочую станцию, войти в	Загрузка ОС. Появление рабочего стола

№ п/п	Действия	Ожидаемый результат
	систему под именем и с правами пользователя Admin	
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 диске D:\	Тестовая последовательность найдена
14	Запустить консоль администрирования СЗИ»	Открытие консоли администрирования СЗИ
15	Для рабочей станции в окне «Настройки машины» раскрыть дерево Список пользователей →User1→Дискреционный. Добавить в ПРД файловый объект D:\$RECYCLE.BIN, установить атрибут его гарантированного удаления и аудит.	Объект добавлен, атрибуты гарантированного удаления и аудит установлены
16	Перезагрузить рабочую станцию, 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	Файл TestDel.txt удален. «Корзина» пуста
19	Выполнить с помощью программного средства «TERRIER 3.0» (WinHex) поиск указанной тестовой последовательности на диске D:\	Тестовая последовательность не найдена
20	Перезагрузить рабочую станцию, выполнить вход в систему от имени и с правами пользователя Admin, запустить консоль администрирования СЗИ	Загрузка рабочего стола и открытие консоли администрирования СЗИ
21	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию,	Появление сообщений, фиксирующих успешные попытки доступа к контролируемому объекту

№ п/п	Действия	Ожидаемый результат
	нажать кнопку Выполнить запрос.	

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 возможности 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 П4.18.

Таблица П4.18 – Действия при проверке очистки оперативной памяти

№ п/п	Действия	Ожидаемый результат
1	**Настройка механизма очистки оперативной памяти**	
1.1	Войти в систему 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 рабочую станцию, в окне **«Настройки машины»** выбрать пункт ***Очистка памяти***. 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*	Появление выбранного процесса в *Списке контролируемых объектов* в **Основной**

№ п/п	Действия	Ожидаемый результат
	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.	**панели настроек клиентов**
1.5	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Новые настройки сохраняются в базе данных СЗИ.
2	**Проверка механизма очистки памяти**	
2.1	В свойствах компьютера 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 рабочую станцию, 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; 2) процесс механизма очистки памяти GIS.Client.MemoryCleaner.exe; В открытом диалоговом окне контролируемого приложения нажать кнопку ***Завершить программу***, при этом следить в диспетчере задач за процессом механизма очистки памяти и дождаться его завершения	Создание файла C:\test_message.txt Изменение в диспетчере задач показателя загрузки центрального процессора, происходящего в результате работы механизма очистки памяти
2.5	Запустить приложение NotMyFault.exe для	Появление синего экрана.

№ п/п	Действия	Ожидаемый результат
	выполнения критической ошибки системы	Перезагрузка операционной системы
2.6	Открыть файл C:\test_message.txt	Открытие файла
2.7	Запустить программное средство TERRIER (WinHex)	Открытие диалогового окна программного средства TERRIER (WinHex)
2.8	Выполнить с помощью программного средства TERRIER (WinHex) поиск на диске D:\ фрагмента тестового файла C:\test_message.txt (включая дамп памяти D:\MEMORY.DMP)	Последовательность не найдена
2.9	В консоли администрирования СЗИ в окне **«Список машин»** выбрать рабочую станцию, в окне **«Настройки машины»** выбрать пункт ***Аудит***	Появление сообщений, фиксирующих события очистки памяти

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.

При этом 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 П4.19.

