

Средство защиты информации от несанкционированного доступа
«Блокхост-Сеть 4»

Руководство администратора безопасности
Часть 1. Управление политиками
Приложение 3

Содержание

Введение	5
1 Условия проведения регламентного тестирования	6
1.1 Материально-техническое и инструментальное обеспечение испытаний	6
1.2 Настройка виртуальной тестовой среды	6
1.3 Настройка параметров сервера безопасности	8
2 Регламентное тестирование СЗИ от НСД «Блокхост-Сеть 4»	9
2.1 Проверка установки СЗИ	12
2.1.1 Проверка установки клиентских частей СЗИ с использованием агента подсистемы развертывания	14
2.1.2 Проверка возможности установки внешних продуктов через подсистему развертывания	18
2.1.3 Проверка возможности установки клиентских и серверных частей СЗИ в виртуальной сети и создание иерархии серверов безопасности	19
2.1.4 Проверка взаимной аутентификации клиентов с сервером СЗИ при их сетевом взаимодействии	23
2.1.5 Проверка контрольных сумм неизменных файлов установленного СЗИ от НСД «Блокхост-Сеть 4»	25
2.2 Проверка подсистемы развертывания	26
2.3 Проверка дискреционного принципа контроля доступа	27
2.3.1 Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа	27
2.3.2 Проверка наличия механизма, претворяющего в жизнь дискреционные ПРД, как для явных, так и для скрытых действий пользователя	38
2.3.3 Проверка предоставления прав санкционировано изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.), в том числе изменения списка пользователей СВТ	39
2.3.4 Проверка контроля запуска процессов по модели разрешенных процессов	44
2.3.5 Проверка контроля запуска программ и файлов (аудит доступа к медиафайлам)	49
2.3.6 Проверка контроля запуска исполняемого файла по маске его имени (аудит запуска приложений)	50
2.4 Проверка мандатного принципа контроля доступа	51
2.4.1 Проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта	51
2.4.2 Проверка запроса и получения классификационных меток при вводе новых данных в систему	57

2.4.3	Проверка реализации мандатного принципа контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов.....	58
2.4.4	Проверка возможности изменения классификационных уровней субъектов и объектов специально выделенными субъектами при реализации мандатных ПРД	60
2.4.5	Проверка реализации диспетчера доступа	62
2.5	Проверка управления СЗИ и иерархии серверов безопасности	64
2.6	Проверка очистки памяти	65
2.6.1	Проверка возможности очистки внешней памяти	65
2.6.2	Проверка возможности очистки оперативной памяти	76
2.6.3	Проверка возможности уничтожения информации на машинных носителях.....	81
2.7	Проверка маркировки документов	83
2.7.1	Проверка контроля печати и маркировки при выводе на печать документа, содержащего защищаемую информацию	83
2.8	Проверка защиты ввода и вывода информации на отчуждаемый физический носитель	86
2.8.1	Проверка возможности различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»)	86
2.8.2	Проверка обеспечения соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства	87
2.8.3	Проверка возможности изменения в назначении и разметке устройств только под контролем СЗИ от НСД «Блокхост-Сеть 4»	94
2.9	Проверка сопоставления пользователя с устройством	96
2.9.1	Проверка возможности обеспечить вывод информации на запрошенное пользователем устройство.....	96
2.9.2	Проверка механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству	101
2.10	Проверка идентификации и аутентификации пользователей	105
2.10.1	Проверка требования от пользователей идентифицировать себя при запросах на доступ и проверка подлинности идентификатора субъекта (аутентификации)	105
2.10.2	Проверка идентификации и аутентификации пользователей при удалённом доступе RDP	131
2.10.3	Проверка возможности аутентификации пользователей с использованием цифровых сертификатов	132
2.10.4	Проверка функционирования политики безопасности аутентификации в контроллере домена с использованием СЗИ от НСД «Блокхост-Сеть 4»	137
2.10.5	Проверка возможности идентификации и аутентификации пользователей в сети с иерархией серверов безопасности без контроллера домена.....	141

2.10.6	Проверка возможности надежно связывать полученную идентификацию со всеми действиями данного пользователя.....	143
2.11	Проверка регистрации	143
2.11.1	Проверка регистрации использования идентификационного и аутентификационного механизмов.....	143
2.11.2	Проверка регистрации запроса на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)	144
2.11.3	Проверка регистрации создания и уничтожения объекта	145
2.11.4	Проверка регистрации действий по изменению ПРД.....	146
2.11.5	Проверка наличия средств выборочного ознакомления с регистрационной информацией	147
2.11.6	Проверка регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).....	150
2.11.7	Проверка функциональных возможностей механизма регистрации событий безопасности.....	152
2.11.8	Проверка аудита событий, возникающих при задании/изменении настроек аудита	157
2.11.9	Проверка регистрации в автономном варианте СЗИ от НСД «Блокхост-Сеть 4»	158
2.11.10	Проверка передачи собранных событий безопасности с головного сервера СЗИ в SIEM-систему	160
2.12	Проверка надежного восстановления	161
2.12.1	Проверка полного восстановления свойств СЗИ от НСД «Блокхост-Сеть 4» после сбоев и отказов оборудования при использовании процедур восстановления .	161
2.13	Проверка целостности СЗИ от НСД «Блокхост-Сеть 4»	162
2.13.1	Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4»	162
2.13.2	Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4» с блокировкой доступа пользователя при нарушении целостности	166
2.13.3	Проверка регистрации событий, связанных с изменением целостности среды	168
2.13.4	Проверка регистрации событий, связанных с изменением аппаратной среды	170
2.14	Проверки работы с токенами (управление ЖЦ токенов).....	171

Введение

Настоящее приложение предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» и содержит описание проверок функциональных возможностей СЗИ от НСД «Блокхост-Сеть 4».

1 Условия проведения регламентного тестирования

1.1 Материально-техническое и инструментальное обеспечение испытаний

Для регламентного тестирования используется стенд, который представляет собой локально-вычислительную сеть (ЛВС), в которой пять ЭВМ объединяются между собой.

ЭВМ 2 – ЭВМ 4 являются рабочими станциями, ЭВМ 1 является сервером безопасности. ЭВМ 5 в зависимости от режима испытаний может являться как рабочей станцией, так и сервером безопасности.

Схема испытательного стенда представлена на рисунке ПЗ.1.

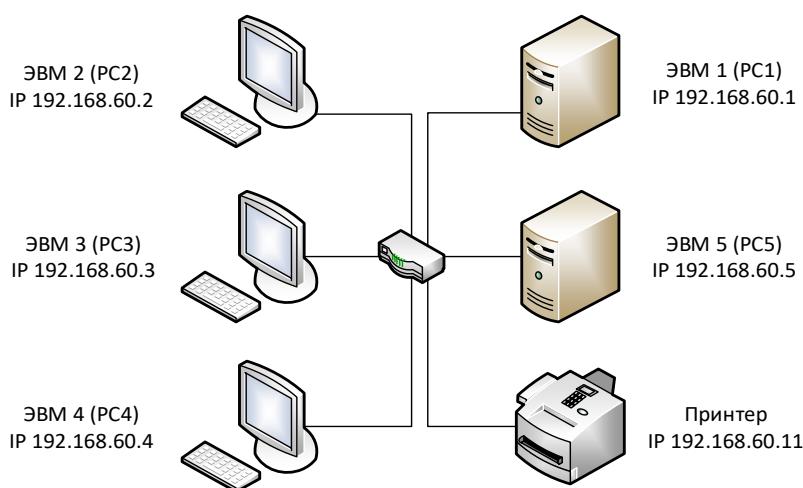


Рисунок ПЗ.1 – Схема стенда

1.2 Настройка виртуальной тестовой среды

Для проведения тестирования СЗИ внутри виртуальных машин, требуется установить на ЭВМ 2 программное обеспечение виртуализации VMware Workstation 15 Pro.

Средствами VMware Workstation 15 Pro создаются виртуальные машины с операционными системами согласно таблице ПЗ.1. На виртуальные машины с ОС MS Windows устанавливается клиентская часть СЗИ, на виртуальные машины с ОС семейства Linux устанавливается клиент управления.

Таблица ПЗ.1 – Состав ПО виртуальных машин

№	Имя	ОС	Серверная часть СЗИ	Клиентская часть СЗИ/клиент управления
1	Ser2008AD	Windows Server 2008R2 Datacenter	—	—
2	ЭВМ1 (PC1)	Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная)	+	+
3	ЭВМ2 (PC2)	Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная)		+
4	ЭВМ3 (PC3)	Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная)		+
5	ЭВМ4 (PC4)	Windows 7 Professional SP1 (32-разрядная/64-разрядная)	—	+
6	ЭВМ5 (PC5)	Windows 7 Enterprise SP1 (32-разрядная/64-разрядная)	—	+
7	ЭВМ6 (PC6)	Windows 7 Ultimate SP1 (32-разрядная/64-разрядная)	—	+
8	ЭВМ7 (PC7)	Windows 8.1 Core (32-разрядная/64-разрядная)	—	+
9	ЭВМ8 (PC8)	Windows 8.1 Professional (32-разрядная/64-разрядная)	—	+
10	ЭВМ9 (PC9)	Windows 8.1 Enterprise (32-разрядная/64-разрядная)	—	+
11	ЭВМ10 (PC10)	Windows 10 Home (32-разрядная/64-разрядная)	—	+
12	ЭВМ11 (PC11)	Windows 10 Pro (32-разрядная/64-разрядная)	—	+
13	ЭВМ12 (PC12)	Windows 10 Enterprise (32-разрядная/64-разрядная)	—	+
14	ЭВМ13 (PC13)	Windows Server 2016 Standard (64-разрядная)	+	+
15	ЭВМ14 (PC14)	Windows Server 2012/2012R2 Foundation (64-разрядная)	+	+
16	ЭВМ15 (PC15)	Astra Linux SE	—	+
17	ЭВМ16 (PC16)	Альт 8 СП	—	+
18	ЭВМ17 (PC17)	РЕД ОС (Муром)	+	+
19	ЭВМ18 (PC18)	РЕД ОС (Муром)	—	+

Виртуальная ЭВМ1 (PC1), в созданной виртуальной сети, выполняет функции головного сервера безопасности СЗИ от НСД «Блокхост-Сеть 4».

Для проведения тестирования функциональных возможностей СЗИ, создание иерархии серверов безопасности, установка серверной части СЗИ проводится последовательно на ЭВМ1 (PC1), ЭВМ17 (PC17) и ЭВМ14 (PC14) вручную, а установка клиентских частей СЗИ через подсистему развертывания и аудита.

Подчиненность клиентских СЗИ показана на рисунке ПЗ.2.

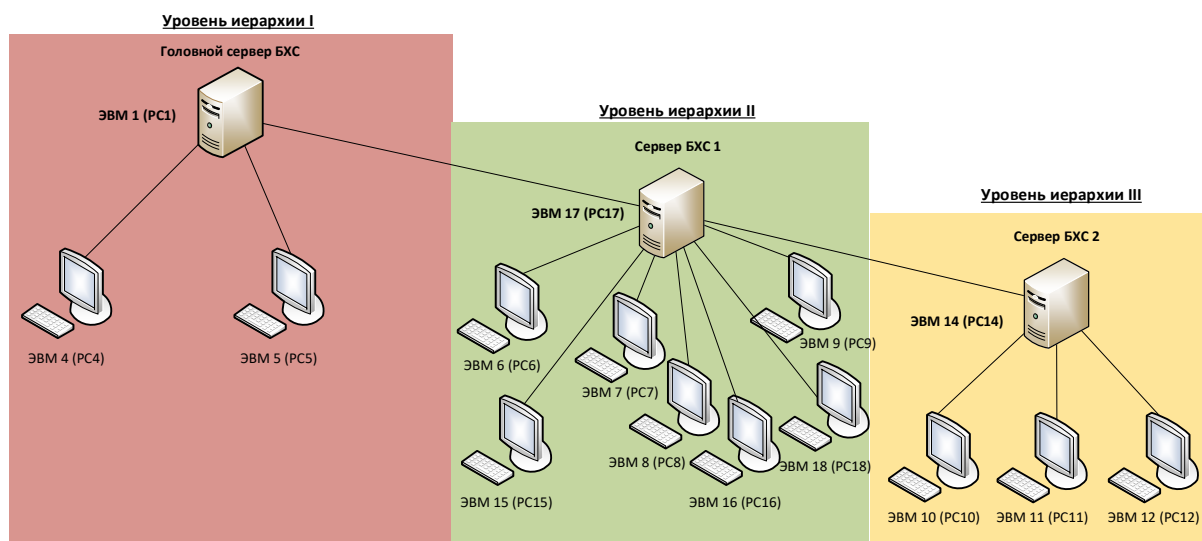


Рисунок П3.2 – Схема иерархии серверов и ЭВМ

1.3 Настройка параметров сервера безопасности

Настройка параметров СЗИ от НСД «Блокхост-Сеть 4» должна осуществляться пользователем со специальной учетной записью «Администратор» в соответствии с условиями применения.

Предварительные настройки серверной и клиентской политик осуществляются в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками».

2 Регламентное тестирование СЗИ от НСД «Блокхост-Сеть 4»

Программа проведения регламентного тестирования для автономного варианта использования СЗИ от НСД «Блокхост-Сеть 4» (используемого локально) и для варианта с удаленным управлением идентична и приведена в таблице П3.2.

Просмотр событий аудита, содержащихся в журнале СЗИ от НСД «Блокхост-Сеть 4», осуществляется администратором безопасности с помощью консоли управления (просмотр событий аудита подробно рассмотрен в разделе 7 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит»).

Таблица П3.2 – Программа проведения регламентного тестирования СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Наименование испытаний (проверок)	Пункт методики
1	Проверка установки СЗИ	2.1
	Проверка установки клиентских частей СЗИ с использованием агента подсистемы развертывания	2.1.1
	Проверка возможности установки внешних продуктов через подсистему развертывания	2.1.2
	Проверка возможности установки клиентских и серверных частей СЗИ в виртуальной сети и создание иерархии серверов безопасности	2.1.3
	Проверка взаимной аутентификации клиентов с сервером СЗИ при их сетевом взаимодействии	2.1.4
	Проверка контрольных сумм неизменных файлов установленного СЗИ от НСД «Блокхост-Сеть 4»	2.1.5
2	Проверка подсистемы развертывания	2.2
3	Проверка дискреционного принципа контроля доступа	2.3
	Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа	2.3.1
	Проверка наличия механизма, претворяющего в жизнь дискреционные ПРД, как для явных, так и для скрытых действий пользователя	2.3.2
	Проверка предоставления прав санкционировано изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.), в том числе изменения списка пользователей СВТ	2.3.3
	Проверка контроля запуска процессов по модели разрешенных процессов	2.3.4
	Проверка контроля запуска программ и файлов (аудит доступа к медиафайлам)	2.3.5
	Проверка контроля запуска исполняемого файла по маске его имени (аудит запуска приложений)	2.3.6

4	Проверка мандатного принципа контроля доступа	2.4
	Проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта при реализации мандатных ПРД	2.4.1
	Проверка запроса и получения классификационных меток при вводе новых данных в систему	2.4.2
	Проверка реализации мандатного принципа контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов	2.4.3
	Проверка возможности изменения классификационных уровней субъектов и объектов специально выделенными субъектами при реализации мандатных ПРД	2.4.4
	Проверка реализации диспетчера доступа	2.4.5
5	Проверка управления СЗИ и иерархии серверов безопасности	2.5
6	Проверка очистки памяти	2.6
	Проверка возможности очистки внешней памяти	2.6.1
	Проверка возможности очистки оперативной памяти	2.6.2
	Проверка возможности уничтожения информации на машинных носителях	2.6.3
7	Проверка маркировки документов	2.7
	Проверка контроля печати и маркировки при выводе на печать документа, содержащего защищаемую информацию	2.7.1
8	Проверка защиты ввода и вывода на отчуждаемый съемный подключаемый носитель информации	2.8
	Проверка возможности различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»)	2.8.1
	Проверка обеспечения соответствия между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства	2.8.2
	Проверка возможности изменения в назначении и разметке устройств только под контролем СЗИ от НСД «Блокхост-Сеть 4»	2.8.3
9	Проверка сопоставления пользователя с устройством	2.9
	Проверка возможности обеспечить вывод информации на запрошенное пользователем устройство	2.9.1
	Проверка механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству	2.9.2
10	Проверка идентификации и аутентификации пользователей	2.10
	Проверка требования от пользователей идентифицировать себя при запросах на доступ и проверка подлинности идентификатора субъекта (аутентификации)	2.10.1
	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	2.10.1.1
	Проверка требования применения установленной политики аутентификации	2.10.1.2
	Проверка идентификации и аутентификации пользователя при входе в систему	2.10.1.3
	Проверка возможности самостоятельного изменения паролей и PIN-кодов пользователем	2.10.1.4

	Управление параметрами механизмов защиты средства доверенной загрузки «SafeNode System Loader»	2.10.1.5
	Проверка идентификации и аутентификации пользователей при удалённом доступе RDP	2.10.2
	Проверка возможности аутентификации пользователей с использованием цифровых сертификатов	2.10.3
	Проверка функционирования политики безопасности аутентификации в контроллере домена с использованием СЗИ от НСД «Блокхост-Сеть 4»	2.10.4
	Проверка возможности идентификации и аутентификации пользователей в сети с иерархией серверов безопасности без контроллера домена	2.10.5
	Проверка возможности надёжно связывать полученную идентификацию со всеми действиями данного пользователя	2.10.6
11	Проверка регистрации	2.11
	Проверка регистрации использования идентификационного и аутентификационного механизмов	2.11.1
	Проверка регистрации запроса на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)	2.11.2
	Проверка регистрации создания и уничтожения объекта	2.11.3
	Проверка регистрации действий по изменению ПРД	2.11.4
	Проверка наличия средств выборочного ознакомления с регистрационной информацией	2.11.5
	Проверка регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.)	2.11.6
	Проверка функциональных возможностей механизма регистрации событий безопасности	2.11.7
	Проверка аудита событий, возникающих при задании/изменении настроек аудита	2.11.8
	Проверка регистрации в автономном варианте СЗИ от НСД «Блокхост-Сеть 4»	2.11.9
	Проверка передачи собранных событий безопасности с головного сервера СЗИ в SIEM-систему	2.11.10
12	Проверка надёжного восстановления	2.12
	Проверка полного восстановления свойств СЗИ от НСД «Блокхост-Сеть 4» после сбоев и отказов оборудования при использовании процедур восстановления	2.12.1
13	Проверка целостности СЗИ от НСД «Блокхост-Сеть 4»	2.13
	Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4»	2.13.1
	Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4» с блокировкой доступа пользователя при нарушении целостности	2.13.2
	Проверка регистрации событий, связанных с изменением целостности среды	2.13.3
	Проверка регистрации событий, связанных с изменением аппаратной среды	2.13.4
	Проверка выполнения программ в отдельной части оперативной памяти	2.13.5
14	Проверки работы с токенами (управление ЖЦ токенов)	2.14

2.1 Проверка установки СЗИ

Описание проверки:

Установка клиентской части СЗИ от НСД «Блокхост-Сеть 4» осуществляется на ЭВМ2 – ЭВМ4 в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

Установка клиента управления осуществляется на ЭВМ3 и ЭВМ4 в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

Установка серверной версии СЗИ от НСД «Блокхост-Сеть 4» осуществляется на ЭВМ1 и ЭВМ5 в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

Выполняемые действия:

На ЭВМ 1 – ЭВМ 5:

1) выполнить установку серверной части СЗИ от НСД «Блокхост-Сеть 4» (на ЭВМ 1 и ЭВМ 5, при этом после успешной установки и проверки на ЭВМ 1 ее следует отключить перед установкой СЗИ на ЭВМ 5), для чего:

- загрузить операционную систему;
- проверить наличие и соответствие требованиям по эксплуатации СЗИ от НСД «Блокхост-Сеть 4», установленного на ЭВМ программного обеспечения;
- установить на сервер СЗИ (ЭВМ 1 и ЭВМ 5) и защищаемые рабочие станции (ЭВМ 2 – ЭВМ 4) драйвера устройств персональной идентификации и аутентификации eToken, Рутокен, JaCarta, ESMART Token;
- установить и удалить клиентские части автономного варианта использования СЗИ для ЭВМ под управлением ОС MS Windows;
- установить агента развертывания через Систему развертывания и аудита на защищаемые рабочие станции ЭВМ2 – ЭВМ4 под управлением ОС MS Windows/Linux в соответствии с разделом 3 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит»;
- установить клиентские части СЗИ через Систему развертывания и аудита на защищаемые рабочие станции ЭВМ 2 – ЭВМ 4 под управлением ОС MS Windows/Linux в соответствии с разделом 4 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит»;
- установить серверную версию СЗИ с персональным идентификатором администратора безопасности на сервер СЗИ (ЭВМ 1 и ЭВМ 5) в соответствии с

подразделом 4.1 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Windows» и «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Linux»;

2) для использования функциональных возможностей СЗИ в полном объеме, активировать лицензию на право использования продукта в соответствии с главой 7 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Windows и главой 7 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Linux;

3) проверить работоспособность устройств, используемых в качестве ключевых носителей: eToken, Рутокен, JaCarta, ESMART Token, путем проверки их распознавания для ПК под управлением ОС Windows ЭВМ 1 – ЭВМ 5;

4) установить клиента управления через систему развертывания и аудита на ЭВМ 3 и ЭВМ 4 под управлением ОС Linux и проверить работоспособность устройств, используемых в качестве ключевых носителей: eToken, JaCarta, ESMART Token, Рутокен ЭЦП путем проверки их распознавания на ЭВМ 3 и ЭВМ 4.

Критерии оценки:

Установка СЗИ от НСД «Блокхост-Сеть 4» выполнена успешно, если во время выполнения и после выполнения перечисленных выше действий на ЭВМ 1 – ЭВМ 5 получены следующие результаты:

- установка и удаление клиентских частей автономного варианта использования СЗИ от НСД «Блокхост-Сеть 4» выполнена без возникновения сбоев и ошибок и соответствовала последовательности действий, указанных в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Windows»;
- установка клиентских частей и клиента управления СЗИ от НСД «Блокхост-Сеть 4» выполнена без возникновения сбоев и ошибок и соответствовала последовательности действий, указанной в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит»;
- установка серверной части СЗИ от НСД «Блокхост-Сеть 4» выполнена без возникновения сбоев и ошибок и соответствовала последовательности действий, указанной в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Windows» и в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по установке в ОС Linux»;
- после завершения установки на каждой ЭВМ успешно запущены службы СЗИ;
- развертывание СЗИ от НСД «Блокхост-Сеть 4» на клиентские ЭВМ выполнено без сбоев и ошибок и процесс соответствовал последовательности действий, изложенных в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит»;

– устройства, используемые в качестве ключевых носителей, работоспособны и идентифицируются без ошибок ОС.

2.1.1 Проверка установки клиентских частей СЗИ с использованием агента подсистемы развертывания

Описание функции:

Подсистема развертывания СЗИ от НСД «Блокхост-Сеть 4» позволяет выполнять удаленную установку клиентских частей СЗИ от НСД «Блокхост-Сеть 4» на рабочие станции с АРМ администратора безопасности.