Таблица П4.19 – 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 от имени и с правами пользователя **Admin**. Создать документы с произвольным содержимым: C:\print1.doc, C:\print1.txt; 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 рабочую станцию. Отредактировать параметры мандатного механизма – файлам print1.doc и print1.txt присвоить иерархическую мандатную метку ***1***, файлу print2.doc – иерархическую мандатную метку ***2***	Успешное присвоение мандатных меток
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*	Успешная настройка параметров
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); - текстовый редактор Блокнот (C:\Windows\System32\Notepad.exe).	Список объектов, печать из которых контролируется СЗИ. Отображение произведенных настроек

№ п/п	Действия	Ожидаемый результат
	Разрешить печать из приложения Winword.exe, установив флажок в поле ***Разрешение*** напротив приложения.	
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 настроить их.	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: 1) C:\Blockhost\PrintControl\BlockHost.dot; 2) C:\Users\user1\AppData\Roaming\Microsoft\Шаблоны\Normal.dot	Отображение произведенных настроек
1.8	В консоли администрирования СЗИ 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*	Успешная настройка параметров
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); -блокнот (C:\Windows\System32\Notepad.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*	Отображение окна «Редактирование настроек шаблона печати». Отображение произведенных настроек

№ п/п	Действия	Ожидаемый результат
	В окне **«Редактирование настроек шаблона печати»** выбрать все маркеры, отметив флажками соответствующие поля, и настроить их.	
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***	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**
2.4	Открыть с помощью приложения Notepad.exe документ print1.txt и отправить документ на печать	Документ доступен для записи, чтения. Отказ печати документа
2.5	Запустить приложение Winword.exe и попытаться открыть файл print2.doc для последующей печати	Невозможность открытия файла print2.doc
2.6	Вход в систему от имени и с правами пользователя **User2** и мандатной меткой ***1***	Загрузка рабочего стола
2.7	Включить все макросы в настройках MS Office в пункте меню Файл →Параметры →Центр управления безопасностью →Параметры центра управления безопасностью →Параметры макросов	Успешное включение макросов
2.8	Открыть с помощью приложения	Документ доступен для записи, чтения.

№ п/п	Действия	Ожидаемый результат
	Notepad.exe документ print1.txt и отправить документ на печать	Отказ печати документа
2.9	Запустить приложение Winword.exe и попытаться открыть файл print2.doc для последующей печати	Невозможность открытия файла print2.doc
3	**Просмотр событий аудита**	
3.1	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих успешные и неудачные попытки вывода информации на печать

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 в соответствии с Инструкцией по обеспечению режима секретности в Российской Федерации № 3–1 от 05.01.2004;
- 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 П4.20.

Таблица П4.20 – 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 от имени и с правами пользователя Admin	Загрузка рабочего стола
2	Запустить консоль администрирования СЗИ	Открытие серверной консоли администрирования
3	В серверной консоли администрирования в окне «Список машин» выбрать сервер безопасности. В окне «Настройки машины» выбрать пункт Мандатный механизм.	В Основной панели настроек клиентов отображаются существующие мандатные метки
4	Создать иерархическую мандатную метку с именем 4 и значением 4	Добавление метки
5	В Основной панели настроек клиентов выделить метку 4	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
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
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	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, 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 удаленного объекта при работе в «помеченном» канале связи

Описание функции

СЗИ «Блокхост-Сеть 3» должно обеспечивать при работе в сети соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой удаленного объекта при работе с «помеченным» каналом связи.

Действия

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.21.

Таблица П4.21 – 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	Создание на рабочей станции объектов файловой системы и присвоение им уровней конфиденциальности согласно таблице П4.10 настоящего Приложения (в случае, если объекты отсутствуют)		Объекты файловой системы успешно созданы. Соответствующие уровни конфиденциальности присвоены
2	**Осуществление санкционированных и несанкционированных попыток доступа к контролируемым объектам доступа**		
2.1	Выполнить вход в систему от имени и с правами пользователя **User2** и значением мандатной метки ***2,Public,Work***		Загрузка рабочего стола
2.2	Чтение	D:\M1\read.txt	Успешно
		D:\M2\read.txt	Успешно
		D:\M3\read.txt	Неудачно
2.3	Копирование:	D:\M1\copy.txt	Неудачно
		D:\M2\copy.txt	Успешно
		D:\M3\copy.txt	Неудачно
2.4	Переименование:	D:\M1\ren.txt	Неудачно

№ п/п	Действия		Ожидаемый результат
		D:\M2\ren.txt	Успешно
		D:\M3\ren.txt	Неудачно
2.5	Перемещение	D:\M1\move.txt	Неудачно
		D:\M2\move.txt	Успешно
		D:\M3\move.txt	Неудачно
2.6	Удаление:	D:\M1\del.txt	Неудачно
		D:\M2\del.txt	Успешно
		D:\M3\del.txt	Неудачно
2.7	Перезагрузить рабочую станцию		Перезагрузка рабочую станцию
3	**Просмотр событий аудита**		
3.1	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль Системы развертывания и аудита		Открытие консоли Системы развертывания и аудита
3.2	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***.		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

Результаты тестирования

Проверка считается успешной, если СЗИ обеспечивает соответствие 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»

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 П4.22.

Таблица П4.22 – 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 рабочей станции USB-накопитель	Идентификация накопителя ОС
2	Выполнить 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 рабочую станцию, в окне **«Настройки машины»** выбрать пункт ***Мандатный механизм***.	Появление в **Основной панели настроек клиентов** параметров мандатного механизма
7	Создать иерархическую мандатную метку ***4***. Присвоить мандатную метку ***4*** подключенному к рабочей станции USB-накопителю	Метка успешно присвоена
8	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Сохранение настроек
9	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих присвоение мандатной метки USB-накопителю

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 П4.23.

Таблица П4.23 – 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 от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Запуск консоли администрирования СЗИ
1.2	В окне **«Список машин»** выбрать рабочую станцию. Добавить пользователей **User1** – **User6** (если они отсутствуют в базе данных СЗИ)	Добавление пользователей в базу данных СЗИ
2	**Задание ПРД устройствам и портам рабочей станции**	
2.1	Создание матрицы ПРД	Определение матрицы ПРД

<table>
<tr><th>№ п/п</th><th>Действия</th><th>Ожидаемый результат</th></tr>
<tr><td></td><td>
<table>
<tr><td rowspan="2">Пользова-тель</td><td colspan="4">Устройства/Порты</td></tr>
<tr><td>CD/ DVD</td><td>LPT</td><td>COM</td><td>USB</td></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></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 клиентов для пользователя User1 установить ПРД к портам и CD-ROM, согласно матрице ПРД, и аудит</td><td>Появление в Основной панели настроек клиентов 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 клиентов для пользователя User2 установить ПРД к портам и CD-ROM и аудит</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 клиентов для пользователя User3 установить ПРД к портам и CD-ROM и аудит</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 клиентов для пользователя User4 установить ПРД к портам и CD-ROM и аудит</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 клиентов для пользователя User5 установить ПРД к</td><td>Отображение ПРД пользователя User5</td></tr>
</table>

№ п/п	Действия	Ожидаемый результат
	портам и CD-ROM и аудит	
2.7	В окне «Настройки машины» раскрыть дерево Список пользователей →User6 →Контроль портов и CD. В **Основной панели настроек клиентов** для пользователя **User6** установить ПРД к портам и CD-ROM и аудит	Отображение ПРД пользователя **User6**
2.8	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Сохранение настроек
2.9	Запустить консоль «Системы развертывания и аудита». В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***.	Появление сообщений, фиксирующих произведенное изменение настроек
3	**Проверка доступа пользователей к устройствам и портам рабочей станции**	
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 принтер (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 рабочую станцию	Перезагрузка рабочей станции
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 принтер (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 рабочую станцию	Перезагрузка рабочей станции
3.7	Выполнить вход в систему от имени и с правами пользователя **User3**	Загрузка рабочего стола
3.8	Чтение файла с CD-ROM	Неудачно