Выполняемые действия:

Перед установкой подсистемы развертывания СЗИ от НСД «Блокхост-Сеть 4» необходимо:

- 1) установить серверную часть СЗИ от НСД «Блокхост-Сеть 4» на сервер безопасности (АРМ администратора безопасности) в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4. Руководство по инсталляции в ОС Windows» и с документом «СЗИ от НСД «Блокхост-Сеть 4. Руководство по инсталляции в ОС Linux»;
- 2) установить дополнительное ПО на удаленные рабочие станции, куда планируется установка СЗИ от НСД «Блокхост-Сеть 4» (.NET Framework 4.5.2, драйвера для персональных электронных идентификаторов);
- 3) отключить брандмауэр Windows или другие сетевые экраны на защищаемых рабочих станциях с ОС Windows.

Порядок действий и ожидаемые результаты испытания приведены в таблицах ПЗ.3, ПЗ.4 и ПЗ.5.

Таблица ПЗ.3 – Проверка установки агента системы развертывания с использованием подсистемы развертывания на ПК с ОС Windows

№ п/п	Действия	Ожидаемый результат
1	Войти в систему на ЭВМ1(РС1) и запустить консоль управления СЗИ	Окно консоли управления СЗИ запущено
2	В консоли выбрать «Развертывание» → «Задачи»	Открытие вкладки Задачи
3	На задаче «Установка агента системы развертывания» нажать два раза левой кнопкой мыши	Открытие задачи Установка агента системы развертывания для редактирования

№ п/п	Действия	Ожидаемый результат
4	В открывшемся окне редактирование задачи, перейти в пункт «Учетные записи» и по кнопке «+» добавить учетные записи пользователей, обладающих административными правами, на компьютерах на которые будет устанавливаться агент развертывания	Учетные записи пользователей добавлены
5	Перейти в пункт «Компьютеры» нажать кнопку «Добавить из домена»	Открылось окно «Добавление компьютеров»
6	В появившемся окне доменной аутентификации необходимо ввести данные доменного пользователя	После аутентификации в окне «Добавление компьютеров из Active Directory» отобразится структура объектов Active Directory выбранного домена
7	В структуре AD выбрать объект «Computers» и в списке «Компьютеры» установить галочку на ЭВМ2 (PC2)	PC2 появился в списке <i>Будут добавлены 1</i>
8	Нажать кнопку «Добавить» и ввести полное имя с доменом ЭВМ2 (PC2)	Добавлен PC2 в список рабочих станций пункте «Компьютеры»
9	Нажать кнопку Поиск по диапазону...	Открытие окна «Поиск по диапазону IP-адресов»
10	В окне «Поиск по диапазону IP-адресов» ввести диапазон в котором находится ЭВМ4 (PC4) и нажать кнопку «Найти»	Добавлен ЭВМ4 (PC4) в список рабочих станций в пункте «Компьютеры»
11	В списке найденных компьютеров, установить галочку на ЭВМ4(PC4) и нажать кнопку «Добавить»	Добавлен ЭВМ4 (PC4) в список рабочих станций в пункте «Компьютеры»
12	Нажать кнопку Применить, а затем ОК	Задача «Установка агента системы развертывания» настроена и готова
13	Выбрать задачу «Установка агента системы развертывания» и нажать кнопку «Запустить»	В поле Результат выполнения задачи появятся сведения о ходе установки агента. По окончании установки статус задачи в списке изменит значение на <i>Завершено</i>
14	Выполнить указанные в пунктах 1 – 13 действия для остальных поддерживаемых ОС Windows на рабочих станциях	Совпадение полученных результатов с приведенными выше результатами

Таблица ПЗ.4 – Проверка установки агента системы развертывания с использованием подсистемы развертывания на ПК с ОС Linux

№ п/п	Действия	Ожидаемый результат
1	Загрузить ОС на ЭВМ17(PC17) и запустить консоль управления СЗИ	Окно консоли управления СЗИ запущено
2	В консоли выбрать «Развертывание» → «Пакеты установки»	Открытие вкладки Пакеты установки
3	Нажать пиктограмму «+», в открывшемся окне «Мастер создания пакетов установки» нажать левой клавишей мыши на кнопку «Выбрать»	Открытие окна «Выбор файла инсталлятора»

№ п/п	Действия	Ожидаемый результат
4	Выбрать и открыть дистрибутив «Агента системы развертывания» для ОС Linux с эталонного диска. Для продолжения последовательно нажать « Далее » → « Создать »	Добавлен «Агент системы развертывания» для ОС Linux
5	В консоли выбрать « Развертывание » → « Задачи »	Открытие вкладки Задачи
6	Нажать пиктограмму «+», в открывшемся контекстном меню выбрать пункт « Установка агента развертывания ». Выбрать добавленный в п.4 настоящей таблицы пакет установки и нажать « Далее »	Открытие задачи « Создание задачи на установку агента развертывания »
7	В окне « Выберите компьютеры » нажать кнопку « Поиск по IP диапазону »	Появится окно « Поиск по диапазону IP-адресов »
8	В окне « Поиск по диапазону IP-адресов » ввести диапазон в котором находится ЭВМ15(РС15) и нажать кнопку « Найти », далее выбрать ЭВМ15(РС15) и нажать кнопку « Добавить »	Добавлена рабочая станция ЭВМ15(РС15)
9	В окне « Добавьте учетные записи » добавить учетную запись администратора безопасности на локальной станции ЭВМ15(РС15)	Учетная запись администратора безопасности добавлена
10	В окне « Параметры выполнения » выбрать « Вручную » и нажать « Далее »	Параметры выполнения установлены
11	Задать имя задачи и нажать « Создать »	Задача « Установка Агента системы развертывания » настроена и готова
12	Выбрать задачу « Установка агента системы развертывания » и нажать кнопку « Запустить »	В поле Статус для задачи появятся сведения о ходе установки на них агента системы развертывания. По окончании установки статус задачи в списке изменит значение на Завершено
13	Выполнить указанные в пунктах 1 – 12 действия для остальных поддерживаемых ОС Linux на рабочих станциях	Совпадение полученных результатов с приведенными выше результатами

Таблица ПЗ.5 – Проверка установки клиентской части СЗИ

№ п/п	Действия	Ожидаемый результат
1	Установка автономного варианта СЗИ (вариант №1) (для ЭВМ с ОС Windows)	
1.1	Запустить на ЭВМ1 установку клиентской части СЗИ с эталонного диска в соответствии с действиями, описанными в 4.6.2 Руководства по инсталляции в ОС Windows	По окончании работы мастера установки СЗИ появится окно окончания установки
1.2	Убедиться, что клиент СЗИ установлен без ошибок	Клиент СЗИ установлен без ошибок

1.3	Деинсталлировать СЗИ в соответствии с разделом 5. Руководства по инсталляции в ОС Windows	СЗИ деинсталлирована без ошибок и сбоев
1.4	Выполнить указанные в пунктах 1.1 – 1.3 действия для остальных поддерживаемых ОС на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
2	Установка клиентской части СЗИ с использованием системы развертывания (вариант №2)	
	Перед выполнением данного пункта необходимо установить агента развертывания в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит», на рабочих станциях, на которых будет установлен клиент	
2.1	Запустить консоль управления СЗИ на ЭВМ1	Окно консоли управления запущено
2.2	В консоли выбрать пункт меню Развертывание → Пакеты установки	Открытие вкладки Пакеты установки
2.3	Нажать пиктограмму «+»	Открытие окна «Мастер создания пакетов установки»
2.4	В «Мастере создания пакетов установки» нажать кнопку «Выбрать»	Открытие окна выбора файла инсталлятора
2.5	Выбрать файл инсталлятора (в соответствии с ОС) с эталонного диска и открыть дистрибутив программы	Дистрибутив программы (в соответствии с ОС) выбран
2.6	Нажать «Далее» и задать имя пакета	Имя пакета задано
2.7	Нажать кнопку «Создать»	Создание пакета установки завершено
2.8	В консоли выбрать пункт меню Развертывание → Задачи	Открытие вкладки Задачи
2.9	Нажать пиктограмму «+», в открывшемся контекстном меню выбрать пункт «Установка программы». Выбрать требуемый пакет установки клиента СЗИ и нажать кнопку Далее	Открытие окна «Создания задачи на установку/изменения программы»
2.10	Выбрать все компоненты для установки и нажать кнопку Далее	Выбраны компоненты установки
2.11	В разделе Компьютеры сформировать список рабочих станций, с установленным агентом развертывания	Список сформирован
2.12	Перейти в пункт Перезагрузка ОС и установить Не перезагружать компьютер , затем нажать кнопку Сохранить и ОК	Задача Установка клиента Блокхост-Сеть настроена и готова
2.13	Выбрать задачу Установка клиента Блокхост-сеть и нажать кнопку Запустить	По окончании установки статус задачи в списке изменит значение на Завершено

2.14	Выполнить указанные в пунктах 2.1 – 2.13 действия для остальных поддерживаемых ОС на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенными выше результатами
------	--	--

Критерии оценки:

Результаты проверки признаются успешными, если:

- локальная установка клиентской части автономного варианта использования СЗИ от НСД «Блокхост-Сеть 4» на рабочие станции выполнена без ошибок и сбоев;
- удаленная установка клиентских частей СЗИ от НСД «Блокхост-Сеть 4» на рабочие станции с АРМ администратора безопасности выполнена без ошибок и сбоев;
- после установки клиентской части СЗИ, при авторизации пользователя, в поле ввода пароля, знак просмотра пароля отсутствует.

2.1.2 Проверка возможности установки внешних продуктов через подсистему развертывания

Описание проверки:

Консоль СЗИ позволяет устанавливать на удаленных рабочих станциях ПО внешних продуктов через подсистему развертывания.

Выполняемые действия:

Перечень действий для проверки возможности установки внешних продуктов через подсистему развертывания и ожидаемые при проверке результаты приведены в таблице ПЗ.6.

Таблица ПЗ.6 – Проверка возможности установки внешних продуктов через подсистему развертывания

№ п/п	Действия	Ожидаемый результат
1	Загрузить ОС на ЭВМ1 и запустить консоль управления СЗИ	Окно консоли управления запущено
2	В консоли выбрать «Развертывание» → «Пакеты установки»	Открытие вкладки Пакеты установки
3	Нажать пиктограмму «+», в открывшемся окне «Мастер создания пакетов установки» нажать левой клавишей мыши на кнопку «Выбрать»	Открытие окна « Выбор файла инсталлятора »
4	Выбрать и открыть подготовленный дистрибутив программы для токена. Ввести дополнительный параметр командной строки /S. Нажать кнопку «Далее»	Выбран дистрибутив для токена
5	Задать имя пакета «rtDrivers»	Имя пакета «rtDrivers» задано
6	Нажать кнопку «Создать» и далее нажать кнопку	Создание пакета установки «rtDrivers»

№ п/п	Действия	Ожидаемый результат
	«Закрыть» для завершения создания пакета установки	
7	В консоли выбрать пункт меню « Развертывание » → « Задачи »	Открытие вкладки Задачи
8	Нажать пиктограмму «+», в открывшемся контекстном меню выбрать пункт «Установка программы». Для продолжения нажать кнопку «Далее»	Открытие окна « Создание задачи на установку/изменение программы »
9	В окне « Создание задачи на установку/изменение программы » выполнить последовательность действий: <ul style="list-style-type: none"> • выбрать пакет установки, добавленный в п.5 настоящей таблицы и нажать «Далее»; • выбрать компьютеры для установки программы и нажать «Далее»; • выбрать тип запуска «Вручную» и нажать «Далее»; • установить параметры перезагрузки операционной системы «Не перезагружать компьютер» и нажать «Далее»; • задать имя задачи «Установка rtDrivers» и нажать «Создать» • закрыть окно «Создание задачи на установку/изменение программы». 	Во вкладке Задачи появилась задача на установку внешнего продукта «Установка rtDrivers»
10	В окне « Развертывание » → « Задачи », запустить задачу «Установка rtDrivers», для этого нажать кнопку «Запустить»	В поле планировщика задач появятся сведения о ходе установки программы. По окончании установки программы, результат выполнения задачи изменит значение « Ожидает выполнения-1 » на « Успешно завершено-1 »
11	Выполнить указанные в пунктах 1–10 действия для всех остальных рабочих станций ЭВМ1 – ЭВМ5 с учетом установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Результаты проверки признаны успешными, если:

- внешняя программа на удаленных рабочих станциях через подсистему развертывания установлена;
- сбоев во время установки нет.

2.1.3 Проверка возможности установки клиентских и серверных частей СЗИ в виртуальной сети и создание иерархии серверов безопасности

Описание проверки:

Вариант с удаленным управлением СЗИ от НСД «Блокхост-Сеть 4» поддерживает многоуровневую иерархию серверов безопасности, развернутых в корпоративной сети. Иерархия серверов безопасности, включает «главный» сервер безопасности («мастер-

сервер») и группу «подчиненных» серверов безопасности, находящихся на нижних уровнях сетевой иерархии (до трех уровней иерархии серверов).

СЗИ от НСД «Блокхост-Сеть 4» предоставляет возможность централизованного управления политиками безопасности СЗИ на уровне «мастер-сервера» СЗИ (первый уровень иерархии серверов). На «мастер-сервере» СЗИ могут создаваться (изменяться) настройки безопасности для «подчиненных» серверов безопасности СЗИ всех уровней, а также настройки безопасности для подчиненных клиентов СЗИ на ПК.

На консоли администрирования визуализировано формирование и изменение списков защищаемых ПК (групп ПК), а также списков серверов безопасности, при помощи средств графического интерфейса (GUI) консоли.


Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.7.

Таблица ПЗ.7 – Проверка установки агента системы развертывания с использованием подсистемы развертывания и аудита

№ п/п	Действия	Ожидаемый результат
1	Установка серверной части СЗИ на сервера безопасности	
1.1	Выполнить установку серверной части СЗИ на PC1, PC14, PC17 в соответствии с действиями, описанными в п. 4.1 Руководства по инсталляции в ОС Windows и в соответствии с п. 4.1 Руководства по инсталляции в ОС Linux	Серверная часть СЗИ установлена на PC1, PC14, PC17
1.2	Выполнить установку серверной части СЗИ на PC17 в соответствии с действиями, описанными в соответствии с п. 4.1 Руководства по инсталляции в ОС Linux	Серверная часть СЗИ установлена на PC17
2	Установка клиентской части СЗИ на клиентские компьютеры сервера безопасности БХС	
2.1	Выполнить установку агента развертывания с сервера безопасности БХС (PC1) на PC2, PC3, PC4, PC5	Агент развертывания установлен на PC2, PC3, PC4, PC5
2.2	Выполнить установку клиентской части СЗИ с сервера безопасности БХС (PC1) на PC2, PC3, PC4, PC5	Клиентская часть СЗИ установлена на PC2, PC3, PC4, PC5
3	Установка клиентской части СЗИ на клиентские компьютеры сервера безопасности БХС1	
3.1	Выполнить установку агента развертывания с сервера безопасности БХС 1 (PC17) на PC6, PC7, PC8, PC9	Агент развертывания установлен на PC6, PC7, PC8, PC9
3.2	Выполнить установку клиентской части СЗИ с сервера безопасности БХС 1 (PC17) на PC6, PC7, PC8, PC9	Клиентская часть СЗИ установлена на PC6, PC7, PC8, PC9
4	Установка клиентской части СЗИ на клиентские компьютеры сервера безопасности БХС2	
4.1	Выполнить установку агента развертывания с сервера безопасности БХС 2 (PC14) на PC10, PC11, PC12, PC13	Агент развертывания установлен на PC10, PC11, PC12, PC13
4.2	Выполнить установку клиентской части СЗИ с сервера безопасности БХС 2 (PC14) на PC10, PC11, PC12, PC13	Клиентская часть СЗИ установлена на PC10, PC11, PC12, PC13
5	Установка клиента управления на клиентские компьютеры сервера безопасности БХС1	
5.1	Выполнить установку агента развертывания с сервера	Агент развертывания установлен на

№ п/п	Действия	Ожидаемый результат
	безопасности БХС 1 (PC17) на PC15, PC16, PC18	PC15, PC16, PC18
5.2	Выполнить установку клиента управления с сервера безопасности БХС 1 (PC17) на PC15, PC16, PC18	Клиент управления установлен на PC15, PC16, PC18
6	Создание головного сервера БХС (PC1)	
6.1	1) Открыть консоль управления СЗИ сервера безопасности БХС (PC1); 2) Перейти на вкладку «Настройки» и далее на вкладку «Построение иерархии серверов»; 3) Выбрать вид подключения «Подчиненные сервера» и нажать кнопку «Подключить»; 4) В открывшемся окне «Подключение подчиненного сервера» скачать сертификат текущего сервера и передать его администратору подчиненного сервера; 5) Для продолжения нажать кнопку «Далее»; 6) В окне «Подключение подчиненного сервера», установить флаг для подтверждения отправки скачанного сертификата администратору подчиненного сервера и нажать на кнопку «Продолжить»; 7) Выбрать группу «Все компьютеры» для включения в нее подчиненного сервера и нажать на кнопку «Далее»; 8) В открывшемся окне «Подключение подчиненного сервера» заполнить поля данными подчиненного сервера БХС1 (PC17) (БХС2 (PC14)): IP-адрес/DNS-имя, Порт-59731 (Для получения данных подчиненного сервера выполнить последовательно строки 7.1 (БХС1) и 8.1 (БХС2) данной таблицы); 9) Нажать на кнопку «Подключить»; 10) В открывшемся окне «Подключение подчиненного сервера», убедиться в правильности полученных параметров подчиненного сервера (имя сервера, идентификатор сервера) БХС1 (PC17) (БХС2 (PC14)). 11) Нажать на кнопку «Ок» для продолжения подключения; 12) Убедились в успешном включении сервера в иерархию; 13) Для завершения подключения подчиненного сервера нажать кнопку «Ок»; 14) Убедиться в том, что статус сервера изменился с Автономного на Мастер-сервер; Выполнить строки 8.1 данной таблицы для БХС2 (PC14) и повторить действия с п.2) по п. 14)	Сервер успешно включен в иерархию Статус сервера изменился на Мастер-сервер
7	Создание подчиненного сервера БХС1 (PC17)	
7.1	1) Открыть консоль управления СЗИ сервера безопасности БХС1 (PC17); 2) Перешли на вкладку «Настройки», «Построение иерархии серверов»; 3) Выбрать вид подключения «Подключение к мастер-серверу» и нажать кнопку «Подключиться»; 4) В открывшемся окне «Подключение к мастер-серверу», нажать кнопку «Добавить сертификат...»; 5) Добавить сертификат, полученный от администратора мастер-сервера сервера БХС (PC1) в соответствии с п.4) строки 6.1 данной таблицы и нажать кнопку «Продолжить»; 6) В открывшемся окне «Подключение к мастер-серверу», скопировать и отправить следующие данные администратору мастер-сервера: IP-адрес, порт; Имя	Статус сервера изменился с Автономного на Подчиненный

№ п/п	Действия	Ожидаемый результат
	<p>сервера; Идентификатор сервера;</p> <p>7) Для продолжения нажмите кнопку «Ок»;</p> <p>8) Убедиться, что сертификат успешно добавлен и закрыть сообщение;</p> <p>9) Ожидать действий администратора мастер-сервера для включения подчиненного сервера в иерархию;</p> <p>10) После завершения выполнения п.14) строки 6.1 данной таблицы убедиться в изменении статуса сервера БХС1 (PC17) с Автономного на Подчиненный и для сервера БХС (PC1) с Автономного на Мастер-сервер</p>	
8	Создание подчиненного сервера БХС2 (PC14)	
8.1	<p>1) Открыть консоль управления СЗИ сервера безопасности БХС2 (PC14);</p> <p>2) Выбрать вкладку «Настройки», «Построение иерархии серверов»;</p> <p>3) Выбрать вид подключения «Подключение к мастер-серверу» и нажать на кнопку «Подключиться»;</p> <p>4) В открывшемся окне «Подключение к мастер-серверу», нажать на кнопку «Добавить сертификат...»;</p> <p>5) Добавить сертификат, полученный от администратора мастер-сервера БХС (PC1) в соответствии с п.4) строки 6.1 данной таблицы и нажать на кнопку «Продолжить»;</p> <p>6) В открывшемся окне «Подключение к мастер-серверу», скопировать и отправить следующие данные администратору мастер-сервера:</p> <ul style="list-style-type: none"> • IP-адрес, порт; • Имя сервера; • Идентификатор сервера; <p>Для продолжения нажмите кнопку «Ок»;</p> <p>7) Убедиться, что сертификат успешно добавлен;</p> <p>8) Закрыть сообщение;</p> <p>9) Ожидать действий администратора мастер-сервера для включения подчиненного сервера в иерархию;</p> <p>10) После завершения выполнения п.14) строки 6.1 данной таблицы убедиться в изменении статуса сервера с Автономного на Подчиненный.</p>	Статус сервера изменился с Автономного на Подчиненный
9	Проверка возможности передачи политик безопасности по иерархии серверов	
9.1	<p>1) Открыть консоль управления СЗИ сервера безопасности БХС (PC1) от имени и с правами Администратора;</p> <p>2) Перейти на вкладку «Политики», «Политика сервера по умолчанию» и установить следующие параметры:</p> <ul style="list-style-type: none"> • Доступ к серверу – для Администратора: «Просмотр» и «Изменение» разрешен; • Сбор событий по иерархии – для Windows/Linux: «Выбрать все» и установить принудительное наследование « Сбор событий  »; • Сохранить выполненные изменения; <p>3) Перейти на вкладку «Политики», «Политика клиента по умолчанию», Windows и установить следующие</p>	Политики настроены

№ п/п	Действия	Ожидаемый результат
	параметры: • Управление входом в ОС – для группы «Все пользователи» установить флаги «Разрешить» во всех параметрах «Аутентификации» и «Типа входа»; • Сложность паролей – для «Паролей пользователей» и «PIN-кода токена» флаги не устанавливать, наследование выключено; • «Контроль устройств» – для всех «USB-устройств», «Доступ разрешен» (все пользователи), включить наследование; для «Других устройств» (CD/DVD, COM, LPT) установить флаги «Доступ разрешен», для «Доверенных списков», список устройства не добавлять, наследование не включено; «Аудит» событий оставить без изменения; • «Очистка оперативной памяти» -- механизм выключен, наследование выключено; • «Аудит целостности файлов» -- механизм выключен, наследование выключено; 4) Перейти на вкладку «Политики», «Политика клиента по умолчанию», Linux и установить параметры аналогичные Windows; 5) Сохранить выполненные изменения	
9.2	В консоли СЗИ БХС (PC1) перейти на подчинённый сервер БХС1 (PC17) и проверяем серверную и клиентскую политику.	Политики соответствуют описанным в п. 9.1
9.3.	В консоли СЗИ БХС (PC1) перейти на подчинённый сервер БХС2 (PC14) и проверяем серверную и клиентскую политику.	Политики соответствуют описанным в п. 9.1

Критерии оценки

Результаты проверки признаются успешными, если:

- иерархия серверов безопасности сформирована без ошибок и сбоев;
- сформированы группы компьютеров, подчиненных серверам безопасности;
- на консоли администрирования визуализирована возможность формирования и изменения групп (списков) защищаемых ПК;
- политики безопасности передаются по иерархии серверов.