№ п/п	Действия	Ожидаемый результат
	Печать на принтер (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Успешно
3.9	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
3.10	Выполнить вход в систему от имени и с правами пользователя **User4**	Загрузка рабочего стола
3.11	Чтение файла с CD-ROM	Неудачно
	Печать на принтер (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
3.12	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
3.13	Выполнить вход в систему от имени и с правами пользователя **User5**	Загрузка рабочего стола
3.14	Чтение файла с CD-ROM	Неудачно
	Печать на принтер (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
3.15	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
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 принтер (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
3.18	Перезагрузить рабочую станцию	Перезагрузка рабочей станции

№ п/п	Действия	Ожидаемый результат
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
4.2	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

Результаты тестирования

Проверка считается успешной, если пользователю обеспечен вывод информации:

- на произвольно используемое устройство;
- на идентифицированное устройство.

1.5.2. Проверка механизма (в идентифицированном СЗИ «Блокхост-Сеть 3»), посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству

Описание функции

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 разрешенных для использования на ЭВМ USB-накопителей к пользователям.

Действия

Проверка выполняется согласно и на основании действий, выполненных в п. 1.4.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П4.24.

Таблица П4.24 – Действия при проверке механизма (в идентифицированном СЗИ «Блокхост-Сеть 3»), посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству

№ п/п	Действия	Ожидаемый результат
1	Войти в систему 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 рабочую станцию. В окне «Настройки машины» раскрыть дерево Список пользователей →User1 →Контроль	Появление в Основной панели настроек клиентов всех доступных портов и CD

№ п/п	Действия	Ожидаемый результат
	портов и CD.	
4	Подключить к USB портам рабочей станции два USB-накопителя	Идентификация накопителей 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: 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: 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	Сохранение настроек
11	Создать файлы C:\iotest1.txt и C:\iotest2.txt с произвольным содержимым	Создание файлов
12	Войти в систему от имени и с правами пользователя User1	Загрузка рабочего стола
13	Скопировать файл C:\iotest1.txt на оба USB-накопителя	Успешное копирование файла
14	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
15	Войти в систему от имени и с правами пользователя User2	Загрузка рабочего стола
16	Скопировать файл C:\iotest2.txt на оба USB-накопителя	Работа с запрещенным USB-накопителем невозможна
17	Перезагрузить рабочую станцию	Перезагрузка рабочей станции

№ п/п	Действия	Ожидаемый результат
18	Войти в систему от имени и с правами пользователя Admin. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита».
19	В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам

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 в СЗИ должны быть предусмотрены ограничения на минимальную длину пароля (минимальная длина – 8 символов), а также на время доступа пользователя в систему.

Действия

С помощью консоли администрирования в базе данных СЗИ регистрируется группа пользователей с указанными ниже параметрами учетных записей и выполняется последовательность действий для проверки (таблица П4.25).

Таблица П4.25 – Управление учетными записями пользователей

№ п/п	Действия	Ожидаемый результат
1	**Проверка возможности добавления учетных записей пользователей**	
1.1	Войти в систему от имени и с правами пользователя Admin. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
1.2	В окне «Список машин» выбрать рабочую станцию, в окне «Настройки машины» выбрать пункт Список пользователей. Выбрать пункт главного меню Управление пользователями →Добавить пользователей.	Появление окна «Добавление пользователей»
1.3	Добавить пользователя User7 (мандатная метка входа 2). Задать пароль пользователя длиной 8 символов	Успешное добавление пользователя User7, пароль задан.
1.4	Добавить пользователя User8 (мандатная метка входа 1). Попытаться задать пароль пользователя длиной 7 символов. Задать пароль длиной 8 символов	Успешное добавление пользователя User8, пароль длиной 7 символов не задан. Пароль длиной 8 символов задан.
1.5	Добавить пользователя User10 (мандатная метка входа 1). Задать пароль пользователя длиной 9 символов	Успешное добавление пользователя User10, пароль задан.