2.1.4 Проверка взаимной аутентификации клиентов с сервером СЗИ при их сетевом взаимодействии

Описание функции:

Взаимная аутентификация клиентов с сервером СЗИ при их сетевом взаимодействии – вход пользователя на свою рабочую станцию и подключение СЗИ от НСД «Блокхост-Сеть 4» к серверной консоли после генерации рабочих станций.

72410666.00063-04 95 01-01

При установке сервера безопасности СЗИ, генерируется уникальный идентификационный ключ, который передается в клиентские части СЗИ при их установке. Взаимная аутентификация клиента и сервера СЗИ осуществляется по:

- «идентификатору машины по умолчанию»;
- «паролю подключения клиента»;
- идентификационного ключа сервера безопасности СЗИ.

Выполняемые действия:

Проверка выполняется на основании действий, выполняемых в п. 2.1.3.

В созданной виртуальной сети выбирается сервер безопасности третьего уровня БХС2 (ЭВМ14).

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.8.

Таблица ПЗ.8 – Проверка установки агента системы развертывания с использованием подсистемы развертывания и аудита

№ п/п	Действия	Ожидаемый результат
1	Проверка подключения клиентских ЭВМ к серверу безопасности БХС2 (РС14)	
1.1	Войти в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
1.2	Запустить серверную консоль управления СЗИ	В вкладке «Менеджер иерархий», в группе «Все компьютеры» отображаются РС10, РС11, РС12
1.3	Закрыть серверную консоль администрирования СЗИ	Консоль закрыта
2	Удаление сервера безопасности БХС2 (РС14)	
2.1	Перейти по ветке «Пуск» – «Панель управления» – «Удаление программ» – «Блокхост-Сеть Сервер» и нажать кнопку «Удалить»	Серверная часть СЗИ с РС14 удалена
2.2	Перезагрузить РС14	
3	Установка сервера безопасности БХС2 (РС14)	
3.1	Выполнить установку серверной части СЗИ, в соответствии с действиями, описанными в п. 4.1. Руководства по инсталляции в ОС Windows на РС14	Серверная часть СЗИ установлена на РС14
3.2	Перезагрузить РС14	
4	Проверка подключения клиентских ЭВМ к серверу безопасности БХС2 (ЭВМ14)	
4.1	Войти в систему от имени и с правами пользователя Admin	Загрузка рабочего стола
4.2	Запустить серверную консоль администрирования СЗИ	На вкладке «Менеджер иерархий», в группе «Все компьютеры» не отображаются РС10, РС11, РС12

№ п/п	Действия	Ожидаемый результат
		(индикация черным цветом)
4.3	Запустить серверную консоль управления и выполнить следующие действия: <ul style="list-style-type: none"> • перейти во вкладку «Менеджер иерархий»; • выбрать РС14; • перейти во вкладку «События»; • установить фильтр по типу событий «События сервера СЗИ» и выполнить поиск; • убедиться в наличии событий об отказе подключения клиентов РС10, РС11, РС12 	Отображаются события РС10, РС11, РС12, РС15, РС16 «Отказ в подключении клиента к серверу» (некорректный ключ)
5	Установка клиентской части СЗИ и клиента управления на клиентские компьютеры, сервера безопасности БХС	
5.1	Выполнить установку клиентской части СЗИ с сервера безопасности БХС 2 (РС14) на РС10, РС11, РС12	Клиентская часть СЗИ установлена (восстановлена) на РС10, РС11, РС12.
6	Проверка подключения клиентских ЭВМ к серверу безопасности БХС2 (РС14)	
6.1	Запустить серверную консоль управления СЗИ	На вкладке «Список машин» отображаются РС10, РС11, РС12, РС15, РС16
6.2	Запустить серверную консоль администрирования и выполнить следующие действия: <ul style="list-style-type: none"> • перейти на вкладку «менеджер иерархий»; • выбрать РС14; • перейти на вкладку «События»; • установить фильтр по категории «События сервера СЗИ» и выполнить поиск; • убедиться в наличии событий подключения клиентов РС10, РС11, РС12 	Отображаются события РС10, РС11, РС12, «Подключение клиента к серверу»
7	Восстановление настроек сервера безопасности БХС2	
7.1	Повторить действия, указанные в п. 8 таблицы П3.7	Настройки восстановлены

Критерии оценки:

Проверка считается успешной если:

- при совпадении идентификационной информации на панели администрирования СЗИ выводится список всех контролируемых рабочих станций;
- СЗИ регистрирует события, связанные с подключением клиента к серверу и отказом в подключении к серверу.

2.1.5 Проверка контрольных сумм неизменных файлов установленного СЗИ от НСД «Блокхост-Сеть 4»

Описание проверки:

После установки (проверки установки) необходимо получить значения контрольных сумм (КС) для неизменных файлов с использованием программы «ФИКС».

Полученные значения контрольных сумм должны соответствовать значениям, указанным в Приложении Б ТУ и Приложении 2 Формуляра.

Контрольное суммирование на ЭВМ1 – ЭВМ5 должно осуществляться с использованием программы «ФИКС» по алгоритму «Уровень-3, программно» для ОС MS Windows.

Контрольное суммирование на ЭВМ3, ЭВМ4 и ЭВМ5 должно осуществляться с использованием программы «ФИКС-UNIX» по алгоритму «Уровень-3» для ОС Linux.

Критерии оценки:

Результаты проверки контроля исходного состояния СЗИ считаются положительными, если после установки (проверки установки) полученные значения КС неизменных файлов совпадают с данными, указанными в Приложениях Б ТУ и Приложении 2 Формуляра.

2.2 Проверка подсистемы развертывания

Описание проверки:

СЗИ осуществляет установку (развертывание) и удаление программного обеспечения клиентских частей СЗИ от НСД «Блокхост-Сеть 4», обеспечивает создание инсталляционных пакетов из файла установщика, с возможностью задания дополнительных параметров установки, а также создание дистрибутивов для AD, осуществляет формирование задач на установку/удаление программ и перезагрузку компьютеров.

Сформированная в СЗИ задача осуществляет формирование списка компьютеров для дальнейших действий по:

- списку компьютеров, зарегистрированных в AD;
- списку компьютеров, зарегистрированных в FreeIPA;
- диапазону IP адресов;
- списку компьютеров, зарегистрированных на сервере СЗИ.

Сформированная в СЗИ задача выполняется по типам запуска:

- вручную;
- сразу после создания/редактирования задачи;
- однократно в заданное время;
- по расписанию;
- после завершения другой задачи.

Сформированная в СЗИ задача осуществляет следующие виды перезагрузки рабочей станции:

- перезагружать компьютер сразу;
- не перезагружать компьютер;
- уведомить пользователя о необходимости перезагрузки.

Выполняемые действия:

Проверка выполняется согласно действиям, выполняемым в пп. 2.1.1 и 2.1.2.

Критерии оценки:

Результаты проверки признаны успешными, если:

- удаленная установка клиентских частей СЗИ от НСД «Блокхост-Сеть 4» и ПО внешних продуктов на рабочие станции с АРМ администратора безопасности выполнена без ошибок и сбоев;
- после установки клиентской части СЗИ, при авторизации пользователя, в поле ввода пароля, знак просмотра пароля отсутствует.

2.3 Проверка дискреционного принципа контроля доступа

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

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 дополнительные ограничения на доступ процессов к объектам файловой структуры.

При разрешении чтения файла доступно чтение содержимого файла и его запуск, если это исполняемый файл. Запрещается изменение содержимого, переименование, перемещение, удаление файла. При этом нельзя изменить содержимое каталога.

При разрешении записи в файл возможно изменение содержимого и удаление файла. Остальные действия невозможны, например, нельзя прочитать содержимое каталога

(подкаталоги и файлы), при этом все его содержимое также имеет запрет по чтению.

Комбинация этих двух разрешений дает полный доступ: чтение и изменение содержимого, запуск исполняемого файла, переименование, перемещение и удаление файла (таблица ПЗ.9).

Таблица ПЗ.9 – Перечень разрешенных операций в зависимости от типа доступа

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

Описание проверки:

СЗИ реализует дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа:

- разграничение доступа субъектов реализуется при входе в информационную систему;
- правила разграничения доступа реализуют разграничение доступа субъектов к техническим средствам, устройствам и внешним устройствам, к объектам, создаваемым общесистемным программным обеспечением и прикладным, специальным программным обеспечением.

Выполняемые действия:

Для проведения проверки потребуется создание каталогов с сетевым (общим) доступом D1, D2 и D3 на РС8, средствами ОС. Схема проведения проверки приведена на рисунке ПЗ.3.

К защищаемым каталогам устанавливаются права доступа групп пользователей, которые выше устанавливаемых средствами СЗИ и предоставляют «Полный доступ» к каталогам (таблица ПЗ.10). Соответственно «Полный доступ» включает в себя, такие права как «Чтение» и «Запись».

Таблица ПЗ.10 – Матрица разграничения доступа, к файловой системе NTFS

Каталог	\D1	\D2	\D3
Прошедшие проверку	Полный доступ	Полный доступ	Полный доступ
Администраторы	Полный доступ	Полный доступ	Полный доступ
Пользователи	Полный доступ	Полный доступ	Полный доступ

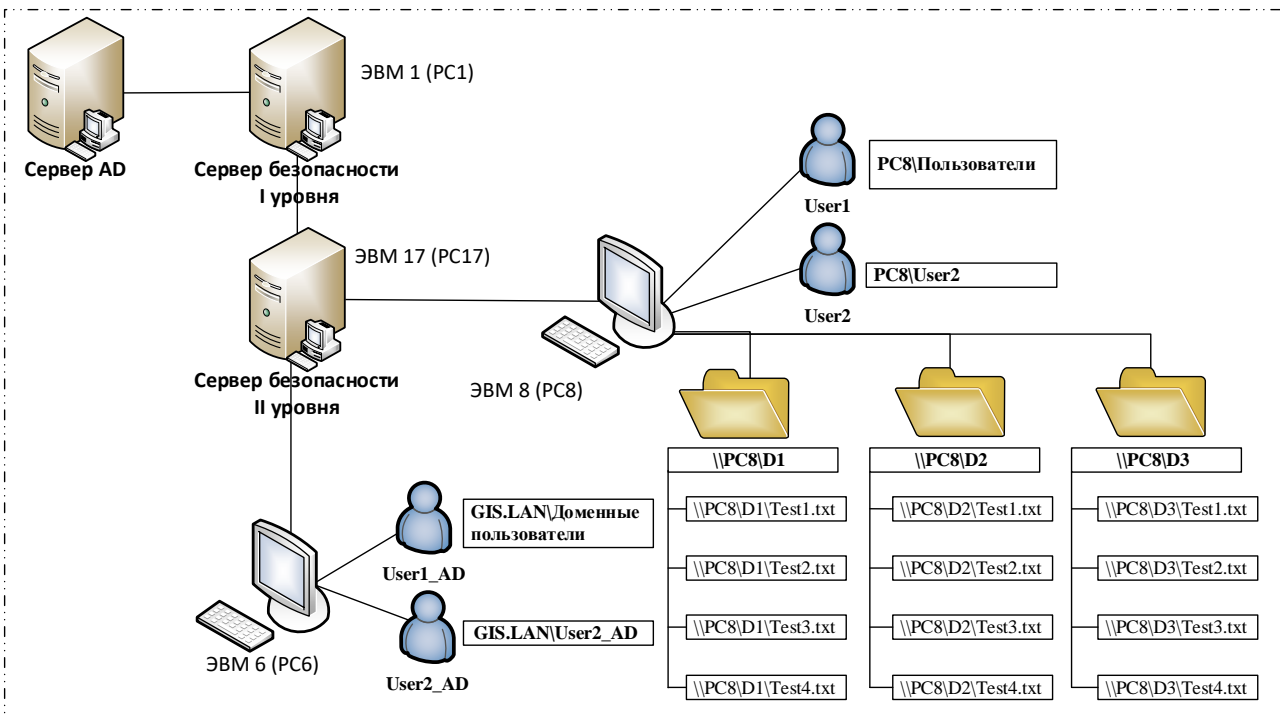


Рисунок ПЗ.3 – Схема проведения проверки дискреционного принципа контроля доступа

Серверная политика «Сбора событий» устанавливается на сервере безопасности I уровня PC1.

Настройки дискреционного доступа производятся непосредственно на PC8 через консоль администрирования СЗИ установленную на сервере безопасности II уровня PC17.

Доступ к каталогам осуществляется с PC6 от имени и с правами доменного пользователя User2_AD. Для проверки доступа группы «пользователи домена» используется учетная запись User1_AD.

Перед выполнением тестов создать учетные записи доменных пользователей User1_AD и User2_AD. На рабочих станциях ЭВМ1 – ЭВМ5 создать учетные записи локальных пользователей User1 и User2 для всех установленных ОС Windows и Linux (РЕД ОС).

Для проведения тестов создаётся матрица доступа, представленная в таблице ПЗ.11, 72410666.00063-04 95 01-01

которая задаётся в явном виде средствами СЗИ, через консоль администрирования установкой соответствующих параметров.

Таблица ПЗ.11 – Матрица разграничения доступа, создаваемая средствами СЗИ

Субъекты доступа (пользователи и группы пользователей)	Атрибуты		Объекты	Атрибуты		Объекты	Атрибуты		Объекты
	R	W		R	W		R	W	
Доменные пользователи	+	+	\D1	+	-	\D2	-	-	\D3
	+	+	Test1	+	+	Test1	+	+	Test1
	+	-	Test2	+	-	Test2	+	-	Test2
	-	-	Test3	-	-	Test3	-	-	Test3
	*	*	Test4	*	*	Test4	*	*	Test4
User2_AD	+	+	\D1	+	-	\D2	-	-	\D3
	+	+	Test1	+	+	Test1	+	+	Test1
	+	-	Test2	+	-	Test2	+	-	Test2
	-	-	Test3	-	-	Test3	-	-	Test3
	*	*	Test4	*	*	Test4	*	*	Test4
Локальные пользователи	+	+	\D1	+	-	\D2	-	-	\D3
	+	+	Test1	+	+	Test1	+	+	Test1
	+	-	Test2	+	-	Test2	+	-	Test2
	-	-	Test3	-	-	Test3	-	-	Test3
	*	*	Test4	*	*	Test4	*	*	Test4
User2	+	+	\D1	+	-	\D2	-	-	\D3
	+	+	Test1	+	+	Test1	+	+	Test1
	+	-	Test2	+	-	Test2	+	-	Test2
	-	-	Test3	-	-	Test3	-	-	Test3
	*	*	Test4	*	*	Test4	*	*	Test4

Для файла Test4 разрешения в явном виде не устанавливаются. Атрибуты доступа наследуются от установленных атрибутов на каталог.

Перечень действий для проверки выполнения контроля доступа и ожидаемый результат после выполнения каждого действия представлен для доменных пользователей представлены в таблице ПЗ.12 и для локальных пользователей в таблице ПЗ.13.

Таблица ПЗ.12 – Алгоритм проведения проверки контроля доступа наименованных субъектов (**доменных пользователей**) к наименованным объектам при использовании дискреционного принципа разграничения доступа СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия	Ожидаемый результат
1	Создание матрицы доступа и тестовых объектов файловой системы	
1.1	Войти на РС8 от имени и с правами пользователя Admin и выполнить следующие действия: 1) создать объекты доступа в соответствии с таблицей ПЗ.10 и ПЗ.11;	Созданы субъекты и объекты доступа

№ п/п	Действия	Ожидаемый результат	
	<ol style="list-style-type: none"> 2) создать субъекты доступа в соответствии с таблицей ПЗ.11; 3) установить общий (сетевой) доступ для каталогов; 4) задать разрешения доступа в соответствии с таблицей ПЗ.10 и ПЗ.11; 5) создать текстовые файлы и задать разграничения доступа, согласно таблице ПЗ.11 		
1.2	<p>Войти на РС17 от имени и с правами пользователя Администратор, запустить консоль управления и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) перейти на вкладку «Политики»; 2) открыть для изменения «Политику клиента по умолчанию»; 3) перейти на вкладку Windows, «Управление входом в ОС»; 4) добавить учетные записи доменных пользователей User1_AD, User2_AD и учетные записи локальных пользователей User1 и User2 с разрешением на «Аутентификацию в Windows»; 5) перейти на вкладку Linux, «Управление входом в ОС»; 6) добавить учетные записи доменных пользователей User1_AD, User2_AD и учетные записи локальных пользователей User1 и User2 с разрешением на «Аутентификацию в ОС»; 7) сохранить сделанные изменения; 8) выбрать РС8; 9) перейти в меню «Настройки», «Блокхост-Сеть», «Дискреционный доступ»; 10) включить тумблер «Механизм включен»; 11) добавить объекты доступа и установить права доступа, согласно таблице ПЗ.11; 12) установить параметр «Аудит» на объектах доступа; 13) сохранить сделанные изменения, для этого нажать кнопку «Применить» 	Создание ПРД	
2	Проверка дискреционного механизма разграничения доступа для заданных пользователям ПРД		
2.1	Осуществить вход в систему РС6 от имени и с правами пользователя User1_AD, входящего в группу «доменные пользователи», и выполнить следующие действия:		
2.1.1	Операции над файлом \\PC8\D1\Test1.txt		
	Чтение	\\PC8\D1 \\PC8\D1\Test1.txt	Успешно. Успешно.
	Изменение	\\PC8\D1\Test1.txt	Успешно.
	Копирование	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test1.txt на Test1asd.txt	Успешно
		\\PC8\D1\Test1asd.txt на Test1.txt	Успешно
	Перемещение	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D1\Test1.txt	Успешно
	Восстановление	\\PC8\D1\Test1.txt	Успешно
Создание нового объекта	\\PC8\D1\ «Новый текстовый документ»	Успешно	
2.1.2	Операции над файлом \\PC8\D1\Test2		
	Чтение	\\PC8\D1\Test2.txt	Успешно
	Изменение	\\PC8\D1\Test2.txt	Ошибка
	Копирование	\\PC8\D1\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test2.txt на \\PC6\C	Ошибка
Удаление	\\PC8\D1\Test2.txt	Ошибка	
2.1.3	Операции над файлом \\PC8\D1\Test3		
	Чтение	\\PC8\D1\Test3.txt	Ошибка
	Изменение	\\PC8\D1\Test3.txt	Ошибка

№ п/п	Действия		Ожидаемый результат
	Копирование	\\PC8\D1\Test3.txt на \\PC6\C	Ошибка
	Переименование	\\PC8\D1\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test3.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D1\Test3.txt	Ошибка
2.1.4	Операции над файлом \\PC8\D1\Test4		
	Чтение	\\PC8\D1\Test4.txt	Успешно.
	Изменение	\\PC8\D1\Test4.txt	Успешно.
	Копирование	\\PC8\D1\Test4.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test4.txt на Test4asd.txt	Успешно
		\\PC8\D1\Test4asd.txt на Test4.txt	Успешно
	Перемещение	\\PC8\D1\Test4.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D1\Test4.txt	Успешно
Восстановление	\\PC8\D1\Test4.txt		
2.1.5	Операции над файлом \\PC8\D2\Test1.txt		
	Чтение	\\PC8\D2	Успешно.
		\\PC8\D2\Test1.txt	Успешно.
	Изменение	\\PC8\D2\Test1.txt	Успешно.
	Копирование	\\PC8\D2\Test1.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test1.txt на Test1asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test1.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D2\Test1.txt	Успешно
	Восстановление	\\PC8\D2\Test1.txt	Успешно
Создание нового объекта	\\PC8\D2\ «Новый текстовый документ»	Ошибка. Отказано в доступе	
2.1.6	Операции над файлом \\PC8\D2\Test2.txt		
	Чтение	\\PC8\D2\Test2.txt	Успешно
	Изменение	\\PC8\D2\Test2.txt	Ошибка
	Копирование	\\PC8\D2\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test2.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test2.txt	Ошибка
2.1.7	Операции над файлом \\PC8\D2\Test3.txt		
	Чтение	\\PC8\D2\Test3.txt	Ошибка
	Изменение	\\PC8\D2\Test3.txt	Ошибка
	Копирование	\\PC8\D2\Test3.txt на \\PC6\C	Ошибка
	Переименование	\\PC8\D2\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test3.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test3.txt	Ошибка
2.1.8	Операции над файлом \\PC8\D2\Test4.txt		
	Чтение	\\PC8\D2\Test4.txt	Успешно
	Изменение	\\PC8\D2\Test4.txt	Ошибка
	Копирование	\\PC8\D2\Test4.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test4.txt на Test4asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test4.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test4.txt	Ошибка
2.1.9	Операции над файлом \\PC8\D3\Test1.txt		
Чтение	\\PC8\D3	Ошибка. Отказано в доступе	
2.2	Осуществить вход в систему PC6 от имени и с правами пользователя User2_AD и выполнить следующие действия:		
2.2.1	Операции над файлом \\PC8\D1\Test1.txt		
	Чтение	\\PC8\D1	Успешно.
		\\PC8\D1\Test1.txt	Успешно.
	Изменение	\\PC8\D1\Test1.txt	Успешно.
	Копирование	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test1.txt на Test1asd.txt	Успешно

№ п/п	Действия		Ожидаемый результат
		\\PC8\D1\Test1.asd.txt на Test1.txt	Успешно
	Перемещение	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D1\Test1.txt	Успешно
	Восстановление	\\PC8\D1\Test1.txt	Успешно
	Создание нового объекта	\\PC8\D1\ «Новый текстовый документ»	Успешно
	Операции над файлом \\PC8\D1\Test2		
2.2.2	Чтение	\\PC8\D1\Test2.txt	Успешно
	Изменение	\\PC8\D1\Test2.txt	Ошибка
	Копирование	\\PC8\D1\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test2.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D1\Test2.txt	Ошибка
	Операции над файлом \\PC8\D1\Test3		
2.2.3	Чтение	\\PC8\D1\Test3.txt	Ошибка
	Изменение	\\PC8\D1\Tes3.txt	Ошибка
	Копирование	\\PC8\D1\Test3.txt на \\PC6\C	Ошибка
	Переименование	\\PC8\D1\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test3.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D1\Test3.txt	Ошибка
	Операции над файлом \\PC8\D1\Test4		
2.2.4	Чтение	\\PC8\D1\Test4.txt	Успешно.
	Изменение	\\PC8\D1\Test4.txt	Успешно.
	Копирование	\\PC8\D1\Test4.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test4.txt на Test4asd.txt	Успешно
		\\PC8\D1\Test4asd.txt на Test4.txt	Успешно
	Перемещение	\\PC8\D1\Test4.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D1\Test4.txt	Успешно
	Восстановление	\\PC8\D1\Test4.txt	Успешно
	Операции над файлом \\PC8\D2\Test1.txt		
2.2.5	Чтение	\\PC8\D2 \\PC8\D2\Test1.txt	Успешно. Успешно.
	Изменение	\\PC8\D2\Test1.txt	Успешно.
	Копирование	\\PC8\D2\Test1.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test1.txt на Test1asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test1.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D2\Test1.txt	Успешно
	Восстановление	\\PC8\D2\Test1.txt	Успешно
	Создание нового объекта	\\PC8\D2\ «Новый текстовый документ»	Ошибка. Отказано в доступе
	Операции над файлом \\PC8\D2\Test2.txt		
2.2.6	Чтение	\\PC8\D2\Test2.txt	Успешно
	Изменение	\\PC8\D2\Test2.txt	Ошибка
	Копирование	\\PC8\D2\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test2.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test2.txt	Ошибка
	Операции над файлом \\PC8\D2\Test3.txt		
2.2.7	Чтение	\\PC8\D2\Test3.txt	Ошибка
	Изменение	\\PC8\D2\Test3.txt	Ошибка
	Копирование	\\PC8\D2\Test3.txt на \\PC6\C	Ошибка
	Переименование	\\PC8\D2\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test3.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test3.txt	Ошибка
	Операции над файлом \\PC8\D2\Test4.txt		
2.2.7	Чтение	\\PC8\D2\Test4.txt	Успешно
	Изменение	\\PC8\D2\Test4.txt	Ошибка

№ п/п	Действия		Ожидаемый результат
	Копирование	\\PC8\D2\Test4.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D2\Test4.txt на Test4asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test4.txt на \\PC6\C	Ошибка
	Удаление	\\PC8\D2\Test4.txt	Ошибка
2.2.9	Операции над файлом \\PC8\D3\Test1.txt		
	Чтение	\\PC8\D3	Ошибка. Отказано в доступе
3	Просмотр событий аудита		
3.1	Войти на PC1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC17, вкладку «События»; 3) установить фильтр по типу событий «Дискреционный доступ»; 4) нажать кнопку «Поиск»		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows и Linux (РЕД ОС)		Совпадение полученных результатов с приведенными выше результатами

Таблица П3.13 – Алгоритм проведения проверки контроля доступа наименованных субъектов (**локальных пользователей**) к наименованным объектам при использовании дискреционного принципа разграничения доступа СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия		Результат
1	Проверка дискреционного механизма разграничения доступа для заданных пользователям ПРД		
1.1	Осуществить вход в систему PC8 от имени и с правами пользователя User1 входящего в группу «пользователи» и выполнить следующие действия:		
	Операции над файлом \\PC8\D1\Test1.txt		
1.1.1	Чтение	\\PC8\D1	Успешно
		\\PC8\D1\Test1.txt	Успешно
	Изменение	\\PC8\D1\Test1.txt	Успешно
	Копирование	\\PC8\D1\Test1.txt	Успешно
	Переименование	\\PC8\D1\Test1.txt на Test1asd.txt	Успешно
		\\PC8\D1\Test1asd.txt на Test1.txt	Успешно
	Перемещение	\\PC8\D1\Test1.txt	Успешно
	Удаление	\\PC8\D1\Test1.txt	Успешно
Восстановление	\\PC8\D1\Test1.txt	Успешно	
Создание нового объекта	\\PC8\D1\ «Новый текстовый документ»	Успешно	
	Операции над файлом \\PC8\D1\Test2		
1.1.2	Чтение	\\PC8\D1\Test2.txt	Успешно
	Изменение	\\PC8\D1\Test2.txt	Ошибка
	Копирование	\\PC8\D1\Test2.txt	Успешно
	Переименование	\\PC8\D1\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test2.txt	Ошибка
	Удаление	\\PC8\D1\Test2.txt	Ошибка
	Операции над файлом \\PC8\D1\Test3		
1.1.3	Чтение	\\PC8\D1\Test3.txt	Ошибка
	Изменение	\\PC8\D1\Tes3.txt	Ошибка

№ п/п	Действия		Результат
	Копирование	\\PC8\D1\Test3.txt	Ошибка
	Переименование	\\PC8\D1\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test3.txt	Ошибка
	Удаление	\\PC8\D1\Test3.txt	Ошибка
1.1.4	Операции над файлом \\PC8\D1\Test4		
	Чтение	\\PC8\D1\Test4.txt	Успешно.
	Изменение	\\PC8\D1\Test4.txt	Успешно.
	Копирование	\\PC8\D1\Test4.txt	Успешно
	Переименование	\\PC8\D1\Test4.txt на Test4asd.txt	Успешно
		\\PC8\D1\Test4asd.txt на Test4.txt	Успешно
	Перемещение	\\PC8\D1\Test4.txt	Успешно
	Удаление	\\PC8\D1\Test4.txt	Успешно
Восстановление	\\PC8\D1\Test4.txt		
1.1.5	Операции над файлом \\PC8\D2\Test1.txt		
	Чтение	\\PC8\D2	Успешно.
		\\PC8\D2\Test1.txt	Успешно.
	Изменение	\\PC8\D2\Test1.txt	Успешно.
	Копирование	\\PC8\D2\Test1.txt	Успешно
	Переименование	\\PC8\D2\Test1.txt на Test1asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test1.txt	Успешно
	Удаление	\\PC8\D2\Test1.txt	Успешно
	Восстановление	\\PC8\D2\Test1.txt	Успешно
Создание нового объекта	\\PC8\D2\ «Новый текстовый документ»	Ошибка. Отказано в доступе	
1.1.6	Операции над файлом \\PC8\D2\Test2.txt		
	Чтение	\\PC8\D2\Test2.txt	Успешно
	Изменение	\\PC8\D2\Test2.txt	Успешно
	Копирование	\\PC8\D2\Test2.txt	Успешно
	Переименование	\\PC8\D2\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test2.txt	Ошибка
	Удаление	\\PC8\D2\Test2.txt	Ошибка
1.1.7	Операции над файлом \\PC8\D2\Test3.txt		
	Чтение	\\PC8\D2\Test3.txt	Ошибка
	Изменение	\\PC8\D2\Test3.txt	Ошибка
	Копирование	\\PC8\D2\Test3.txt	Ошибка
	Переименование	\\PC8\D2\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test3.txt	Ошибка
1.1.8	Операции над файлом \\PC8\D2\Test4.txt		
	Чтение	\\PC8\D2\Test4.txt	Успешно
	Изменение	\\PC8\D2\Test4.txt	Ошибка
	Копирование	\\PC8\D2\Test4.txt	Успешно
	Переименование	\\PC8\D2\Test4.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test4.txt	Ошибка
1.1.9	Операции над файлом \\PC8\D3\Test1.txt		
	Чтение	\\PC8\D3	Ошибка. Отказано в доступе

№ п/п	Действия	Результат	
1.2	Осуществить вход в систему PC8 от имени и с правами локального пользователя User2 и выполнить следующие действия:		
1.2.1	Операции над файлом \\PC8\D1\Test1.txt		
	Чтение	\\PC8\D1	Успешно.
		\\PC8\D1\Test1.txt	Успешно.
	Изменение	\\PC8\D1\Test1.txt	Успешно.
	Копирование	\\PC8\D1\Test1.txt	Успешно
	Переименование	\\PC8\D1\Test1.txt на Test1asd.txt	Успешно
		\\PC8\D1\Test1asd.txt на Test1.txt	Успешно
	Перемещение	\\PC8\D1\Test1.txt	Успешно
Удаление	\\PC8\D1\Test1.txt	Успешно	
Восстановление	\\PC8\D1\Test1.txt	Успешно	
Создание нового объекта	\\PC8\D1\ «новый текстовый документ»	Успешно	
1.2.2	Операции над файлом \\PC8\D1\Test2		
	Чтение	\\PC8\D1\Test2.txt	Успешно
	Изменение	\\PC8\D1\Test2.txt	Ошибка
	Копирование	\\PC8\D1\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test2.txt на \\PC6\C	Ошибка
Удаление	\\PC8\D1\Test2.txt	Ошибка	
1.2.3	Операции над файлом \\PC8\D1\Test3		
	Чтение	\\PC8\D1\Test3.txt	Ошибка
	Изменение	\\PC8\D1\Test3.txt	Ошибка
	Копирование	\\PC8\D1\Test3.txt	Ошибка
	Переименование	\\PC8\D1\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D1\Test3.txt	Ошибка
Удаление	\\PC8\D1\Test3.txt	Ошибка	
1.2.4	Операции над файлом \\PC8\D1\Test4		
	Чтение	\\PC8\D1\Test4.txt	Успешно.
	Изменение	\\PC8\D1\Test4.txt	Успешно.
	Копирование	\\PC8\D1\Test4.txt	Успешно
	Переименование	\\PC8\D1\Test4.txt на Test4asd.txt	Успешно
		\\PC8\D1\Test4asd.txt на Test4.txt	Успешно
	Перемещение	\\PC8\D1\Test4.txt	Успешно
	Удаление	\\PC8\D1\Test4.txt	Успешно
Восстановление	\\PC8\D1\Test4.txt		
1.2.5	Операции над файлом \\PC8\D2\Test1.txt		
	Чтение	\\PC8\D2	Успешно.
		\\PC8\D2\Test1.txt	Успешно.
	Изменение	\\PC8\D2\Test1.txt	Успешно.
	Копирование	\\PC8\D2\Test1.txt	Успешно
	Переименование	\\PC8\D2\Test1.txt на Test1asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test1.txt	Успешно
	Удаление	\\PC8\D2\Test1.txt	Успешно
Восстановление	\\PC8\D2\Test1.txt	Успешно	
Создание нового объекта	\\PC8\D2\ «новый текстовый документ»	Ошибка. Отказано в доступе	
1.2.6	Операции над файлом \\PC8\D2\Test2.txt		
	Чтение	\\PC8\D2\Test2.txt	Успешно

№ п/п	Действия		Результат
	Изменение	\\PC8\D2\Test2.txt	Успешно
	Копирование	\\PC8\D2\Test2.txt	Успешно
	Переименование	\\PC8\D2\Test2.txt на Test2asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test2.txt	Ошибка
	Удаление	\\PC8\D2\Test2.txt	Ошибка
1.2.7	Операции над файлом \\PC8\D2\Test3.txt		
	Чтение	\\PC8\D2\Test3.txt	Ошибка
	Изменение	\\PC8\D2\Test3.txt	Ошибка
	Копирование	\\PC8\D2\Test3.txt	Ошибка
	Переименование	\\PC8\D2\Test3.txt на Test3asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test3.txt	Ошибка
1.2.8	Операции над файлом \\PC8\D2\Test4.txt		
	Чтение	\\PC8\D2\Test4.txt	Успешно
	Изменение	\\PC8\D2\Test4.txt	Ошибка
	Копирование	\\PC8\D2\Test4.txt	Успешно
	Переименование	\\PC8\D2\Test4.txt на Test4asd.txt	Ошибка
	Перемещение	\\PC8\D2\Test4.txt	Ошибка
1.2.9	Операции над файлом \\PC8\D3\Test1.txt		
	Чтение	\\PC8\D3	Ошибка. Отказано в доступе
2	Просмотр событий аудита		
2.1	Войти на PC1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC17, вкладку «События»; 3) установить фильтр по категории «Дискреционный доступ»; 4) нажать кнопку «Поиск»		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows и Linux (РЕД ОС)		Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка контроля доступа наименованных субъектов (пользователей, процессов) 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 «субъект доступа – объект доступа» (формировать матрицу доступа);
- контроль доступа применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов);
- средства СЗИ обеспечивают регистрацию всех событий, связанных с попытками получения доступа к контролируемым объектам.

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

Описание проверки:

СЗИ содержат механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Дополнительно, СЗИ содержит механизм, осуществляющий дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД).

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

Дискреционные ПРД являются дополнением мандатных ПРД.

Выполняемые действия:

Проверка выполняется на основе действий, выполненных в п. 2.3.1, указанных в таблице ПЗ.12, на основе созданной матрицы доступа таблицы ПЗ.11, и основные ее этапы приведены в таблице ПЗ.14.

Таблица ПЗ.14 – Этапы проверки механизма ПРД СЗИ от НСД «Блокхост-Сеть 4»

№	Действия	Ожидаемый результат	
1	Осуществить вход в систему РС6 от имени и с правами пользователя User1_AD входящего в группу «доменные пользователи», и выполнить следующие действия:		
1.2	Запустить файловый менеджер Far	Появление интерфейса программы	
2	Операции над файлом \\PC8\D1\Test1.txt с помощью файлового менеджера Far		
	Чтение	\\PC8\D1 \\PC8\D1\Test1.txt	Успешно. Успешно.
	Изменение	\\PC8\D1\Test1.txt	Успешно.
	Копирование	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test1.txt на Test1asd.txt	Успешно
		\\PC8\D1\Test1asd.txt на Test1.txt	Успешно
	Перемещение	\\PC8\D1\Test1.txt на \\PC6\C	Успешно
	Удаление	\\PC8\D1\Test1.txt	Успешно
	Восстановление	\\PC8\D1\Test1.txt	Успешно
3	Операции над файлом \\PC8\D1\Test2 с помощью файлового менеджера Far		
	Чтение	\\PC8\D1\Test2.txt	Успешно
	Изменение	\\PC8\D1\Test2.txt	Ошибка
	Копирование	\\PC8\D1\Test2.txt на \\PC6\C	Успешно
	Переименование	\\PC8\D1\Test2.txt на Test2asd.txt	Ошибка

№	Действия	Ожидаемый результат
	Перемещение	\\PC8\D1\Test.txt на \\PC6\C
	Удаление	\\PC8\D1\Test2.txt
4	Просмотр событий	
4.1	Войти на PC1 от имени и справами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать сервер СЗИ PC17, вкладку «События»; • установить фильтр по категории «Дискреционный доступ»; • нажать кнопку «Поиск» 	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows и Linux (РЕД ОС)	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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.

2.3.3 Проверка предоставления прав санкционировано изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.), в том числе изменения списка пользователей СВТ

Описание проверки:

Защита информации о событиях безопасности реализуется предоставлением доступа к механизму регистрации событий и к его настройке администраторам безопасности.

- обеспечивается резервное копирование записей регистрации (аудита);
- доступ к записям о регистрации событий безопасности (аудиту) предоставляется привилегированным учетным записям с ролью в СЗИ «Аудитор» или «Администратор».

Права изменять ПРД предоставляются выделенным субъектам (администрации, службе безопасности и т.д.).

Выполняемые действия:

Для проведения проверки потребуется создать доменных пользователей Safety_AD и User2_AD.

На сервере безопасности I уровня PC1 создаётся локальный пользователь «Safety» и средствами консоли администрирования СЗИ создаётся пользователь Блокхост-Сеть «Auditor» и предоставляются разрешения для доступа к СЗИ согласно таблице ПЗ.15.

Таблица ПЗ.15 – Предоставляемые разрешения для доступа к СЗИ

№ п/п	Пользователь	Предоставляемые разрешения для доступа к СЗИ	
		Просмотр	Изменение
1	GIS.LAN\Safety_AD	+	+
2	Пользователь Блокхост-Сеть \Auditor	+	-
3	PC1\Safety	+	+
4	GIS.LAN\User2_AD		

Пользователю GIS.LAN\User2_AD разрешения для доступа к СЗИ не устанавливаются, от имени данного пользователя будут осуществляться несанкционированные попытки доступа к СЗИ.

Доступ к консоли администрирования СЗИ осуществляется согласно схеме на рисунке ПЗ.4.

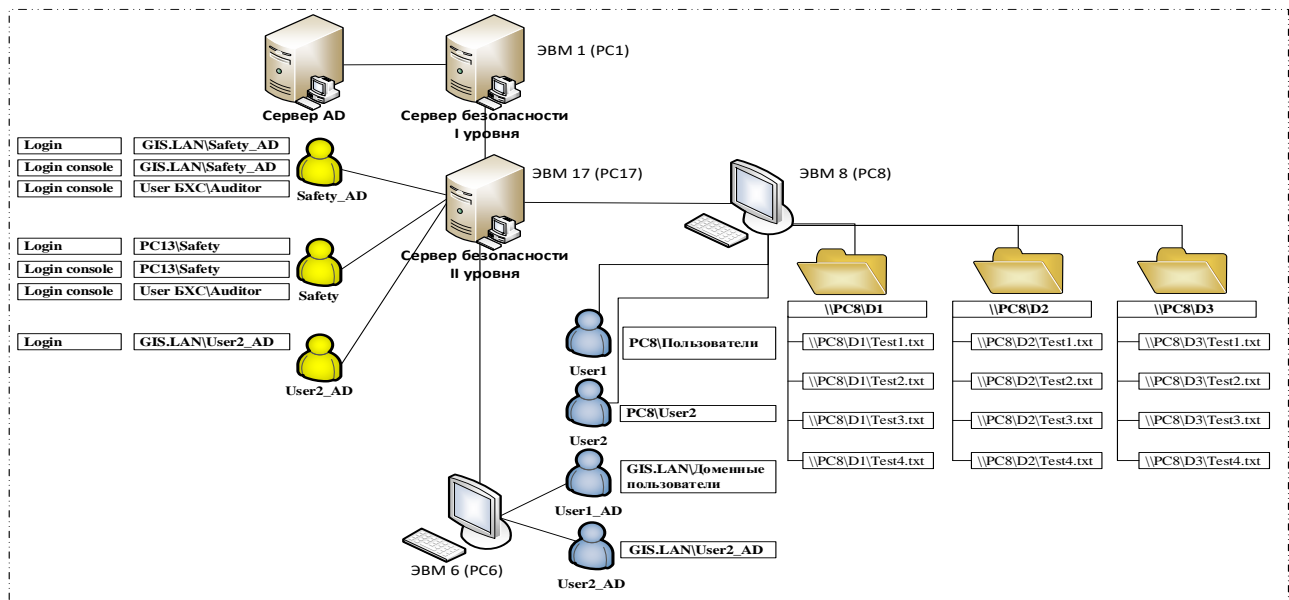


Рисунок ПЗ.4 – Схема проверки предоставления прав изменять ПРД

Пользователи, осуществившие санкционированный доступ и имеющие достаточные права для администрирования СЗИ и изменения ПРД, устанавливают новые ПРД согласно представленной таблице ПЗ.16.

Таблица ПЗ.16 – Изменения вносимые в матрицу разграничения доступа средствами СЗИ

Субъекты доступа (пользователи и группы пользователей)	Атрибуты		Атрибуты (устанавливаемые)		Объекты
	R	W	R	W	
Доменные пользователи	-	-			\\D3
	+	+			Test1

	+	-			Test2
	-	-			Test3
	*	*			Test4
Локальные пользователи	-	-			\\D3
	+	+			Test1
	+	-			Test2
	-	-			Test3
	*	*			Test4
User2	-	-	+	+	\\D3
	+	+	-	-	Test1
	+	-			Test2
	-	-	+	+	Test3
	*	*			Test4

Установленные ПРД проверяются на PC8 пользователями User1 и User2.

Подробное описание выполняемых при проверке действий и ожидаемые результаты приведены в таблице П3.17.

Таблица П3.17 – Проверка предоставления прав изменения ПРД выделенным субъектам в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	Создание субъектов доступа для администрирования СЗИ	
1.1	Создать учетные записи доменных пользователей Safety_AD и User2_AD	Пользователи созданы
1.2	Войти на сервере безопасности I уровня PC1 от имени Администратора и создать учетную запись локального пользователя Safety	Локальный пользователь создан
1.3	От имени и с правами Администратор загрузить консоль управления СЗИ и выполнить следующие действия: 1) выбрать PC1, «Политики», «Политика сервера по умолчанию»; 2) перейти на вкладку «Доступ к серверу»; 3) нажать кнопку «+» и последовательно выполнить следующие действия: • создать «Пользователя Блокхост-Сеть «Auditor»; • добавить пользователя GIS.LAN\Safety_AD; • добавить пользователя PC1\Safety; 4) назначить разрешения для доступа к СЗИ согласно таблице П3.15; 5) нажать кнопку «Ок» для сохранения изменений; 6) закрыть консоль управления СЗИ; 7) завершить работу Администратора в ОС	Субъекты доступа для администрирования СЗИ созданы
2	Осуществление санкционированных и несанкционированных попыток доступа к администрированию СЗИ	
2.1	От имени и с правами пользователя GIS.LAN\User2_AD войти на сервер безопасности I уровня PC1	Успешно
2.1.1	Запустить консоль управления СЗИ	Отказ в доступе «У

№ п/п	Действия	Ожидаемый результат
		пользователя недостаточно прав».
2.1.2	Завершить работу GIS.LAN\User2_AD в ОС	Завершение работы в ОС
2.2	От имени и с правами пользователя GIS.LAN\Safety_AD войти на сервер безопасности I уровня PC1	Успешно
2.3	Запустить консоль управления СЗИ от имени и с правами пользователя «Auditor»	Успешно
	<ul style="list-style-type: none"> Проверить возможность изменения ПРД. Убедиться, что настройки ПРД не доступны для редактирования. 	Настройки ПРД отображаются, но не доступны для редактирования. Пользователь «Auditor» не имеет права для администрирования СЗИ, только «Просмотр»
	<ul style="list-style-type: none"> Перейти во вкладку «События» и проверить доступность событий безопасности. Убедиться, что пользователю с правами «Auditor» доступны записи событий безопасности. Завершить работу консоли управления СЗИ. 	Доступны записи событий безопасности (аудиту)
2.4	Запустить консоль управления СЗИ от имени и с правами пользователя «Safety_AD»	Успешно
	Выполнить следующие действия: <ul style="list-style-type: none"> выбрать PC8; перейти по пути «Настройки», «Дискреционный доступ»; удалить разрешения для групп «Локальные пользователи» и «Active Directory»; добавить локального пользователя PC8\User2; установить разрешение на просмотр и изменение согласно таблице ПЗ.16; нажать кнопку «Применить» для сохранения изменений 	Настройки ПРД отображаются, и доступны для редактирования. Пользователь имеет права для администрирования СЗИ.
2.5	Войти на PC8 от имени и с правами пользователя User2 и выполнить следующие действия:	Успешно
	<ul style="list-style-type: none"> Войти в каталог PC8\D3 	Успешно. Каталог доступен
	<ul style="list-style-type: none"> Открыть файл Test1.txt Открыть файл Test3.txt, внести изменения и сохранить 	Ошибка. Успешно
2.6	Перейти на PC1, закрыть консоль и завершить работу в ОС	Завершена работа в ОС пользователя Safety_AD
2.7	От имени и с правами пользователя PC1\Safety войти на сервер безопасности I уровня PC1	Успешно
2.7.1	Запустить консоль управления СЗИ от имени и с правами пользователя «Auditor»	Успешно
2.7.2	Проверить доступность изменения ПРД	Настройки ПРД отображаются, но не доступны для редактирования. Пользователь «Auditor» имеет права для администрирования СЗИ,

№ п/п	Действия	Ожидаемый результат
		только «Просмотр»
2.7.3	Завершить работу консоли управления СЗИ	Работа консоль управления СЗИ завершена
2.7.4	Запустить консоль управления СЗИ от имени и с правами пользователя «Safety»	Успешно
	Выполнить следующие действия: <ul style="list-style-type: none"> • выбрать PC8; • перейти по пути «Настройки», «Дискреционный доступ»; • восстановить разрешения для каталога D3 в соответствии с матрицей доступа представленной в таблице Таблица П3.10; • применить сделанные изменения 	Настройки ПРД отображаются, и доступны для редактирования. Пользователь имеет права для администрирования СЗИ.
2.8	Войти на PC8 от имени и с правами пользователя User1	Успешно
	<ul style="list-style-type: none"> • Открыть каталог D3 	Ошибка. Отказано в доступе
3	Осуществление санкционированного изменения списка пользователей СВТ	
3.1	От имени и с правами пользователя PC1\Safety войти на сервер безопасности I уровня PC1	Успешно
3.2.	Запустить консоль управления СЗИ от имени и с правами пользователя PC1\Safety	Успешно
3.3	Выполнить следующие действия: <ul style="list-style-type: none"> • выбрать сервер безопасности PC17 и перейти по пути, «Политики», «Политики клиента по умолчанию», Windows, «Управление входом в ОС», «Дополнительные настройки» • установить флаг «Включить механизм «Пользователи с разрешением на вход в ОС» на клиентских компьютерах» • установить принудительное применение политики (кликнуть по замку) • сохранить сделанные изменения в клиентской политике 	Клиентская политика сформирована
3.4	В менеджере иерархий выбрать PC8 и выполнить следующие действия: <ul style="list-style-type: none"> • перейти по пути, «Настройки», «Пользователи с разрешением на вход в ОС»; • добавить пользователя PC8\User1; • удалить псевдоним «Все пользователи»; • применить сделанные изменения 	Пользователи с разрешением на вход в ОС сформированы
3.5	Войти на PC8 от имени и с правами пользователя PC8\User1	Успешно
3.6	Завершить работу пользователя PC8\User1 в ОС	Выход пользователя из ОС
3.7	Войти на PC8 от имени и с правами пользователя User2	Ошибка. Пользователю запрещён вход
3.8	От имени и с правами пользователя GIS.LAN\Safety_AD войти на сервер безопасности I уровня PC1 и восстановить состояние СЗИ	Успешно
3.9	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать PC17; • выбрать вкладку «События»; • нажать кнопку «Поиск»; • убедиться в появлении событий изменений ПРД 	Появление сообщений, фиксирующих изменение ПРД

Критерии оценки:

Проверка считается успешной, если:

- выделенным субъектам успешно предоставлены полномочия на изменения ПРД, изменения списка пользователей и защищаемых объектов;
- СЗИ способно ассоциировать выделенного субъекта с ролями безопасности.
- администратор СЗИ успешно изменил ПРД пользователя, включенного в список СЗИ рабочей станции, а пользователь не смог осуществить ранее разрешенный доступ, в связи с изменением ПРД. Администратор может также успешно изменять списки пользователей и списки защищаемых объектов;
- доступ к записям о регистрации событий безопасности (аудиту) предоставляется привилегированным учетным записям с ролью в СЗИ «Аудитор» или «Администратор».