№ п/п	Действия	Ожидаемый результат
2	**Проверка возможности изменения имени учетной записи пользователя**	
2.1	В окне «Настройки машины» выделить параметр Список пользователей. В Основной панели настроек клиентов выделить пользователя User7 и выбрать пункт меню Управление пользователями →Изменение пользователя	Появление окна «Изменение пользователя»
2.2	Изменить имя пользователя User7 на User2	Предупреждение о существовании пользователя с именем User2 в СЗИ – имя пользователя не изменяется
2.3	Изменить имя пользователя на User9	Сообщение об успешном изменении настроек пользователя
2.4	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	Сохранение настроек
2.5	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос	Появление сообщений аудита, фиксирующих изменение настроек СЗИ.

Методика проверки выполненных в таблице П4.25 действий приведена в таблице П4.26.

Таблица П4.26 – 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 от имени и с правами несанкционированного пользователя **User11**	Запрет входа в систему
1.2	Выполнить попытку входа в систему 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 от	Запрет входа в систему

№ п/п	Действия	Ожидаемый результат
	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	
1.4	Выполнить попытку входа в систему 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
1.5	Выполнить попытку входа в систему 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
1.6	Выполнить попытку входа в систему 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
1.7	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
1.8	Выполнить попытку входа в систему от имени и с правами санкционированного пользователя **User9**.	Вход в систему

№ п/п	Действия	Ожидаемый результат
	Указать: 1) верный пароль; 2) верный идентификатор входа; 3) верный PIN-код идентификатора входа; 4) верную **мандатную метку** входа, равную **«1»**	
1.9	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
1.10	Выполнить попытку входа в систему 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
1.11	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
1.12	Выполнить попытку входа в систему 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	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита».	Открытие консоли «Системы развертывания и аудита».
1.14	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
2	**Проверка возможности изменения пароля пользователями без привлечения администратора безопасности СЗИ**	
2.1	Войти в систему от имени и с правами пользователя **User9**	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
2.2	Нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**	Появление диалога выбора действий ОС Windows
2.3	Нажать ссылку ***Смена пароля***.	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 подтверждения 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 ***Смена пароля***	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); - повторить ввод нового пароля в поле ввода ***Подтвердите пароль***; - в поле ввода ***PIN-код*** ввести PIN-код доступа к ключевому носителю. Нажать кнопку подтверждения для запуска процедуры изменения пароля.	Пароль изменен. Загрузка рабочего стола.
2.8	Нажать комбинацию клавиш **<Ctrl>+<Alt>+<Del>**	Появление диалога выбора действий ОС Windows
2.9	Нажать кнопку ***Смена пароля***	Появление диалогового окна **«Смена пароля»**
2.10	Заполнить поля диалога: - в поле ввода ***Старый пароль*** ввести текущий пароль; - в поле ввода ***Новый пароль*** ввести новый пароль (длиной 9 символов); - повторить ввод нового пароля в поле ввода ***Подтвердите пароль***; - в поле ввода ***PIN-код*** ввести PIN-код	Пароль изменен. Загрузка рабочего стола.

№ п/п	Действия	Ожидаемый результат
	доступа к ключевому носителю. Нажать кнопку ***Изменить пароль*** для запуска процедуры изменения пароля	
2.11	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
2.12	Попытаться войти в систему от имени и с правами пользователя **User9** с указанием пароля длиной 7 символов	Вход в систему невозможен
2.13	Попытаться войти в систему от имени и с правами пользователя **User9** с указанием старого пароля длиной 8 символов	Вход в систему невозможен
2.14	Попытаться войти в систему от имени и с правами пользователя **User9** с указанием нового пароля длиной 9 символов (измененного через диалог **«Смена пароля»**)	Успешный вход пользователя в систему
2.15	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
2.16	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита».	Открытие консоли «Системы развертывания и аудита».
2.17	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
3	**Проверка возможности изменения пароля пользователя администратором безопасности СЗИ**	
3.1	В консоли администрирования СЗИ в окне **«Настройки машины»** выбрать пункт ***Список пользователей***	В **Основной панели настроек клиентов** отображается список пользователей
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***	Сохранение настроек