2.3.4 Проверка контроля запуска процессов по модели разрешенных процессов**Описание проверки:**

Механизм «Замкнутая программная среда» позволяет сформировать список разрешенных для запуска процессов, доступных для выбранного пользователя на клиентской рабочей станции.

Механизм замкнутой программной среды (ЗПС) работает по принципу «белого списка». При настроенном механизме ЗПС СЗИ от НСД «Блокхост-Сеть 4» отслеживает все обращения пользователя на запуск процессов и, в случае отсутствия процесса в списке разрешенных для этого пользователя, блокирует его запуск.

Замкнутая программная среда может быть сформирована вручную путем добавления процессов в список разрешенных для выбранных пользователей или автоматически (все процессы, необходимые пользователю, анализируются в течение некоторого временного промежутка во время работы пользователя, и по завершению анализа добавляются в список ЗПС автоматически).

После создания списка разрешенных процессов выбранные пользователи смогут запускать только те процессы, которые добавлены в список. При запуске процесса из списка разрешенных для пользователя формируется событие аудита на запуск программы.

Выполняемые действия:

- 1) Через сервер СЗИ на выбранной ЭВМ (Windows/Linux (РЕД ОС)) формируется замкнутая программная среда, которая распространяется на пользователей User1 и User2.

2) От имени пользователей запускаем процессы regedit и notepad и данные попытки должны быть удачны (Windows). От имени пользователей запускаем процесс mkdir и данные попытки должны быть удачны (Linux (РЕД ОС)).

3) Редактируем настройку замкнутой программной среды и удаляем пользователя User2, и программу regedit (Windows)/mkdir (Linux (РЕД ОС)) из списка.

4) От имени пользователя User2 запускаем все процессы regedit и notepad и попытки должны быть неудачны т.к. к пользователю не применяется механизм замкнутой программной среды. От имени пользователя User2 запускаем все процессы mkdir, и попытка должна быть неудачна т.к. к пользователю не применяется механизм замкнутой программной среды (Linux (РЕД ОС)).

5) От имени пользователя User1 запускаем:

– процесс regedit и попытка должна быть **неудачной**, т.к. процесс **исключен** из списка разрешённых программ;

– процесс notepad и попытка должна быть **удачной**, т.к. процесс **входит** в список разрешённых программ.

6) Через сервер СЗИ на выбранной ЭВМ2 проверяем список событий в котором присутствуют события отказа по политике замкнутой программной среды.

Подробное описание выполняемых при проверке действий и ожидаемые результаты приведены в таблице ПЗ.18.

Таблица ПЗ.18 – Контроль запуска процессов СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия	Ожидаемый результат
Windows		
1	Настройка списка разрешённых процессов на PC2 через сервер СЗИ PC1	
1.1	1) Запустить консоль управления СЗИ на PC1 под учетной записью Администратора ; 2) В подсистеме «Менеджер иерархий» выбрать PC2; 3) Открыть последовательно вкладки «Настройки», «Замкнутая программная среда»; 4) Включить механизм, для этого установить тумблер в положение «Механизм включен»; 5) Нажать пиктограмму «+»; 6) Выбрать режим создания замкнутой программной среды «Стандартный режим»; 7) Нажать кнопку «Далее»; 8) На вкладке «Наименование» добавить имя группы программ: «Группа программ 1»; 9) Перейти на вкладку «Программы» и нажать пиктограмму «+»; 10) В открывшемся окне «Добавление процессов/программ» на вкладке «Приложения» установить флаг «Все процессы»; 11) Перейти на вкладку «Запущенные процессы» и установить флаг	Список разрешенных программ для пользователя User1, User2 сформирован

№ п/п	Действия	Ожидаемый результат
	«Все процессы»; 12) Перейти на вкладку «Файловая система» и установить флаги на «Все процессы» и на C:\windows\regedit.exe и notepad.exe; 13) После установки флагов нажать кнопку «Добавить»; 14) Перейти во вкладку «Пользователи» и добавить пользователей User1 и User2; 15) Нажмите кнопку «Создать» для сохранения «Группы программ 1»	
2	Проверка запуска процессов пользователем User1 и User2 на PC2	
2.1	Выполнить вход в систему PC2 от имени и с правами пользователя User1	Загрузка рабочего стола
2.1.1	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «regedit»	Программа «Редактор реестра» запущена
2.1.2	1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «notepad»	Программа запущена
2.2	Выполнить вход в систему от имени и с правами пользователя User2	Загрузка рабочего стола
2.2.1	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «regedit»	Программа «regedit» запущена
2.2.2	1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать команду «notepad»	Программа запущена
3	Редактирование настройки замкнутой программной среды	
3.1	1) Запустить консоль управления СЗИ на PC1 под учетной записью Администратора ; 2) В подсистеме «Менеджер иерархий» выбрать PC2; 3) Перейти на вкладку «Настройки», «Замкнутая программная среда»; 4) Открыть группу «Группа программ 1» на редактирование; 5) В окне «Редактирование группы программ» выбрать вкладку «Программы»; 6) Удалить из списка программ программу regedit; 7) На вкладке «Пользователи» удалить из списка пользователя User2; 8) Сохранить сформированную настройку	Список разрешенных программ для пользователя User1, User2 отредактирован
4	Проверка запуска программ от имени пользователя User2	
4.1.	Выполнить вход в систему от имени и с правами пользователя User2	Вход не выполнен
5	Проверка запуска программ от имени пользователя User1	
5.1.	Выполнить вход в систему от имени и с правами пользователя User1 на PC2	Загрузка рабочего стола
5.1.1	Выполнить следующие действия: 1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду	Программа запущена

№ п/п	Действия	Ожидаемый результат
	«Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать и выполнить команду «notepad»	
5.1.2	1) На кнопке «Пуск» вызвать контекстное меню и выбрать команду «Выполнить»; 2) В окне «Выполнить», в строке «Открыть» набрать и выполнить команду «regedit.exe»	Отказ в доступе. Появляется сообщение «Windows не удаётся получить доступ к указанному устройству, пути или файлу. Возможно у Вас нет нужных разрешений для доступа к этому объекту»
6	Регистрация событий безопасности	
6.1	Войти в систему PC1 от имени и с правами пользователя Администратора	Загрузка рабочего стола
6.2	1) Запустить консоль управления СЗИ на PC1 под учетной записью Администратор; 2) В подсистеме «Менеджер иерархий» выбрать PC2; 3) Перейти на вкладку «События»; 4) Установить фильтр по типу события «Запуск приложений»; 5) Нажать кнопку «Поиск»	Информация о событиях безопасности загружена
7	Выполнить указанные в пунктах 1–6 действия для остальных поддерживаемых ОС Windows рабочих станциях	Совпадение полученных результатов с приведенными выше результатами
Linux (РЕД ОС)		
8	Настройка списка разрешённых процессов на PC18 через сервер СЗИ PC17	
8.1	1) Запустить консоль управления СЗИ на PC17 под учетной записью Администратора ; 2) В подсистеме «Менеджер иерархий» выбрать PC18; 3) Открыть последовательно вкладки «Настройки», «Замкнутая программная среда»; 4) Включить механизм, для этого установить тумблер в положение «Механизм включен»; 5) Нажать пиктограмму «+»; 6) Выбрать режим создания замкнутой программной среды «Стандартный режим»; 7) На вкладке «Наименование» добавить имя группы программ: «Группа программ 1»; 8) Перейти на вкладку «Программы» и нажать пиктограмму «+»; 9) В открывшемся окне «Добавление процессов/программ» на вкладке «Приложения» установить флаг «Все процессы»; 10) Перейти на вкладку «Запущенные процессы» и установить флаг «Все процессы»; 11) Перейти на вкладку «Файловая система» и установить флаги на «Все процессы» и mkdir; 12) После установки флагов нажать кнопку «Добавить»;	Список разрешенных программ для пользователя User1, User2 сформирован

№ п/п	Действия	Ожидаемый результат
	13) Перейти во вкладку «Пользователи» и добавить пользователей User1 и User2; 14) Нажать кнопку «Создать» для сохранения «Группы программ 1»	
9	Проверка запуска процессов пользователем User1 и User2 на PC18	
9.1	Выполнить вход в систему PC18 от имени и с правами пользователя User1	Загрузка рабочего стола
9.2	Выполнить следующие действия: 1) Открыть «Терминал»; 2) В окне «Терминала», набрать команду «mkdir --help»; 3) Выполнить команду mkdir --help; 4) Выполнить выход из системы пользователя User1	Программа «mkdir» запущена
9.3	Выполнить вход в систему от имени и с правами пользователя User2	Загрузка рабочего стола
9.4	Выполнить следующие действия: 1) Открыть «Терминал»; 2) В окне «Терминала», набрать команду mkdir --help; 3) Выполнить команду mkdir --help; 4) Выполнить выход из системы пользователя User2	Программа «mkdir» запущена
10	Редактирование настройки замкнутой программной среды	
10.1	1) Запустить консоль управления СЗИ на PC17 под учетной записью Администратора; 2) В подсистеме «Менеджер иерархий» выбрать PC18; 3) Перейти на вкладку «Настройки», «Замкнутая программная среда»; 4) Открыть группу «Группа программ 1» на редактирование; 5) В окне «Редактирование группы программ» выбрать вкладку «Программы»; 6) Удалить из списка программ, программу mkdir; 7) На вкладке «Пользователи» удалить из списка пользователя User2; 8) Сохранить сформированную настройку	Список разрешенных программ для пользователя User1, User2 отредактирован
11	Проверка запуска программ от имени пользователя User2 на PC18	
11.1	Выполнить вход в систему от имени и с правами пользователя User2 на PC18	Вход не выполнен
12	Проверка запуска программ от имени пользователя User1 на PC18	
12.1	Выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
12.2	Выполнить следующие действия: 1) Открыть «Терминал»; 2) В окне «Терминала», набрать команду mkdir --help; 3) Выполнить команду mkdir --help	Отказ в доступе
13	Регистрация событий безопасности	
13.1	Войти в систему PC17 от имени и с правами пользователя Администратора	Загрузка рабочего стола
13.2	1) Запустить консоль управления СЗИ на PC17 под учетной записью Администратор; 2) В подсистеме «Менеджер иерархий» выбрать PC18; 3) Перейти на вкладку «События»; 4) Установить фильтр по типу события «Запуск приложений»; 5) Нажать кнопку «Поиск»	Информация о событиях безопасности загружена

Критерии оценки:

Проверка считается успешной, если:

- СЗИ контролирует запуск процессов, по модели разрешённых процессов, указанных в явном виде, для каждого пользователя;
- СЗИ контролирует запуск через ассоциированные файлы приложений;
- СЗИ реализует регистрацию событий, связанных с контролем запускаемых процессов.

2.3.5 Проверка контроля запуска программ и файлов (аудит доступа к медиафайлам)

Описание проверки:

СЗИ реализует идентификацию и аутентификацию объектов файловой системы, запускаемых и исполняемых модулей.

Выполняемые действия:

Проверка выполняется на основе действий, выполненных в п. 2.3.1 и основные ее этапы приведены в таблице ПЗ.19.

Таблица ПЗ.19 – Контроль запуска по типу файлов СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС на РС1 от имени Администратора и запустить консоль управления СЗИ под учетной записью Администратора	Появление консоли управления
2	1) В консоли управления СЗИ выбрать сервер безопасности (РС17); 2) Перейти на вкладку «Политики», «Политика клиента по умолчанию», Windows, «Аудит доступа к медиафайлам»; 3) Установить флаги на «Аудиофайлы», «Видеофайлы» и «Изображения»; 4) Нажмите кнопку «Ок» для сохранения изменений	Политика аудита доступа к медиафайлам установлена
3	Войти в ОС на РС8 от имени пользователя User1	Загрузка рабочего стола
4	Открыть соответствующей программой (назначенной по умолчанию) любой аудио, видео файл и файл изображения	Запуск аудио, видео файла и открытие файла изображения осуществляется успешно
5	Закреть приложения с аудио, видео и изображениями	Закрытие процессов
6	1) Войти в ОС на РС1 от имени Администратора; 2) Загрузить консоль управления СЗИ от имени Администратора; 3) Выбрать РС8; 4) Перейти на вкладку «События»; 5) Выбрать тип события «Аудит доступа к медиафайлам»;	Появление сообщений о запуске аудио, видео и изображения.

№ п/п	Действия	Ожидаемый результат
	6) Нажать кнопку «Поиск»; 7) Убедиться в появлении событий доступа к медиафайлам	
7	Выполнить указанные в пунктах 1–6 действия на остальных рабочих станциях с установленными ОС Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка считается успешной, если:

– средства СЗИ обеспечивают регистрацию событий по открытию аудио, видео файлов, а также файлов изображений.

2.3.6 Проверка контроля запуска исполняемого файла по маске его имени (аудит запуска приложений)

Описание проверки:

СЗИ реализует идентификацию и аутентификацию объектов файловой системы, запускаемых и исполняемых модулей.

Выполняемые действия:

Проверка выполняется на основе действий, выполненных в п. 2.3.1, а основные ее этапы приведены в таблице ПЗ.20.

Таблица ПЗ.20 – Контроль запуска исполняемых файлов, имена которых задаются по маске

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС на PC1 от имени Администратора и запустить консоль управления СЗИ под учетной записью Администратора	Появление консоли управления СЗИ
2	1) Через консоль управления СЗИ выбрать сервер безопасности PC17; 2) Выбрать вкладку «Политики»; 3) Выбрать «Политику клиента по умолчанию»; 4) Перейти на вкладку Windows, «Аудит запуска приложений»; 5) Нажать пиктограмму «+»; 6) В окне «Маска/имя файла» задать маску note* и описание: «Блокнот»; 7) Нажать кнопку «Добавить»; 8) Сохранить изменения	Настройки Контроля запуска по маске имени файла для PC17 установлены
3	Войти в ОС на PC8 от имени пользователя User1	Загрузка рабочего стола
4	Запустить wordpad.exe	Запуск успешен
5	Запустить notepad.exe	Запуск успешен
6	1) Войти на PC1 от имени Администратора и загрузить консоль управления СЗИ; 2) Выбрать PC8; 3) Перейти на вкладку «События»; 4) Выбрать тип события «Запуск приложений»; 5) Нажать кнопку «Поиск»;	Появление сообщений о запуске notepad.exe

№ п/п	Действия	Ожидаемый результат
	б) Убедиться в появлении сообщения о запуске приложения notepad.exe	
7	Выполнить указанные в пунктах 1 – 6 действия для остальных поддерживаемых ОС Windows на рабочих станциях в виртуальной сети	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка считается успешной, если СЗИ обеспечивает регистрацию событий запуска исполняемых файлов по маске.

2.4 Проверка мандатного принципа контроля доступа

2.4.1 Проверка принципа сопоставления классификационных меток каждого субъекта и каждого объекта

Описание проверки:

СЗИ реализует мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

- разграничение доступа субъектов реализуется при входе в информационную систему;
- правила разграничения доступом реализуют разграничение доступа субъектов к техническим средствам, устройствам и внешним устройствам, к объектам, создаваемым общесистемным программным обеспечением и прикладным, специальным программным обеспечением.

СЗИ реализует поддержку и сохранение установленных меток безопасности, которые используются для контроля доступа субъектов к объектам доступа.

- СЗИ реализует изменение атрибутов безопасности авторизованным пользователям;
- СЗИ реализует отображение атрибутов безопасности объектов доступа на экране монитора и при выводе информации на печать.

Выполняемые действия:

Для проведения проверки на РС8 создаются сетевые папки и назначаются права доступа согласно таблице ПЗ.21. Пользователям предоставляются полные права.

Таблица П3.21 – Матрица разграничения доступа, реализуемая средствами ОС

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

Доступ к сетевым папкам будет осуществляться от имени и с правами локальных и доменных пользователей из сегментов сети с установленной СЗИ и без таковой.

PC17 выполняет функции сервера безопасности СЗИ от НСД «Блокхост-Сеть 4» II уровня, к которому подключены PC6 и PC8.

Схема испытательного стенда и подключений пользователей для проверки сетевого мандатного принципа разграничения доступа приведена на рисунке П3.5.

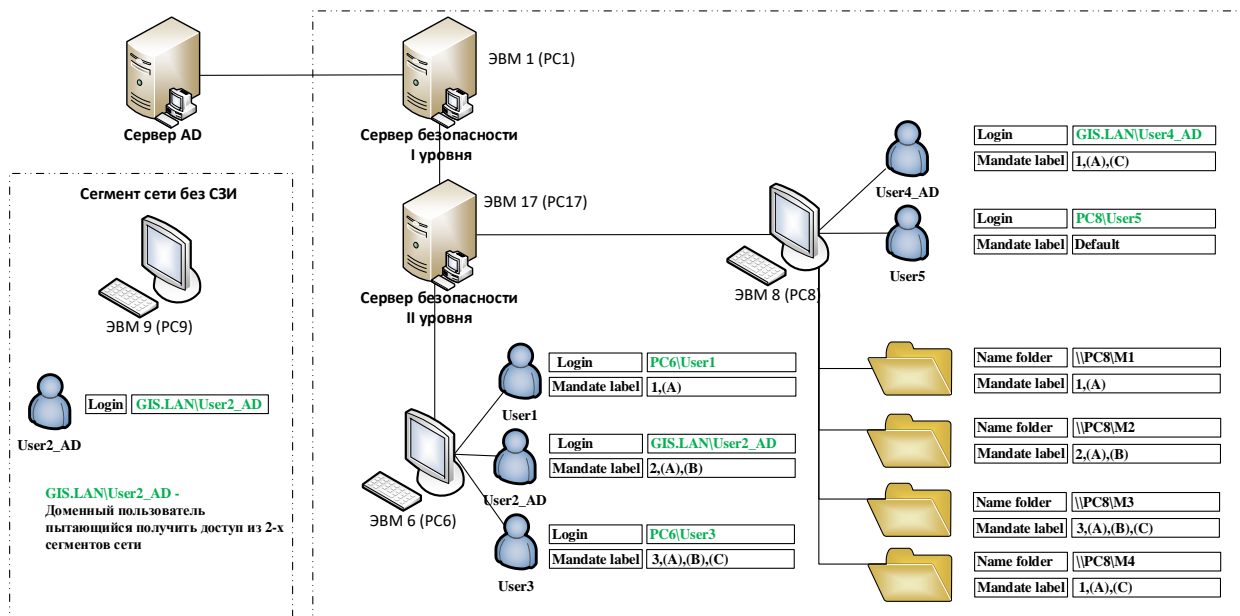


Рисунок П3.5 – Схема проведения проверки сопоставления классификационных меток

Через консоль администрирования СЗИ включается механизм мандатного доступа на PC6 и PC8, устанавливаются мандатные метки и категории для каталогов и пользователей представленной в таблице П3.22.

Таблица П3.22 – Матрица разграничения доступа

ЭВМ	СУБЪЕКТЫ	ОБЪЕКТЫ			
		\\PC8\M1	\\PC8\M2	\\PC8\M3	\\PC8\M4
		мандатная метка	мандатная метка	мандатная метка	мандатная метка
		1	2	3	1
		Категория	Категория	Категория	Категория
		(A)	(A), (B)	(A), (B), (C)	(A), (C)
PC6	PC6\User1	RW	-	-	-

	мандатная метка = 1,(A)				
PC6	GIS.LAN\User2_AD	R	RW	-	-
	мандатная метка = 2,(A),(B)				
PC6	GIS\User3	R	R	RW	R
	мандатная метка = 3,(A),(B),(C)				
PC8	GIS.LAN\User4_AD	R	-	-	RW
	мандатная метка = 1,(A),(C)				
PC9	GIS.LAN\User2_AD	X	X	X	X

Действия, выполняемые при проверке, приведены в таблице ПЗ.23.

Таблица ПЗ.23 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	Действия	Ожидаемый результат
1	Создание матрицы доступа и тестовых объектов файловой системы	
1.1	Войти на PC8 от имени и с правами пользователя Admin и выполнить следующие действия: <ul style="list-style-type: none"> • создать объекты доступа; • установить общий (сетевой) доступ для каталогов; • задать разрешение доступа согласно таблице ПЗ.20; • создать текстовые файлы: <ul style="list-style-type: none"> – c:\M1\read_1.txt; – c:\M2\read_2.txt; – c:\M3\read_3.txt – c:\M4\read_4.txt 	Объекты доступа созданы
1.2	Войти на PC17 от имени и с правами пользователя «Администратор», запустить консоль управления и выполнить следующие действия: <ul style="list-style-type: none"> • выбрать PC8; • перейти в меню «Настройки», «Мандатный доступ»; • включить тумблер «Механизм включён»; • перейти в вкладку «Каталоги»; • добавить каталоги согласно таблице ПЗ.21; • установить права доступа, согласно таблице ПЗ.22; • перейти в вкладку «Пользователи»; • добавить пользователей и установить права доступа, согласно таблице ПЗ.22; • сохранить сделанные изменения 	ПРД для PC8 созданы

№ п/п	Действия	Ожидаемый результат								
	<ul style="list-style-type: none"> выбрать РС6; перейти в меню «Настройки», «Мандатный доступ»; включить тумблер «Механизм включён»; перейти на вкладку «Каталоги»; добавить каталоги согласно таблице ПЗ.21; установить уровни доступа в соответствии с таблицей ПЗ.22; перейти на вкладку «Пользователи»; установить права доступа, согласно таблице ПЗ.22; сохранить сделанные изменения 	ПРД для РС6 созданы								
2	Просмотр событий аудита									
2.1	<ul style="list-style-type: none"> через консоль управления СЗИ выбрать РС17; выбрать вкладку «События»; из выпадающего списка «По категории» выбрать категорию «События клиента СЗИ»; нажать кнопку «Поиск». 	Появление сообщений, фиксирующих произведенные изменения настроек								
3	Проверка осуществления санкционированных попыток доступа к объектам доступа									
3.1	Выполнить вход в систему PC6 от имени и с правами локального пользователя PC6\User1 и значением мандатной метки 1, А									
3.2	Чтение файлов	<table border="1"> <tr> <td>\\PC8\M1\read_1.txt</td> <td>Успешно</td> </tr> <tr> <td>\\PC8\M2\read_2.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> <tr> <td>\\PC8\M3\read_3.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> <tr> <td>\\PC8\M4\read_4.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> </table>	\\PC8\M1\read_1.txt	Успешно	\\PC8\M2\read_2.txt	Неудачно. Отказ в доступе к папке	\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке	\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
\\PC8\M1\read_1.txt	Успешно									
\\PC8\M2\read_2.txt	Неудачно. Отказ в доступе к папке									
\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке									
\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке									
3.3	Запись файлов	<table border="1"> <tr> <td>\\PC8\M1\read_1.txt в \\PC8\M1</td> <td>Успешно. Создана копия файла</td> </tr> <tr> <td>\\PC8\M1\read_1.txt в \\PC8\M2</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> <tr> <td>\\PC8\M1\read_1.txt в \\PC8\M3</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> <tr> <td>\\PC8\M4\read_4.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> </table>	\\PC8\M1\read_1.txt в \\PC8\M1	Успешно. Создана копия файла	\\PC8\M1\read_1.txt в \\PC8\M2	Неудачно. Отказ в доступе к папке	\\PC8\M1\read_1.txt в \\PC8\M3	Неудачно. Отказ в доступе к папке	\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
\\PC8\M1\read_1.txt в \\PC8\M1	Успешно. Создана копия файла									
\\PC8\M1\read_1.txt в \\PC8\M2	Неудачно. Отказ в доступе к папке									
\\PC8\M1\read_1.txt в \\PC8\M3	Неудачно. Отказ в доступе к папке									
\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке									
3.4	Перезагрузить PC6	Появление окна аутентификации СЗИ								
3.5	Выполнить вход в систему PC6 от имени и с правами доменного пользователя GIS.LAN\User2_AD и значением мандатной метки 2, А, В									
3.6	Чтение файлов	<table border="1"> <tr> <td>\\PC8\M1\read_1.txt</td> <td>Успешно</td> </tr> <tr> <td>\\PC8\M2\read_2.txt.</td> <td>Успешно</td> </tr> <tr> <td>\\PC8\M3\read_3.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> <tr> <td>\\PC8\M4\read_4.txt</td> <td>Неудачно. Отказ в доступе к папке</td> </tr> </table>	\\PC8\M1\read_1.txt	Успешно	\\PC8\M2\read_2.txt.	Успешно	\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке	\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
\\PC8\M1\read_1.txt	Успешно									
\\PC8\M2\read_2.txt.	Успешно									
\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке									
\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке									
	Запись файлов	<table border="1"> <tr> <td>\\PC8\M2\read_2.txt в \\PC8\M1</td> <td>Неудачно</td> </tr> <tr> <td>\\PC8\M2\read_2.txt в \\PC8\M2</td> <td>Успешно. Создана копия файла</td> </tr> <tr> <td>\\PC8\M1\read_1.txt в \\PC8\M2</td> <td>Успешно. Создана копия файла</td> </tr> </table>	\\PC8\M2\read_2.txt в \\PC8\M1	Неудачно	\\PC8\M2\read_2.txt в \\PC8\M2	Успешно. Создана копия файла	\\PC8\M1\read_1.txt в \\PC8\M2	Успешно. Создана копия файла		
\\PC8\M2\read_2.txt в \\PC8\M1	Неудачно									
\\PC8\M2\read_2.txt в \\PC8\M2	Успешно. Создана копия файла									
\\PC8\M1\read_1.txt в \\PC8\M2	Успешно. Создана копия файла									

№ п/п	Действия		Ожидаемый результат
3.7	Перезагрузить PC6		Появление окна аутентификации СЗИ
3.8	Выполнить вход в систему PC6 от имени и с правами локального пользователя PC6\User3 и значением мандатной метки 3, А, В, С		
3.9	Чтение файлов	\\PC8\M1\read_1.txt	Успешно
		\\PC8\M2\read_2.txt	Успешно
		\\PC8\M3\read_3.txt	Успешно
		\\PC8\M4\read_4.txt	Успешно
	Запись файлов	\\PC8\M1\read_1.txt в \\PC8\M1	Неудачно
		\\PC8\M2\read_2.txt в \\PC8\M2	Неудачно
		\\PC8\M3\read_3.txt в \\PC8\M3	Успешно. Создана копия файла
		\\PC8\M4\read_4.txt в \\PC8\M4	Неудачно
		\\PC8\M1\read_1.txt в \\PC8\M3	Успешно
		\\PC8\M2\read_2.txt в \\PC8\M3	Успешно
		\\PC8\M4\read_4.txt в \\PC8\M3	Успешно
		\\PC8\M3\read_3.txt в \\PC8\M1	Неудачно
\\PC8\M3\read_3.txt в \\PC8\M2	Неудачно		
\\PC8\M3\read_3.txt в \\PC8\M4	Неудачно		
3.10	Перезагрузить PC6		Появление окна аутентификации СЗИ
3.11	Выполнить вход в систему PC8 от имени и с правами доменного пользователя GIS.LAN\User4_AD и значением мандатной метки 1, А, С		
3.12	Чтение файлов	C:\M1\read_1.txt	Успешно
		C:\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		C:\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		C:\M4\read_4.txt	Успешно
	Запись файлов	C:\M4\read_4.txt в C:\M1	Неудачно
		C:\M4\read_4.txt в C:\M4	Успешно. Создана копия файла
		C:\M1\read_1.txt в C:\M4	Успешно
Перезагрузить PC8		Появление окна аутентификации СЗИ	
4	Проверка осуществления несанкционированных попыток доступа к объектам доступа		
4.1	Выполнить вход в систему PC9 от имени и с правами доменного пользователя GIS.LAN\User2_AD		
	Чтение файлов	\\PC8\M1\read_1.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке
4.2	Перезагрузить PC9		Появление окна аутентификации
4.3	Выполнить вход в систему PC9 от имени и с правами локального пользователя PC9\User2		
	Чтение файлов	\\PC8\M1\read_1.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M2\read_2.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		\\PC8\M4\read_4.txt	Неудачно. Отказ в доступе к папке

№ п/п	Действия	Ожидаемый результат
4.4	Перезагрузить РС9	Появление окна аутентификации
5	Просмотр событий аудита	
5.1	Войти на РС1 от имени и правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ РС1, вкладку «События»; 3) нажать кнопку «Поиск»	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
6	Выполнить указанные в пунктах 1 – 5 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных ОС Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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

- средства СЗИ обеспечивают назначение классификационных меток (уровней конфиденциальности) объектам файловой системы и пользователям (процессам пользователей) с помощью меток конфиденциальности;
- СЗИ обеспечивают управление потоками информации (при работе с объектами доступа, расположенными на локальной рабочей станции) на основе сопоставления классификационных уровней:
 - субъект получает доступ к объекту по чтению, если значение его иерархической метки больше или равно значению иерархической метки объекта, а неиерархическая категория объекта входит в состав неиерархических категорий субъекта;
 - субъект получает доступ к объекту по записи, если значение его иерархической метки равно значению иерархической метки объекта, а все неиерархические категории субъекта входят в состав неиерархических категорий объекта);
- СЗИ реализует мандатный механизм контроля доступа к защищаемым ресурсам для всех пользователей СЗИ и ОС;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым локальным объектам.

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

Описание проверки:

СЗИ реализует мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

- разграничение доступа субъектов реализуется при входе в информационную систему;
- правила разграничения доступом реализуют разграничение доступа субъектов к техническим средствам, устройствам и внешним устройствам, к объектам, создаваемым общесистемным программным обеспечением и прикладным, специальным программным обеспечением.

Выполняемые действия:

Действия, выполняемые по изменению значений классификационных меток, в данной проверке подробно не описываются, поскольку они представлены в таблице ПЗ.23 пункта 2.4.1. По умолчанию, любому добавляемому в список СЗИ субъекту присваивается иерархическая мандатная метка со значением 1 и не назначены неиерархические категории. Изменение значения присвоенной пользователю иерархической метки возможно после его добавления в список пользователей.

При добавлении новых объектов иерархическая метка, равная иерархической 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 иерархическая метка с низшим значением (со значением 1 без присвоения неиерархических категорий). Изменение значения иерархической метки нового объекта возможно сразу после его появления в СВТ.

Действия при проверке данного пункта указаны в таблице ПЗ.24.

Таблица ПЗ.24 – Действия при проверке запроса и получение классификационных меток при вводе новых данных в систему в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	Создание объекта доступа	
1.1	Войти на РС8 от имени и с правами Администратор и создать файл test_label.txt в каталоге \\PC8\M1	Создание файла
2	Создание субъекта доступа	

№ п/п	Действия	Ожидаемый результат
2.1	Войти на РС17 от имени и с правами пользователя «Администратор», запустить консоль управления и выполнить следующие действия: <ul style="list-style-type: none"> • выбрать РС8; • перейти в меню «Настройки», «Мандатный доступ»; • перейти в вкладку «Пользователи»; • установить мандатные метки и категорию 1, (A) для локального пользователя User5; • применить сделанные изменения. 	Появление пользователя с мандатной меткой и категорией 1,(A)
3	Сопоставление классификационных меток	
3.1	Войти на РС8 от имени и с правами пользователя User5 и значением мандатной метки 1, A и выполнить следующие действия:	Загрузка рабочего стола
3.2	Чтение файлов \\PC8\M1test_label.txt	Успешно
3.3	Запись файлов \\PC8\M1test_label.txt	Успешно
4	Просмотр событий аудита	
4.1	Войти в ОС РС1 от имени и с правами пользователя Admin	Загрузка рабочего стола
4.2	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать сервер СЗИ РС17, вкладку «События»; • нажать кнопку «Поиск» 	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
5	Выполнить указанные в пунктах 1 – 4 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Испытания проверки запроса и получения классификационных 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.

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

Описание проверки:

СЗИ реализует мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если классификационный уровень субъекта

в иерархической классификации не меньше, чем классификационный уровень объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта.

– субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Выполняемые действия:

Проверка выполняется на основе действий, выполненных в п. 2.4.1, согласно таблице ПЗ.22, в которой приведена проверка реализации мандатного принципа контроля доступа применительно ко всем объектам при явном доступе.

Действия при проверке реализации мандатного механизма СЗИ при скрытом доступе пользователей к объектам приведены в таблице ПЗ.25.

Таблица ПЗ.25 – Действия при проверке реализации мандатного принципа контроля доступа применительно ко всем объектам при скрытом доступе со стороны любого из субъектов

№ п/п	Действия	Ожидаемый результат	
1	Выполнить вход в систему PC6 от имени и с правами доменного пользователя GIS.LAN\User2_AD и значением мандатной метки 2, A, B	Загрузка рабочего стола	
2	Запустить программу Far	Появление интерфейса программы	
2.1	Чтение файлов	D:\M1\read_1.txt	Успешно
		D:\M2\read_2.txt.	Успешно
		D:\M3\read_3.txt	Неудачно. Отказ в доступе к папке
		D:\M4\read_4.txt	Неудачно. Отказ в доступе к папке
2.2	Запись файлов	D:\M2\read_2.txt в D:\M1	Неудачно
		D:\M2\read_2.txt в D:\M2	Успешно. Создана копия файла
		D:\M1\read_1.txt в D:\M2	Успешно. Создана копия файла
3	Войти на PC1 от имени и справами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC17, вкладку «События» 3) установить фильтр по категории «Дискреционный доступ» 4) нажать кнопку «Поиск»	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам	
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows	Совпадение полученных результатов с приведенными выше результатами	

Критерии оценки:

Проверка считается успешной, если:

- результаты явного и скрытого доступа субъектов к объектам при проверке по п. 2.4.3 совпадают с результатами, полученными при проверке явного доступа субъектов к объектам по п. 2.4.1.

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

Описание проверки:

Реализация мандатных ПРД предусматривает возможность сопровождения изменения классификационных уровней субъектов и объектов специально выделенными субъектами (АБ СЗИ).

Выполняемые действия:

Проверка осуществляется на основе действий, выполняемых в пп. 2.3.3 и 2.4.1.

Пользователи Safety_AD и User2_AD на сервере безопасности СЗИ II уровня попытаются изменить мандатные метки и категории для пользователя User1 и каталога M1, через консоль управления СЗИ.

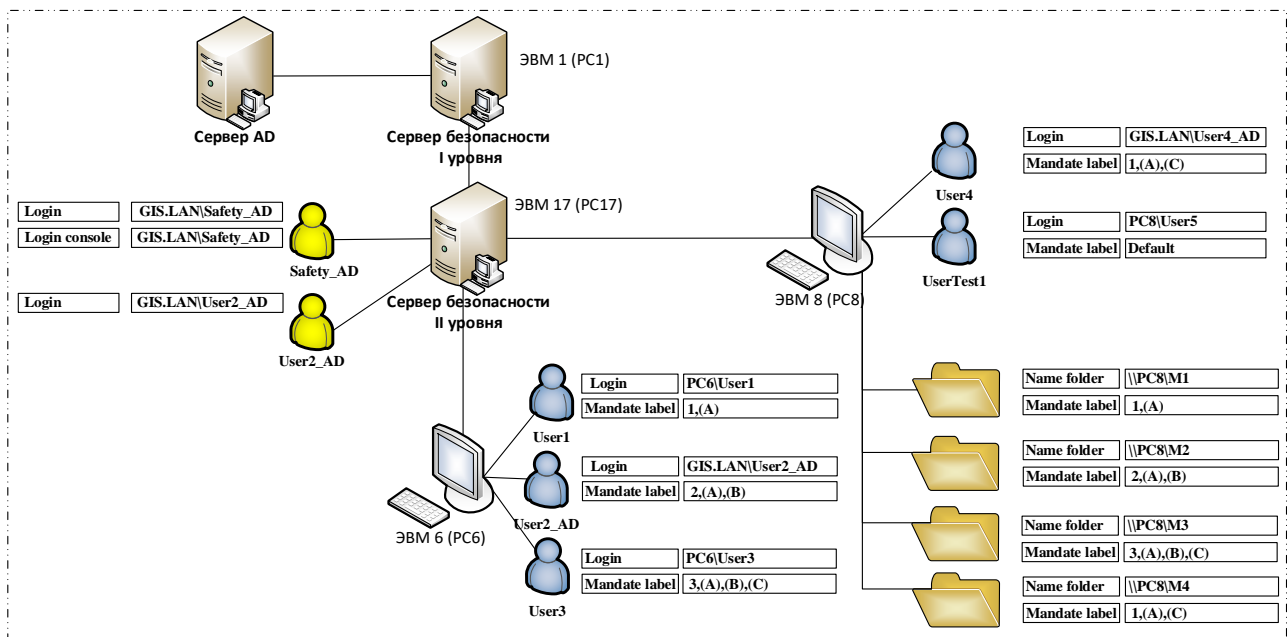


Рисунок ПЗ.6 – Схема проверки изменения классификационных уровней

Подробные действия при проверке данного пункта указаны в таблице ПЗ.26.

Таблица ПЗ.26 – Действия при проверке возможности сопровождения (изменения) классификационных уровней субъектов и объектов специально выделенными субъектами в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	От имени и с правами пользователя GIS.LAN\User2_AD войти на сервер безопасности II уровня PC17	Успешно
1.1	Запустить консоль управления СЗИ	Отказ в доступе «У пользователя недостаточно прав».
2	От имени и с правами пользователя GIS.LAN\Safety_AD войти на сервер безопасности II уровня PC17	Успешно
2.1	Запустить консоль управления СЗИ от имени и с правами пользователя БХС «Safety_AD»	Успешно
2.2	Выполнить следующие действия: <ul style="list-style-type: none"> • выбрать PC8; • перейти по пути «Настройки», «Мандатный доступ», «Пользователи»; • выбрать пользователя User1 • изменить уровень доступа с метки 1 «Открытые данные» на метку 2 «Конфиденциальные данные»; • изменить мандатную категорию с (А) на (В); • перейти в вкладку «Каталоги» • выбрать каталог «М1» • изменить уровень доступа с метки 1 «Открытые данные» на метку 2 «Конфиденциальные данные»; • изменить мандатную категорию с (А) на (В) • применить сделанные изменения • восстановить параметры • применить сделанные изменения 	Успешное изменение мандатной метки и мандатной категории субъектам и объектам доступа
2.3	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC17, вкладку «События»; 3) установить фильтр на раздел: «Типы событий» - «События клиента СЗИ»; 4) нажать кнопку «Поиск»; 5) убедиться в появлении сообщений, фиксирующих произведенное изменение настроек 	Появление сообщений, фиксирующих произведенное изменение настроек
2.4	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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

2.4.5 Проверка реализации диспетчера доступа

Описание проверки:

В СЗИ 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.

Выполняемые действия:

Проверка выполняется на основе проверок согласно п. 2.3.1 и 2.4.1 диспетчер доступа реализует функциональность контроля и разграничения доступа в полном объеме.

Схема проверки представлена на рисунке ПЗ.7. Для каталога D1 расположенного на PC8, устанавливаются дискреционные и мандатные атрибуты доступа, представленные в таблице ПЗ.27.

Доступ к каталогу D1 осуществляется доменным пользователем User1_AD с PC6.

Таблица ПЗ.27 – Устанавливаемые дискреционные и мандатные атрибуты доступа

Субъекты доступа (пользователи и группы пользователей)	Дискреционные атрибуты		Объекты	Мандатные атрибуты	
	R	W		Мандатная метка	Категория
User1_AD	+	+	\\D1	2	(A)
	+	+	Test1	*	*
мандатная метка = 2,(A)	+	-	Test2	*	*
	-	-	Test3	*	*
	*	*	Test4	*	*

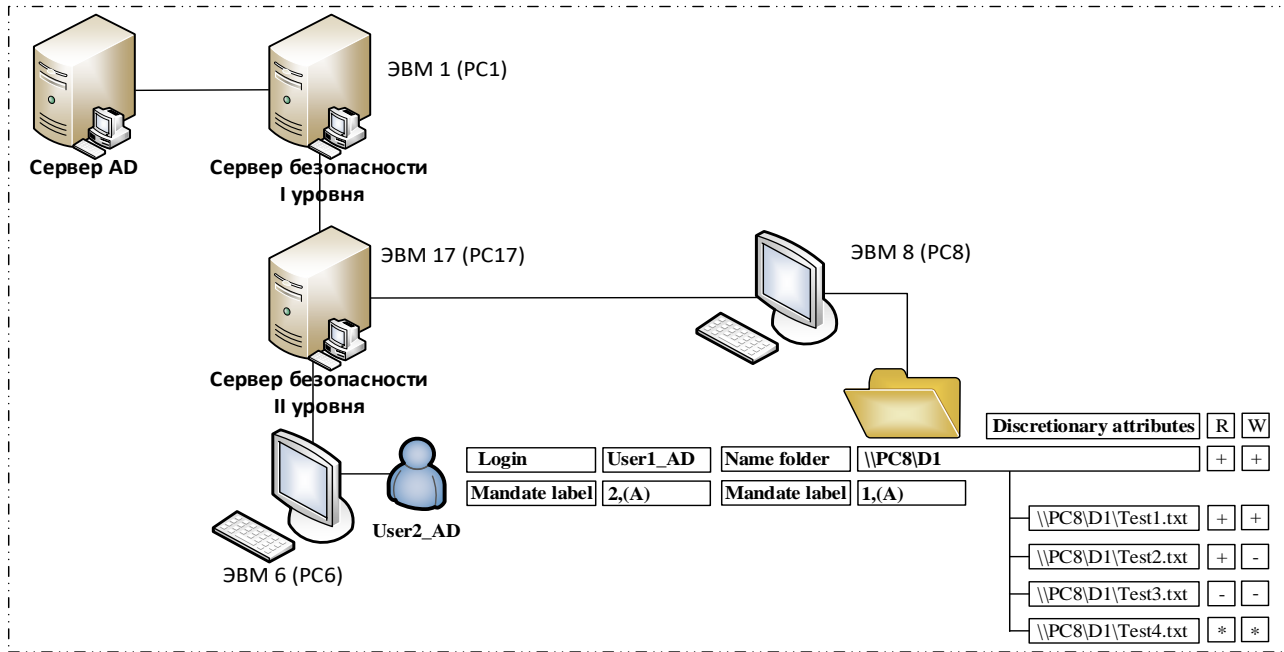


Рисунок П3.7 – Схема проверки реализации диспетчера доступа

Подробные действия при проверке данного пункта указаны в таблице П3.28.

Таблица П3.28 – Действия при проверке реализации диспетчера доступа

№ п/п	Действия	Ожидаемый результат	
1	Проверка осуществления санкционированных попыток доступа к объектам доступа		
1.1	Войти на PC17 от имени и с правами пользователя «Администратор», запустить консоль администрирования и выполнить следующие действия:		
	• выбрать PC8;		
	• перейти в меню «Настройки», «Мандатный доступ», «Каталоги»;	ПРД для PC8 созданы	
	• добавить каталог C:\D1 и установить мандатные метки и категории согласно таблице П3.27;		
	• перейти в меню «Настройки», «Мандатный доступ», «Пользователи»;		
	• установить мандатные метки и категории согласно таблице П3.26 пользователю User1_AD;		
	• применить сделанные изменения.		
2	Выполнить вход в систему PC6 от имени и с правами доменного пользователя User1_AD и значением мандатной метки 2, A		
2.1	Чтение каталога \\PC8\D1\	Успешно	
2.2	Чтение файлов	\\PC8\D1\test_1.txt	Успешно
		\\PC8\D1\test_2.txt	Неудачно. Отказ в доступе к папке
		\\PC8\D1\test_3.txt	Неудачно. Отказ в доступе к папке
		\\PC8\D1\test_4.txt	Успешно
2.3	Запись файлов \\PC8\D1\test_1.txt	Успешно. Создана копия файла	

		\\PC8\D1\test_2.txt	Неудачно. Отказ в доступе к папке
		\\PC8\D1\test_3.txt	Неудачно. Отказ в доступе к папке
		\\PC8\D1\test_4.txt	Успешно
3	Просмотр событий аудита		
3.1	Войти в ОС PC1 от имени и с правами пользователя Admin		Загрузка рабочего стола
3.2	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль администрирования СЗИ; 2) выбрать сервер СЗИ PC17, вкладку «События»; 3) нажать кнопку «Поиск»; 4) убедиться в появлении событий, фиксирующих произведенные попытки доступа к контролируемым объектам		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем Windows		Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Положительные результаты проверки согласно пункту 2.3.1 и положительные результаты при проверке настоящего пункта методики 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 контролируемые.