№ п/п	Действия	Ожидаемый результат
	→***Сохранить***	
3.5	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
3.6	Попытаться войти в систему от имени и с правами пользователя **User10** с указанием старого пароля	Вход в систему невозможен
3.7	Попытаться войти в систему от имени и с правами пользователя **User10** с указанием нового пароля (измененного через диалоговое окно консоли администрирования СЗИ **«Изменение пароля пользователя»**)	Успешный вход пользователя в систему
3.8	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
3.9	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита».	Открытие «Системы развертывания и аудита».
3.10	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
3.11	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
4	**Проверка возможности изменения PIN-кода идентификаторов входа пользователей администратором безопасности СЗИ**	
4.1	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
4.2	Подключить ключевой носитель пользователя к рабочей станции	Идентификация ключевого носителя средствами ОС рабочей станции
4.3	В консоли администрирования СЗИ 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***, ввести новые данные в окно смены PIN-кода и нажать кнопку ***Изменить***	Успешная смена PIN-кода

№ п/п	Действия	Ожидаемый результат
4.6	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Сохранение настроек
4.7	Повторить пункты 5.2 – 5.6 для всех поддерживаемых в СЗИ идентификаторов входа	Совпадение полученных результатов с приведенными выше результатами
4.8	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
4.9	Попытаться войти в систему от имени и с правами пользователя **User9** с указанием старого PIN-кода	Вход в систему невозможен
4.10	Попытаться войти в систему от имени и с правами пользователя **User9** с указанием нового PIN-кода	Успешный вход пользователя в систему
4.11	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
4.12	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита».
4.13	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
5	**Проверка возможности удаления учетной записи пользователя**	
5.1	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
5.2	В консоли администрирования СЗИ в окне **«Список машин»** выбрать рабочую станцию, в окне **«Настройки машины»** выбрать пункт ***Список пользователей***	В **Основной панели настроек клиентов** отображается список пользователей
5.3	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
5.4	Подтвердить удаление пользователя	Пользователь удален из СЗИ
5.5	Сохранить произведенные настройки, выбрав пункт меню ***Главная***	Сохранение настроек

№ п/п	Действия	Ожидаемый результат
	→***Сохранить***	
5.6	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
5.7	Попытаться войти в систему от имени и с правами пользователя **User10**	Вход в систему невозможен
5.8	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
5.9	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита»
5.10	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему
6	**Проверка возможности временного ограничения на вход пользователей в систему**	
6.1	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 временно́го контроля
6.2	Установить параметры ***Вести аудит временных разрешений***, ***Включить временные ограничения*** и установить разрешение на работу по средам с 08:00 до 14:00	Успешное задание настроек
6.3	Сохранить произведенные настройки, выбрав пункт меню ***Главная*** →***Сохранить***	Сохранение настроек
6.4	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
6.5	Попытаться войти в систему от имени и с правами пользователя **User9**	Вход в систему невозможен
6.6	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль администрирования СЗИ	Открытие консоли администрирования СЗИ
6.7	В консоли администрирования в окне **«Список машин»** выбрать рабочую станцию, в окне **«Настройки машины»** раскрыть дерево ***Список пользователей***→ ***User9*** выбрать пункт ***Ограничение по времени***	В **Основной панели настроек клиентов** отображаются настройки механизма временно́го контроля

№ п/п	Действия	Ожидаемый результат
6.8	Установить разрешение на работу по средам с 08:00 до 18:00	Успешное изменение настроек
6.9	Сохранить произведенные настройки, выбрав пункт меню ***Главная →Сохранить***	Сохранение настроек
6.10	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
6.11	Попытаться войти в систему от имени и с правами пользователя **User9**	Успешный вход пользователя в систему
6.12	Перезагрузить рабочую станцию	Перезагрузка рабочей станции
6.13	Войти в систему от имени и с правами пользователя **Admin**. Запустить консоль «Системы развертывания и аудита».	Открытие консоли «Системы развертывания и аудита».
6.14	В окне выбрать **«Мониторинг»** выбрать рабочую станцию, нажать кнопку ***Выполнить запрос***	Появление сообщений аудита, фиксирующих попытки входа пользователей в систему

Результаты тестирования

Результаты проверки считаются положительным, если:

- при вводе имени пользователя, предъявлении зарегистрированного ключевого носителя и верного пароля осуществляется вход в систему;
- при предъявлении незарегистрированного ключевого носителя или ввода неверного пароля появляется приглашение вновь предъявить права на вход в систему, а в случае, если количество попыток входа для пользователя превысило максимальное число попыток входа, равное трем, то 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 блокирует возможность задания пароля пользователя длиной менее 8 буквенно-цифровых символов.

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.

Журнал содержит всю информацию 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 связанных с попытками аутентификации событий, а также отправку их на SIEM.

Действия

Проверка выполняется на основании действий, выполненных в п. 1.6.1. Журнал содержит информацию об использовании идентификационного и аутентификационного механизмов (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 согласно действиям, произведенным в п. 1.1.1.1, 1.1.2.1. Журнал содержит информацию о запросах на доступ к защищаемому ресурсу (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 доступом к защищаемым ресурсам, 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).

1.7.3 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 П4.27.

Таблица П4.27 – Действия при проверке регистрации создания и уничтожения объекта

№ п/п	Действия	Ожидаемый результат
1	Войти в систему 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 рабочую станцию, в окне «Настройки машины» раскрыть дерево Список пользователей→ User1 выбрать пункт Дискреционный. Установить на контроль D:\, 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 доступаПрисвоить мандатную метку 1 объекту D:\	В Основной панели настроек клиентов установлены настройки мандатного механизма
5	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	Сохранение настроек
6	Войти в систему от имени и с правами пользователя User1	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
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	Войти в систему от имени и с правами пользователя Admin. Запустить консоль «Системы развертывания и аудита»	Открытие консоли «Системы развертывания и аудита».
12	В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос	Наличие информации о действиях с объектом доступа

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» содержит средство выборочного ознакомления с регистрационной информацией, которое позволяет гибко работать с журналом.

Действия

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

Таблица П4.28 – 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 администрирования СЗИ	Открытие консоли администрирования СЗИ
3	В окне «Список машин» выбрать рабочую станцию, в окне «Настройки машины» выбрать пункт Аудит. В главном меню выбрать пункт Аудит →Фильтр	Отображение сообщений аудита о работе модулей СЗИ в Основной панели настроек клиентов. Появление окна «Настройки фильтра»
4	В окне «Настройки фильтра» выбрать пункты и критерии, согласно которым будет выполнена фильтрация. Нажать кнопку Ок	В Основной панели настроек клиентов будут отображены только сообщения, которые отвечают критериям фильтра

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 П4.29.

Таблица П4.29 – 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
3	В консоли администрирования СЗИ в окне «Список машин» выбрать рабочую станцию, в окне «Настройки машины» выбрать пункт Мандатный механизм. Задать мандатные метки с ведением аудита для файлов: - C:\LogTest\test1.txt – мандатную метку 1; - C:\LogTest\test2.txt – мандатную метку 2	Правила 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 дискреционного доступа заданы
5	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	Сохранение настроек
6	Перезагрузить рабочую станцию	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 компьютер	Появление интерфейса СЗИ

№ п/п	Действия	Ожидаемый результат
		«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 компьютер	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 рабочую станцию, нажать кнопку Выполнить запрос	Отображены сведения обо всех действиях пользователей и для каждого события содержит дату и время, субъект, тип, статус

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 П4.30.

Таблица П4.30 – 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 руководства 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 рабочую станцию, 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 появились настройки механизмов СЗИ выбранной ЭВМ

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 П4.31.