2.5 Проверка управления СЗИ и иерархии серверов безопасности

Описание проверки:

СЗИ осуществляет централизованное управление функциональными возможностями безопасности, клиентов СЗИ на защищаемых ПК, а также на СБ СЗИ.

СЗИ обеспечивает централизованное управление клиентами СЗИ, на защищаемых ПК, а также серверами безопасности СЗИ, развернутыми в сети ИС. Управление клиентами и СБ СЗИ осуществляется при помощи настроек безопасности и политик, которые назначаются для ПК/группы ПК или для пользователей/группы пользователей в зависимости от назначаемой политики.

СЗИ предоставляет АБ СЗИ графический интерфейс – консоль управления, с помощью которой он сможет осуществлять управление настройками безопасности.

Настройки безопасности передаются на выбранный ПК с сервера безопасности СЗИ и хранятся в БД настроек клиента СЗИ.

В СЗИ реализована возможность централизованного управления защищаемыми ПК в составе ИС, а также возможность управления несколькими ПК, объединенных в именованные группы.

В СЗИ реализованы функции АБ СЗИ по управлению группами ПК:

- создание/удаление группы ПК;
- включение/исключение ПК в (из) группы;
- перемещение ПК между группами.

В консоли администрирования СЗИ реализована возможность формирования и визуализации списков защищаемых ПК/групп ПК, а также серверов безопасности, при помощи средств графического интерфейса.

Выполняемые действия:

Проверка выполняется согласно действиям, выполняемым в п. 2.1.3 настоящего документа.

Критерии оценки:

Результаты проверки признаются успешными, если:

- иерархия серверов безопасности сформирована без ошибок и сбоев;
- сформированы группы компьютеров, подчиненных серверам безопасности;
- на консоли администрирования визуализирована возможность формирования и изменения групп (списков) защищаемых ПК;
- политики безопасности передаются по иерархии серверов.

2.6 Проверка очистки памяти

2.6.1 Проверка возможности очистки внешней памяти

В СЗИ от НСД «Блокхост-Сеть 4» очистка внешней памяти выполняется модулем диспетчера доступа и гарантированного удаления. При попытке удаления поставленного на контроль гарантированного удаления файла диспетчер доступа запрещает удаление средствами ОС и запускает модуль гарантированного удаления.

Модуль гарантированного удаления перехватывает запрос на удаление только при включенной политике в настройках СЗИ. Поставленные на контроль файлы удаляются путем затирания их содержимого по специальному алгоритму, который исключает считывание остаточной информации на диске после удаления.

Описание проверки:

Уничтожение информации реализуется многократной перезаписью МНИ специальными битовыми последовательностями и очисткой физического пространства накопителя.

- СЗИ обеспечивает регистрацию действий по удалению защищаемой информации
- СЗИ обеспечивает уничтожение (стирание) информации на машинных носителях, исключая возможность восстановления защищаемой информации полной многократной перезаписью машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами.

Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя, через реестры, оперативную память, внешние запоминающие устройства, ресурсы файловой системы и иные общие для пользователей ресурсы информационной системы.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.29.

Таблица ПЗ.29 – Действия при проверке очистки внешней памяти

№ п/п	Действия	Ожидаемый результат
Проверка очистки внешней памяти в ОС Windows		
1	Войти в ОС PC2 под именем и с правами пользователя Администратора	Загрузка ОС. Появление рабочего стола
2	Создать текстовый файл с уникальным именем <i>C:\TestDel.txt</i> и на USB-носителе <i>E:\TestDel_flash.txt</i> Набрать в указанном файле текст, содержащий следующую тестовую последовательность: Secret File 0xjhqWXpTHWAFhHfjXjGd5fAwrLAB1XJIE4lsAUyd2tQ1d6gh& 8*(hyrt%4#erj90 Сохранить файл <i>TestDel.txt</i> и <i>TestDel_flash.txt</i>	Созданные файлы <i>C:\TestDel.txt</i> , <i>E:\TestDel_flash.txt</i> сохранены
3	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на диске <i>C:\</i> и на USB-носителе	Тестовая последовательность найдена

№ п/п	Действия	Ожидаемый результат
4	<p>От имени и с правами пользователя Администратор вошли на PC1 в консоли управления СЗИ:</p> <ul style="list-style-type: none"> • выбрать сервер безопасности PC1; • перейти на вкладку «Политики»; • выбрать «Клиентские политики», «Политика клиента по умолчанию»; • в окне «Политика клиента по умолчанию» выбрать раздел Windows и вкладку «Гарантированное удаление файлов»; • установить флаги у параметров «Системный диск», «Не системные диски» и «Вести аудит гарантированного удаления»; • сохранить сделанные изменения. 	Политика гарантированного удаления файлов установлена
5	Перезагрузить PC2, выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
6	Произвести удаление тестовых файлов C:\TestDel.txt и E:\TestDel_flash.txt (поместить в «Корзину»)	Файлы C:\TestDel.txt и E:\TestDel_flash.txt удалены (помещен в «Корзину»)
7	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на диске C:\ и на USB-носителе	Тестовая последовательность найдена
8	Восстановить файл из «Корзины» и удалить с помощью сочетания клавиш <Shift>+	«Корзина» пуста. Файл удален
9	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на диске C:\ и на USB-носителе	Тестовая последовательность не найдена
10	Перезагрузить PC2, войти в систему под именем и с правами пользователя Администратора	Загрузка ОС. Появление рабочего стола
11	<p>Создать текстовый файл с уникальным именем C:\TestDel.txt и на USB-носителе E:\TestDel_flash.txt</p> <p>Набрать в указанном файле текст, содержащий следующую тестовую последовательность:</p> <p>Secret File 0xjqhWXpTHWAFhHfjXjGd5fAwrLAbB1XJIE4lsAUyD2tQ1d6gh&8*(hyrt%4#erj90</p> <p>Сохранить файл TestDel.txt и TestDel_flash.txt</p>	Созданные файлы C:\TestDel.txt и E:\TestDel_flash.txt сохранены
12	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на диске C:\ и на USB-носителе	Тестовая последовательность найдена
13	Перезагрузить PC2, выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола
14	Произвести удаление тестовых файлов C:\TestDel.txt и E:\TestDel_flash.txt (поместить в «Корзину»)	Файлы C:\TestDel.txt и E:\TestDel_flash.txt удалены (помещен в «Корзину»)
15	Очистить корзину	«Корзина» пуста. Файлы C:\TestDel.txt и E:\TestDel_flash.txt удалены
16	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на диске C:\	Тестовая последовательность не найдена
17	Просмотр событий аудита	
18	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать сервер СЗИ PC1, вкладку «События»; 	Появление сообщений, фиксирующих успешные попытки доступа к контролируемому объекту

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> нажать кнопку «Поиск». 	
19	Выполнить указанные в пунктах 1 – 18 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
20	Выполнить проверку возможности очистки внешней памяти без использования СЗИ от НСД «Блокхост-Сеть 4»	Тестовая последовательность найдена при удалении с помощью сочетания клавиш <Shift>+ и при удалении с помощью очистки корзины
Проверка очистки внешней памяти в ОС Linux		
1	Перезагрузить РС18, выполнить вход в систему от имени и с правами пользователя Администратор	Загрузка рабочего стола
2	Открыть терминал и выполнить следующие подготовительные действия: <ul style="list-style-type: none"> установить утилиту blknmbr (разработана для подтверждения свойств Изделия и не входит в состав дистрибутива изделия); создать в ОС Linux раздел НЖМД с файловой системой ext3 объемом не менее 1 Гб; добавить данный раздел в каталог /media/hdd. 	Подготовительные действия выполнены. Раздел ext3 добавлен
3	Гарантированное удаление файла размером менее 4 Кбайт	
3.1	Выполнить следующие действия: <ul style="list-style-type: none"> создать файл test.txt в каталоге /media/hdd и записать в него текст qwerty1234; считать номер блока файла test.txt с помощью команды: <code>./blknmbr /media/hdd/test.txt</code>; считать содержимое блока с помощью команды: <code>dd if=/dev/sda3 of=/dev_sda3 bs=4096 count=1 skip=(номер блока файла)</code>; удалить файл test.txt с помощью утилиты gupt, для этого выполнить команду: <code>/opt/Blockhost/client/bhgupt /media/hdd/test.txt</code>; перейти в каталог /media/hdd и убедиться, что файл test.txt удален. 	Файл test.txt создан. Считано содержимое блока файла. Файл test.txt удален с помощью утилиты gupt
3.2	Считать содержимое блока с помощью команды: <code>dd if=/dev/sda3 of=/dev_sda3_new bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блока файла считано (случайная последовательность)
3.3	Провести анализ содержимого НЖМД на наличие текста qwerty1234 с помощью утилиты mc	Провели анализ НЖМД
4	Гарантированное удаление файла размером более 4 Кбайт	
4.1	Выполнить следующие действия: <ul style="list-style-type: none"> создать файл test.txt в каталоге /media/hdd и записать в него текст размером 10240 байт, начинающийся и заканчивающийся последовательностью символов Secret File 0xjqhWXpTHWAFhHfjXjGd5fAwRLAbB1XJIE4lsAUyd2tQ1d6gh&8*(hyrt%4#erj90 считать номера блоков файла test.txt с помощью команды: <code>./blknmbr /media/hdd/test.txt</code>; считать содержимое блоков с помощью команды: <code>dd if=/dev/sda3 of=/dev_sda3 bs=4096 count=1 skip=(номер блока файла)</code>; удалить файл test.txt с помощью утилиты gupt, для этого выполнить команду: <code>/opt/Blockhost/client/bhgupt /media/hdd/test.txt</code>; перейти в каталог /media/hdd и убедиться, что файл test.txt удален. 	Файл test.txt создан. Считаны номера блоков файла. Считано содержимое блоков. Файл test.txt удален с помощью утилиты gupt
4.2	Считать содержимое блоков файла test.txt с помощью	Содержимое блока файла считано

№ п/п	Действия	Ожидаемый результат
	команды: dd if=/dev/sda3 of=dev_sda3_new bs=4096 count=2 skip=(номер первого блока файла)	(случайная последовательность)
4.3	Провести анализ содержимого НЖДМ с помощью утилиты mc на наличие символов Secret File 0xjhhqWXpTHWAFhHfjXjGd5fAwrLAbB1XJIE4lsAUyd2tQ1d6gh&8*(hyrt%4#erj90	Провели анализ НЖДМ. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.4.1 данной таблицы
5	Гарантированное уничтожение данных на свободном пространстве НЖМД после удаления файла размером менее 4 КБайт	
5.1	Выполнить следующие действия: <ul style="list-style-type: none"> создать файл test.txt в каталоге /media/hdd и записать в него текст qwerty1234; считать номер блока файла test.txt с помощью команды: ./blknmbr /media/hdd/test.txt; считать содержимое блока с помощью команды: dd if=/dev/sda3 of=dev_sda3 bs=4096 count=1 skip= (номер блока файла); перейти в каталог /media/hdd; удалить файл test.txt с помощью средств ОС. 	Файл test.txt создан. Считан номер блока файла. Считано содержимое блока файла. Файл test.txt удален
5.2	Считать содержимое блока с помощью команды: dd if=/dev/sda3 of=dev_sda3_new bs=4096 count=1 skip=(номер блока файла)	Содержимое блока файла считано
5.3	Стереть свободное пространство на разделе НЖМД с помощью утилиты gupt, выполнив команду: /opt/Blockhost/client/bhgupt -d /media/hdd	Свободное пространство на НЖМД стерто средствами gupt
5.4	Считать содержимое блока с помощью команды: dd if=/dev/sda3 of=dev_sda3_new bs=4096 count=1 skip=(номер блока файла)	Считали содержимое блока файла
5.5	Провести анализ содержимого НЖДМ на наличие текста qwerty1234 с помощью утилиты mc	Провели анализ НЖДМ. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.5.2 данной таблицы
6	Гарантированное стирание свободного пространства НЖМД после удаления файлов	
6.1	Выполнить следующие действия: <ul style="list-style-type: none"> создать файлы test0.txt, test1.txt, ... и test6.txt в каталоге /media/hdd с произвольным содержанием и размером 81920 байт (4096 x 20 блоков); считать номера блоков созданных файлов с помощью команды: ./blknmbr /media/hdd/<name file>.txt; перейти в каталог /media/hdd; удалить файлы test0.txt, test1.txt и test3.txt с помощью команды средств ОС; считать содержимое блоков для каждого файла с помощью команды: dd if=/dev/sda3 of=dev_sda3_N bs=4096 count=20 skip=(номер первого блока каждого файла), где N – порядковый номер файла 	Созданы файлы test0.txt, test1.txt, ... test6.txt. Считаны номера блоков созданных файлов. Удалены файлы test0.txt, test1.txt, test3.txt
6.2	Стереть свободное пространство на разделе НЖМД с помощью утилиты gupt, выполнив команду: /opt/Blockhost/client/bhgupt -d /media/hdd	Свободное пространство на НЖМД стерто
6.3	Перейти в каталог /media/hdd и убедиться в наличии файлов test2.txt, test4.txt, test5.txt и test6.txt	Убедились в наличие файлов test2.txt, test4.txt, test5.txt и test6.txt в каталоге /media/hdd
6.4	Считать содержимое блоков для каждого файла с помощью	Содержимое блока каждого файла

№ п/п	Действия	Ожидаемый результат
	команды: <code>dd if=/dev/sda3 of=dev_sda3_N_new bs=4096 count=20 skip=(номер первого блока каждого файла)</code>	считано
6.5	Убедиться, что содержимое файлов <code>test2.txt</code> , <code>test4.txt</code> , <code>test5.txt</code> и <code>test6.txt</code> не повреждено и соответствует данным внесенным в файлы в п.6.1 данной таблицы	Убедились, что содержимое файлов <code>test2.txt</code> , <code>test4.txt</code> , <code>test5.txt</code> и <code>test6.txt</code> не повреждено
6.6	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code>	Провели анализ НЖДМ. Убедились в невозможности восстановить исходные файлы <code>test0.txt</code> , <code>test1.txt</code> и <code>test3.txt</code>
7	Рекурсивное гарантированное удаление каталога с файлами	
7.1	Выполнить следующие действия: <ul style="list-style-type: none"> в каталоге <code>/media/hdd</code> создать каталог <code>test</code> и внутри него создать подкаталоги <code>test1</code> и <code>test2</code> соответственно с файлами <code>a.txt</code>, <code>b.txt</code> и <code>c.txt</code>, <code>d.txt</code>. В каталоге <code>/media/hdd/test</code> создать файл <code>test.txt</code>. Размеры созданных файлов должны быть менее 4096 байт с произвольным содержимым; считать номера блоков для всех созданных файлов с помощью команды: <code>./blknmbr /media/hdd/.../<name file>.txt</code>; считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>.txt bs=4096 count=1 skip=(номер блока файла)</code>; удалить каталог <code>/media/hdd/test</code> рекурсивно с помощью команды: <code>/opt/Blockhost/client/bhgupt -r /media/hdd/test</code>; перейти в каталог <code>/media/hdd</code> и убедиться в удалении подкаталога <code>test</code>; считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>_new.txt bs=4096 count=1 skip=(номер блока файла)</code>. 	Созданы файлы и подкаталоги. Удалили каталог <code>test</code> средствами <code>gupt</code> . Считано содержимое блоков для каждого файла.
7.2	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое считанных файлов не соответствует данным внесенным в файлы при их создании	Провели анализ НЖДМ. Убедились, что содержимое считанных файлов не соответствует данным внесенным в файлы при их создании
8	Гарантированное удаление файлов по списку	
8.1	Выполнить следующие действия: <ul style="list-style-type: none"> создать файлы <code>test1.txt</code>, <code>test2.txt</code> и <code>test3.txt</code> в каталоге <code>/media/hdd</code> с произвольным содержанием и размером каждого файла менее 4096 байт; считать номера блоков созданных файлов с помощью команды: <code>./blknmbr /media/hdd/<name file>.txt</code>; считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>.txt bs=4096 count=1 skip=(номер первого блока файла)</code>; создать текстовый файл <code>names.txt</code> в каталоге <code>/media/hdd</code> и внести в него список созданных файлов, через разделитель «;»: <code>/media/hdd/test1.txt</code>; <code>/media/hdd/test2.txt</code>; <code>/media/hdd/test3.txt</code>; удалить файлы согласно созданному списку с помощью команды: <code>/opt/Blockhost/client/bhgupt -f /media/hdd/names.txt</code>. 	Созданы файлы <code>test1.txt</code> , <code>test2.txt</code> , <code>test3.txt</code> . Считаны номера блоков и их содержимое. Удалили файлы <code>test1.txt</code> , <code>test2.txt</code> , <code>test3.txt</code> с использованием <code>gupt</code> и файла списка
8.2	Перейти в каталог <code>/media/hdd</code> и убедиться в отсутствии файлов <code>test1.txt</code> , <code>test2.txt</code> и <code>test3.txt</code>	Убедились в отсутствии файлов <code>test1.txt</code> , <code>test2.txt</code> и <code>test3.txt</code>
8.3	Считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>_new.txt bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блока каждого файла считано
8.4	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code>	Провели анализ НЖДМ.

№ п/п	Действия	Ожидаемый результат
	и убедиться, что содержимое файлов test1.txt, test2.txt и test3.txt не соответствует данным внесенным в файлы в п.9.1 данной таблицы	Убедились, что содержимое файлов test1.txt, test2.txt и test3.txt не соответствует данным, внесенным в файлы в п.9.1 данной таблицы
9	Гарантированное удаление каталогов по списку из файла	
9.1	<p>Выполнить следующие действия:</p> <ul style="list-style-type: none"> • в каталоге /media/hdd создать каталог test и внутри него создать подкаталоги test1 и test2 соответственно с файлами a.txt, b.txt и c.txt, d.txt. Размеры файлов должны быть менее 4096 байт с произвольным содержимым; • считать номера блоков для всех созданных файлов с помощью команды: <code>./blknmbr /media/hdd/.../<name file>.txt</code>; • считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>.txt bs=4096 count=1 skip=(номер блока файла)</code>; • создать текстовый файл names.txt в каталоге /media/hdd и внести в него список созданных подкаталогов, через разделитель «;»:<ul style="list-style-type: none"> ○ /media/hdd/test1; ○ /media/hdd/test2; • удалить каталоги согласно списку с помощью команды: <code>/opt/Blockhost/client/bhgupt -f /media/hdd/names.txt</code> 	Созданы файлы и подкаталоги. Считано содержимое блоков для каждого файла. Удалили каталог средствами <code>gupt</code> по списку
9.2	Перейти в каталог /media/hdd и убедиться в отсутствии каталогов test1 и test2	Убедились в отсутствии каталогов test1 и test2
9.3	Считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name file>_new.txt bs=4096 count=1 skip=(номер блока файла)</code>	Считали содержимое блоков каждого файла
9.4	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое полученных файлов в удаленных каталогах не соответствует данным сохраненным в п.10.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученных файлов в удаленных каталогах не соответствует файлам, сохраненным в п.10.1 данной таблицы
10	Гарантированное удаление файлов на USB носителях	
10.1	<p>Выполнить следующие действия:</p> <ul style="list-style-type: none"> • примонтировать USB-носитель и создать на нем файл test.txt; • записать в файл test.txt текст <code>qwerty1234</code>; • считать номера блоков для созданного файла с помощью команды: <code>./blknmbr /(путь до USB-носителя)/test.txt</code>; • считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/<имя USB-устройства> of=test.txt bs=4096 count=1 skip=(номер блока файла)</code>; • удалить файл с помощью команды: <code>/opt/Blockhost/client/bhgupt /(путь до USB-носителя)/test.txt</code>; • перейти на USB-носитель и убедиться, что файл test.txt удален; • считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/<имя USB-устройства> of=test_new.txt bs=4096 count=1 skip=(номер блока файла)</code>; 	Создан файл test.txt на USB-носителе. Удален файл test.txt утилитой <code>gupt</code> . Считано содержимое блоков файла.
10.2	Провести анализ содержимого USB-диска и убедиться, что содержимое полученных файлов не соответствует данным внесенным в файл при его создании.	Провели анализ USB-диска. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.11.1 данной таблицы

№ п/п	Действия	Ожидаемый результат
11	Гарантированное удаление нескольких файлов	
11.1	Выполнить следующие действия: <ul style="list-style-type: none"> • в каталоге /media/hdd создать файлы test.txt, test2.txt и записать в них текст qwerty1234; • считать номера блоков для всех созданных файлов с помощью команды: ./blknbr /media/hdd/<name file>.txt; • считать содержимое блоков для каждого файла с помощью команды: dd if=/dev/sda3 of=<name file>.txt bs=4096 count=1 skip=(номер блока файла); • гарантированно удалить созданные файлы с помощью команды: /opt/Blockhost/client/bhgupt /media/hdd/test.txt /media/hdd/test2.txt 	Созданы файлы. Считаны номера блоков для каждого файла. Считано содержимое блоков для каждого файла. Удалили файлы средствами gupr
11.2	Перейти в каталог /media/hdd и убедиться в отсутствии файлов test.txt и test2.txt	Убедились в отсутствии файлов test.txt и test2.txt
11.3	Считать содержимое блоков для каждого файла с помощью команды: dd if=/dev/sda3 of=<name file>_new.txt bs=4096 count=1 skip=(номер блока файла)	Содержимое блока каждого файла считано
11.4	Провести анализ содержимого НЖДМ с помощью утилиты mc и убедиться, что содержимое полученных файлов не соответствует содержимому файлов, созданных в п.12.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученных файлов не соответствует содержимому файлов, созданных в п.12.1 данной таблицы
12	Гарантированное удаление файла, имеющего символическую ссылку	
12.1	Выполнить следующие действия: <ul style="list-style-type: none"> • в каталоге /media/hdd создать файл test.txt и записать в него текст qwerty1234; • считать номера блоков для созданного файла с помощью команды: ./blknbr /media/hdd/test.txt; • считать содержимое блоков для созданного файла с помощью команды: dd if=/dev/sda3 of=test.txt bs=4096 count=1 skip=(номер блока файла); • создать символическую ссылку на файл с помощью команды: ln -sf /media/hdd/test.txt softlink; • убедиться в возможности просмотра файла по символической ссылке с помощью команды: cat ./softlink; • гарантированно удалить созданный файл с помощью команды: /opt/Blockhost/client/bhgupt /media/hdd/test.txt 	Создан файл test.txt. Считаны номера блоков для файла. Считано содержимое блоков для файла. Создана символическая ссылка к файлу. Удалили файл средствами gupr
12.2	Перейти в каталог /media/hdd и убедиться в отсутствии файла test.txt	Убедились в отсутствии файла test.txt
12.3	Считать содержимое блоков для созданного файла с помощью команды: dd if=/dev/sda3 of=test_new.txt bs=4096 count=1 skip=(номер блока файла)	Содержимое блоков файла считано (случайная последовательность)
12.4	Убедиться в недоступности файла test.txt по символической ссылке softlink с помощью команды: cat ./softlink	Убедились в недоступности файла test.txt по символической ссылке softlink
12.5	Провести анализ содержимого НЖДМ с помощью утилиты mc и убедиться, что содержимое полученного файла не соответствует содержимому файла созданному в п.13.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.13.1 данной таблицы
13	Гарантированное удаление файла, имеющего жесткую ссылку	
13.1	Выполнить следующие действия: <ul style="list-style-type: none"> • в каталоге /media/hdd создать файл test.txt и записать в него текст qwerty1234; 	Создан файл. Считаны номера блоков для файла. Считано содержимое блоков для файла.