Таблица П4.31 – Действия при проверке наличия стандартизированного интерфейса пользователя

№ п/п	Действия	Ожидаемый результат
1	Включить рабочую станцию	Появление интерфейса СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
2	Убедиться, что интерфейс процесса аутентификации пользователя 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

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 П4.32.

Таблица П4.32 – Действия при проверке обеспечения надежности интерфейса

№ п/п	Действия	Ожидаемый результат
1	Включить рабочую станцию	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:	Появление интерфейса СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
	- включить рабочую станцию; - войти в систему от имени и с правами пользователя Admin; - открыть консоль администрирования СЗИ; - обеспечить аварийное завершение, путем симуляции сбоя по питанию	
4	Включить рабочую станцию	Появление интерфейса СЗИ «Блокхост-Сеть 3»

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 П4.33.

Таблица П4.33 – Действия при проверке логического изолирования интерфейса пользователя и СЗИ от других таких же интерфейсов

№ п/п	Действия	Ожидаемый результат
1	Включить рабочую станцию	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.

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 П4.34.

Таблица П4.34 – 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 ЭВМ	Появление интерфейса СЗИ
2	Войти в систему от имени и с правами Admin	Загрузка рабочего стола
3	Проверить работоспособность СЗИ	Механизмы защиты СЗИ функционируют
4	Выключение питания ЭВМ и включение его 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

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 П4.35.

Таблица П4.35 – Действия при проверке наличия периодического контроля целостности СЗИ «Блокхост-Сеть 3»

№ п/п	Действия	Ожидаемый результат
1	Войти в систему 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 рабочую станцию. В окне «Настройки машины» выбрать параметр Контроль целостности.	В Основной панели настроек клиента отобразились настройки механизма контроля целостности.
4	В Основной панели настроек клиента: - отметить параметр Включить контроль целостности; - в поле Периодичность контроля (чч:мм:сс) установить интервал 1 мин.	Механизм контроля целостности включен и установлена периодичность контроля равная 1 мин.
5	Сохранить произведенные настройки, выбрав пункт меню Главная →Сохранить	Изменения сохранены
6	В окне «Настройки машины» выбрать параметр Контроль целостности. Добавить следующие файлы (объекты) на контроль и отметить для каждого из них параметр Аудит: - C:\test.txt; - blockpost.sys; -GIS.BlockPost.GUI.exe; - GIS.Client.MemoryCleaner.exe; - GIS.Client.LogDispatcher.exe; - GIS.Client.IntegrityChecker.exe	Файлы поставлены на контроль. Пункт Аудит у каждого объекта активирован
7	Перезагрузить рабочую станцию	Загрузка операционной системы
8	Внести изменения в файл c:\test.txt	Изменения внесены и сохранены
9	С помощью программы WinHEX внести изменение в файл blockpost.sys и сохранить	Изменения внесены и сохранены

№ п/п	Действия	Ожидаемый результат
10	Перезагрузить рабочую станцию	Загрузка операционной системы
11	Открыть blockpost.sys программой WinHEX и убедиться, что файл восстановлен к исходному состоянию	В файле не содержится внесенных изменений
12	Открыть файл C:\test.txt и убедиться, что файл восстановлен	В файле не содержится внесенных изменений
13	Запустить консоль «Системы развертывания и аудита». В окне выбрать «Мониторинг» выбрать рабочую станцию, нажать кнопку Выполнить запрос	Наличие записей об успешном восстановлении файлов, поставленных на контроль

Результаты тестирования

Проверка считается успешной, если обеспечивается контроль целостности программной и информационной частей СЗИ и полное восстановление свойств СЗИ при нарушении целостности файлов СЗИ.

1.10.2 Проверка выполнения программ в отдельной части оперативной памяти

Описание функции

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

Действия

Выполняется средствами ОС.

Результаты тестирования

Обеспечивается средствами ОС.