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> считать номера блоков для созданного файла с помощью команды: <code>./blknmbr /media/hdd/test.txt</code>; считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test.txt bs=4096 count=1 skip=(номер блока файла)</code>; создать жесткую ссылку на файл с помощью команды: <code>ln /media/hdd/test.txt /media/hdd/hardlink</code>; убедиться в возможности просмотра файла по ссылке с помощью команды: <code>cat /media/hdd/hardlink</code>; гарантированно удалить созданный файл с помощью команды: <code>/opt/Blockhost/client/bhgupt --rm-hardlinks force /media/hdd/test.txt</code> 	Создана жесткая ссылка к файлу. Удалили файл средствами <code>gupt</code>
13.2	Перейти в каталог <code>/media/hdd</code> и убедиться в отсутствии файла <code>test.txt</code>	Убедились в отсутствии файла <code>test.txt</code>
13.3	Считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test_new.txt bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блоков файла считано (случайная последовательность)
13.4	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое полученного файла не соответствует содержимому файла созданному в п.14.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.14.1 данной таблицы
14	Гарантированное удаление файла с жесткой ссылкой без ее удаления	
14.1	Выполнить следующие действия: <ul style="list-style-type: none"> в каталоге <code>/media/hdd</code> создать файл <code>test.txt</code> и записать в него текст <code>qwerty1234</code>; считать номера блоков для созданного файла с помощью команды: <code>./blknmbr /media/hdd/test.txt</code>; считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test.txt bs=4096 count=1 skip=(номер блока файла)</code>; создать жесткую ссылку на файл с помощью команды: <code>ln /media/hdd/test.txt /media/hdd/hardlink</code>; убедиться в возможности просмотра файла по ссылке с помощью команды: <code>cat /media/hdd/hardlink</code> удалить созданный файл с помощью команды: <code>/opt/Blockhost/client/bhgupt --rm-hardlinks noforce /media/hdd/test.txt</code> 	Создан файл. Считаны номера блоков для файла. Считано содержимое блоков для файла. Создана жесткая ссылка к файлу. Удалили файл средствами <code>gupt</code>
14.2	Перейти в каталог <code>/media/hdd</code> и убедиться в отсутствии файла <code>test.txt</code>	Убедились в отсутствии файла <code>test.txt</code>
14.3	Убедиться в недоступности ссылке <code>hardlink</code> с помощью команды: <code>cat /media/hdd/hardlink</code>	Убедились в недоступности жесткой ссылки <code>hardlink</code>
14.4	Считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test_new.txt bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блоков файла считано
14.5	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое полученного файла не соответствует содержимому файла созданному в п.15.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.15.1 данной таблицы
15	Гарантированное удаление файла после изменения его атрибутов	
15.1	Выполнить следующие действия: <ul style="list-style-type: none"> в каталоге <code>/media/hdd</code> создать файл <code>test.txt</code> и записать в него текст <code>qwerty1234</code>; 	Создан файл <code>test.txt</code> . Считаны номера блоков для файла. Считано содержимое блоков для

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> считать номера блоков для созданного файла с помощью команды: <code>./blknmbr /media/hdd/test.txt;</code> считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test.txt bs=4096 count=1 skip=(номер блока файла);</code> изменить атрибуты созданного файл с помощью команды: <code>chattr +i -V /media/hdd/test.txt;</code> гарантированно удалить созданный файл с помощью команды: <code>/opt/Blockhost/client/bhgupt --clear-attributes /media/hdd/test.txt</code> 	файла. Изменили атрибуты файла. Удалили файл средствами <code>gupt</code>
15.2	Перейти в каталог <code>/media/hdd</code> и убедиться в отсутствии файла <code>test.txt</code>	Убедились в отсутствии файла <code>test.txt</code>
15.3	Считать содержимое блоков для созданного файла с помощью команды: <code>dd if=/dev/sda3 of=test_new.txt bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блоков файла считано (случайная последовательность)
15.4	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое полученного файла не соответствует содержимому файла созданному в п.16.1 данной таблицы	Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.16.1 данной таблицы
16	Гарантированное удаление каталога после изменения его атрибутов	
16.1	Выполнить следующие действия: <ul style="list-style-type: none"> в каталоге <code>/media/hdd</code> создать каталог <code>test</code> и внутри него создать несколько подкаталогов <code>test1</code> и <code>test2</code> соответственно с файлами <code>a.txt</code>, <code>b.txt</code> и <code>c.txt</code>, <code>d.txt</code> произвольного содержимого. Размер файлов должен быть менее 4096 байт; в каталоге <code>/media/hdd/test</code> создать файл <code>test.txt</code> размером менее 4096 байт с произвольным содержанием; считать номера блоков для всех созданных файлов с помощью команды: <code>./blknmbr /media/hdd/./<name_file>.txt;</code> изменить атрибуты созданного каталога <code>test</code> с помощью команды: <code>chattr +i -RV /media/hdd/test;</code> гарантированно удалить созданный каталог <code>/media/hdd/test</code> рекурсивно с помощью команды: <code>/opt/Blockhost/client/bhgupt -r --clear-attributes /media/hdd/test</code> 	Созданы каталоги и файлы. Изменили атрибуты каталога <code>test</code> . Удалили каталог <code>test</code> средствами <code>gupt</code>
16.2	Перейти в каталог <code>/media/hdd</code> и убедиться в отсутствии каталога <code>test</code>	Убедились в отсутствии каталога <code>test</code>
16.3	Считать содержимое блоков для каждого файла с помощью команды: <code>dd if=/dev/sda3 of=<name_file>.txt bs=4096 count=1 skip=(номер блока файла)</code>	Содержимое блоков файлов считано
16.4	Провести анализ содержимого НЖДМ с помощью утилиты <code>mc</code> и убедиться, что содержимое полученных файлов не соответствует содержимому файлов, созданных в п.17.1 данной таблицы	Провели анализ НЖДМ. Убедились, что содержимое полученных файлов не соответствует содержимому файлов, созданных в п.17.1 данной таблицы
17	Гарантированное удаление файлов на НЖМД с файловой системой NTFS	
17.1	Выполнить следующие действия: <ul style="list-style-type: none"> предварительно в ОС создать для проведения испытаний раздел НЖМД с файловой системой NTFS; примонтировать данный раздел в каталог <code>/media/hdd</code> в каталоге <code>/media/hdd</code> создать файл <code>test.txt</code> и записать в него текст <code>qwerty1234</code>; попытаться удалить созданный файл с помощью команды: <code>/opt/Blockhost/client/bhgupt /media/hdd/test.txt</code> 	Файл не удален
18	Гарантированное удаление файлов на НЖМД с файловой системой FAT	

№ п/п	Действия	Ожидаемый результат
18.1	Выполнить следующие действия: <ul style="list-style-type: none"> • предварительно в ОС создать для проведения испытаний раздел НЖМД с файловой системой FAT; • примонтировать данный раздел в каталог /media/hdd • в каталоге /media/hdd создать файл test.txt и записать в него текст qwerty1234; • попытаться удалить созданный файл с помощью команды: /opt/Blockhost/client/bhgupt /media/hdd/test.txt 	Файл удален
19	Гарантированное удаление файла с очисткой блоков журнала файловой системы	
19.1	Выполнить следующие действия: <ul style="list-style-type: none"> • примонтировать вновь раздел в каталог /media/hdd с помощью команды: mount -o data=journal /dev/sda3 /media/hdd/; • считать номера блоков для созданного файла с помощью команды: ./blknmbr /media/hdd/test.txt; • считать структуру журнала с помощью команды: jls /dev/sda3 > jls.txt; • с помощью утилиты mc открыть файл jls.txt и по номеру блока для созданного файла, полученного с помощью blknmbr, найти номер блока журнала; • выполнить команду: jcat /dev/sda3 номер блока журнала > jcat.txt, для поиска номера блоков, в которые записаны сигнатуры; • гарантированно удалить созданный файл с очисткой блоков журнала с помощью команды: /opt/Blockhost/client/bhgupt -j /media/hdd/test.txt 	Создан файл. Считаны номера блоков для файла. Считали структуру журнала. Удалили файл средствами gipt с очисткой блоков журнала
19.2	Перейти в каталог /media/hdd и убедиться в удалении файла test.txt	Убедились в удалении файла test.txt
19.3	Выполнить команду: jcat /dev/sda3 номер блока журнала > jcat_new.txt и с помощью утилиты mc убедиться, что сигнатура не найдена.	Сигнатура не найдена
19.4	Считать содержимое блоков для созданного файла с помощью команды: dd if=/dev/sda3 of=dev_sda3.txt bs=4096 count=1 skip=(номер блока файла)	Содержимое блоков файла считано
19.5	Провести анализ содержимого НЖМД с помощью утилиты mc и убедиться, что содержимое полученного файла не соответствует содержимому файла созданному в п.20.1 данной таблицы	Убедились, что содержимое полученного файла не соответствует содержимому файла созданному в п.20.1 данной таблицы
20	Просмотр событий аудита	
20.1	Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль администрирования СЗИ; • выбрать рабочую станцию РС18; • войти во вкладку «События»; • нажать кнопку «Поиск» 	Появление событий, фиксирующих успешные попытки гарантированного удаления по требованию, выполненные в настоящей таблице

Критерии оценки:

Проверка считается успешной, если обеспечивается возможность гарантированного удаления объектов по требованию пользователя без возможности его восстановления.

2.6.2 Проверка возможности очистки оперативной памяти

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 оперативной памяти путем обнуления ее содержимого.

Описание проверки:

Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя, через реестры, оперативную память, внешние запоминающие устройства, ресурсы файловой системы и иные общие для пользователей ресурсы информационной системы.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.30.

Таблица ПЗ.30 – Действия при проверке очистки оперативной памяти

№ п/п	Действия	Ожидаемый результат
1	Настройка механизма очистки оперативной памяти (Windows)	
1.1	От имени и с правами пользователя Администратор на PC1 в консоли управления СЗИ: <ul style="list-style-type: none"> • перейти в окно «Менеджер иерархий»; • выбрать сервер безопасности PC1; • перейти во вкладку «Политики»; • выбрать «Клиентские политики», «Политика клиента по умолчанию»; • в окне «Политика клиентов по умолчанию» выбрать раздел Windows и вкладку «Очистка оперативной памяти»; • установить тумблер «Механизм включён»; • установить флаг у параметра «Формировать события аудита»; • добавить через пиктограмму «+» Приложения для очистки оперативной памяти «notepad.exe», «winword.exe»; • сохранить сделанные изменения, нажав клавишу «Применить» 	Политика очистки оперативной памяти установлена
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 E: на PC2	Параметры установлены
2.2	Перезагрузить PC2, выполнить вход в систему от имени и с правами пользователя User1	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
2.3	Запустить приложение <i>C:\CheckMemoryCleaner.exe</i>	Открытие диалогового окна приложения
2.4	В окне приложения указать длину блока в байтах и путь к файлу <i>C:\test_message.txt</i> для записи фрагмента и нажать кнопку Генерировать . Указанный файл и дампы памяти обязательно необходимо сохранить на разных дисковых пространствах	Запись тестового фрагмента в оперативную память и в файл по указанному пути
2.5	Открыть диспетчер задач и найти в отображаемых процессах: 1) контролируемый процесс <i>CheckMemoryCleaner.exe</i> ; 2) процесс механизма очистки памяти <i>GIS.Client.MemoryCleaner.exe</i> ; 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	Создан файл <i>C:\test_message.txt</i> Изменение в диспетчере задач показателя загрузки центрального процессора, происходящего в результате работы механизма очистки памяти
2.6	Запустить приложение <i>NotMyFault.exe</i> для выполнения критической ошибки системы	Появление синего экрана. Перезагрузка операционной системы
2.7	Открыть файл <i>C:\test_message.txt</i>	Открытие файла
2.8	Запустить программное средство TERRIER 3.0 (WinHex)	Открытие диалогового окна программного средства TERRIER 3.0 (WinHex)
2.9	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск на диске <i>E:\</i> фрагмента тестового файла <i>C:\test_message.txt</i> (включая дампы памяти <i>E:\MEMORY.DMP</i>)	Последовательность не найдена
3	Просмотр событий аудита	
3.1	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: • запустить консоль управления СЗИ; • выбрать сервер СЗИ PC1, вкладку «События»; • нажать кнопку «Поиск»	Появление сообщений, фиксирующих события очистки памяти
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
5	Проверка механизма очистки оперативной памяти (РЕД ОС)	
6	Настройка механизма очистки оперативной памяти	
6.1	Выполнить вход в систему PC18 от имени и с правами пользователя Администратор	Загрузка рабочего стола
6.2	Открыть на рабочей станции терминал и выполнить следующие команды: • <code>cd ~</code> • создать рабочий каталог: <code>mkdir bhem_test</code> • установить пакеты: <code>sudo dnf upgrade && sudo dnf install git gcc kernel-devel</code> • скачать и собрать утилиту LiME • установить пакеты: <code>sudo dnf install git && sudo dnf install make && sudo dnf install kernel-headers && sudo dnf install gcc</code> • <code>cd ~</code> • <code>mkdir lime</code> • <code>cd lime</code> • <code>git clone https://github.com/504ensicsLabs/LiME.git</code> . (в конце должна присутствовать точка) • <code>cd lime/src</code>	Рабочие каталоги созданы. Скрипт подготовлен и скопирован

№ п/п	Действия	Ожидаемый результат						
	<ul style="list-style-type: none"> • make • скопировать собранный скрипт в каталог bhemem_test: cp lime-(текущая версия).ko ~/bhemem_test/lime.ko • подготовить скрипт dmp для снятия дампа со следующим содержанием: #!/usr/bin/env -S bash LIME_NAME=lime LIME=lime.ko DEST=tcp:4444 FORMAT=raw on_exit() { echo "Unloading \$LIME_NAME..." rmmod \$LIME_NAME } on_sigint() { echo "Interrupted!" if [[-f "\$DEST"]]; then echo "Deleting \$DEST..." rm "\$DEST" fi on_exit exit 3 } show() { echo "\$@" >&2 } warn() { show "WARNING: \$@" } die() { rc=\$1 shift echo -n "\$(tput smso)" >&2 show "ERROR: \$@" echo -n "\$(tput sgr0)" >&2 exit \$rc } [["\$EUID" -ne 0]] && die 1 "Run as root" [[-f \$LIME]] die 2 "\$LIME not found" echo "Destination: \$DEST" echo "Creating dump ..." insmod \$LIME "path=\$DEST format=\$FORMAT" rmmod \$LIME_NAME • скопировать скрипт dmp в каталог bhemem_test • скопировать тестовую утилиту bhemem_test в каталог bhemem_test 							
6.3	Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор , загрузить консоль управления СЗИ	Консоль управления СЗИ загружена						
6.4	В консоли управления СЗИ выполнить следующие действия: <ul style="list-style-type: none"> • открыть «Менеджер иерархий»; 	<table border="0"> <tr> <td>Политика</td> <td>очистки</td> </tr> <tr> <td>оперативной</td> <td>памяти</td> </tr> <tr> <td>установлена.</td> <td>Механизм</td> </tr> </table>	Политика	очистки	оперативной	памяти	установлена.	Механизм
Политика	очистки							
оперативной	памяти							
установлена.	Механизм							

№ п/п	Действия	Ожидаемый результат
	строки длиной более 30 символов в 2.txt	длиной более 30 символов и перенесли их в файл 2.txt
7.14	Выполнить скрипт <i>fgrep</i> "****ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ**** ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ**** ВНМЕМ****ВНМЕМ" 1.txt > r_header.txt	Выполнили поиск остаточной информации по шаблону
7.15	Убедиться в наличии остаточной информации в файле r_header.txt	Убедились в наличии остаточной информации до очистки ОП
7.16	Выполнить скрипт <i>fgrep</i> "****ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ**** ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ ****ВНМЕМ" 2.txt > r_str.txt	Выполнили поиск остаточной информации по шаблону после очистки ОП
7.17	Убедиться в отсутствии остаточной информации в файле r_str.txt	Убедились в отсутствии остаточной информации после очистки ОП
7.18	Повторить проверку механизма очистки памяти с п.7.1 по п.7.17 настоящей таблицы с параметром test (bhmем_test test) и поисковой строкой остаточной информации: "****ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ**** ВНМЕМ****ВНМЕМ****ВНМЕМ****ВНМЕМ ****ВНМЕМ-test"	Совпадение ожидаемых результатов
8	Просмотр событий аудита	
8.1	Войти на РС17 от имени пользователя и с правами Администратора и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) в окне «Менеджер иерархий» выбрать РС18 и затем раздел «События»; 3) установить следующие параметры фильтра: • Системы – Linux; • Уровни важности – Все уровни; • Типы событий: «Очистка оперативной памяти»; • По времени: За последние (Дней) – 1; • Выполнить «Поиск»; 4) убедиться, что в отчете отображаются все события очистки оперативной памяти	Убедились в наличии сообщений, фиксирующих события очистки оперативной памяти
9	Управление механизмом очистки оперативной памяти из локальной консоли управления Linux (РЕД ОС)	
9.1	Выполнить вход в систему на РС18 от имени и с правами пользователя Администратор	
9.2	Выполнить действия в соответствии с п.6.2 настоящей таблицы	Рабочие каталоги созданы. Скрипт подготовлен и скопирован
9.3	На рабочей станции РС18 открыть локальную консоль управления от имени и с правами Администратора (убедиться, что локальная консоль управления не управляется политикой сервера, при необходимости отключить механизм управления). Выполнить следующие действия: • перейти во вкладку «Очистка памяти»; • включить механизм очистки оперативной памяти, установив переключатель в положение «Механизм очистки памяти включен»; • в разделе «Контролируемые файлы/пакеты», добавить через пиктограмму «+»: bhmем_test; • сохранить внесенные изменения	Политика очистки оперативной памяти установлена. Механизм очистки оперативной памяти включен
9.4	Войти на РС8 от имени и с правами пользователя	Рабочий каталог создан.

№ п/п	Действия	Ожидаемый результат
	Администратор и выполнить действия в соответствии с п.6.5 настоящей таблицы	Файлы скачаны
10	Проверка механизма очистки памяти	
10.1	Выполнить действия в соответствии с п.7 настоящей таблицы	Совпадение результатов
11	Просмотр событий аудита	
11.1	На рабочей станции РС18, открыть локальную консоль управления от имени и с правами администратора. Выполнить следующие действия: <ul style="list-style-type: none"> • перейти во вкладку «События аудита»; • выбрать период: «День»; • обновить события; • убедиться, что в журнале событий аудита отображены события об очистке оперативной памяти 	Убедились в наличии сообщений, фиксирующих события очистки оперативной памяти

Критерии оценки:

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;
- АБ СЗИ может осуществлять управление и администрирование настройками безопасности для очистки остаточной информации;
- АБ СЗИ может управлять клиентской политикой списка процессов очистки ОП;
- средства СЗИ обеспечивают надежную регистрацию всех процедур очистки памяти.

2.6.3 Проверка возможности уничтожения информации на машинных носителях

Описание проверки:

Реализуется уничтожение (стирание) информации на машинных носителях, исключая возможность восстановления защищаемой информации.

Уничтожение информации реализуется многократной перезаписью МНИ специальными битовыми последовательностями и очисткой физического пространства накопителя.

- СЗИ обеспечивает регистрацию действий по удалению защищаемой информации
- СЗИ обеспечивает уничтожение (стирание) информации на машинных носителях, исключая возможность восстановления защищаемой информации полной многократной перезаписью машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства

накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.31.

Таблица ПЗ.31 – Действия при проверке очистки оперативной памяти

№ п/п	Действия	Ожидаемый результат
1	Настройка механизма очистки оперативной памяти	
1.1	Политика гарантированного удаления файлов установлена в проверке, изложенной в таблице ПЗ.29	
2	Формирование задачи «Гарантированного удаления по требованию» в подсистеме развертывания	
	Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль администрирования СЗИ; • выбрать вкладку «Развёртывание», «Задачи»; • отредактировать задачу «Установка Гарантированного удаления по требованию»; • в вкладке «Компьютеры» добавить РС8; • установить в «Планировщике» тип запуска «Вручную»; • перезагрузка системы «Перегружать компьютер как можно скорее»; • запустить задачу. 	Утилита установлена
3	Войти в ОС РС2 под именем и с правами пользователя Admin	Загрузка ОС. Появление рабочего стола
4	Создать текстовый файл с уникальным именем на USB-носителе <i>E:\TestDel_flash.txt</i> Набрать в указанном файле текст, содержащий следующую тестовую последовательность: Secret File 0xjqhWXPtHwAFhHfjXjGd5fAwRLAbB1XJIE4lsAUyd2tQ1d6gh&8*(hyrt%4#erj90 Сохранить файл <i>TestDel.txt</i> и <i>TestDel_flash.txt</i>	Создан файл <i>E:\TestDel_flash.txt</i> сохранены
5	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на USB-носителе	Тестовая последовательность найдена
6	На рабочем столе запустить утилиту «Гарантированное удаление по требованию» и выполнить следующие действия:	Файл удалён
	<ul style="list-style-type: none"> • через пиктограмму «+» добавить объект «Файл»; • выбрать устройство - USB-носитель; • выбрать файл <i>TestDel_flash.txt</i>; • нажать кнопку «Гарантировано удалить»; • в всплывающем окне подтвердить удаление 	

№ п/п	Действия	Ожидаемый результат
7	Выполнить с помощью программного средства TERRIER 3.0 (WinHex) поиск указанной тестовой последовательности на USB-носителе	Тестовая последовательность отсутствует

Критерии оценки:

Проверка считается успешной, если в области физического размещения удаленного файла не содержится информация, которая была в файле до его удаления.

2.7 Проверка маркировки документов

2.7.1 Проверка контроля печати и маркировки при выводе на печать документа, содержащего защищаемую информацию

Описание проверки:

СЗИ реализует поддержку и сохранение установленных меток безопасности, которые используются для контроля доступа субъектов доступа к объектам доступа.

- СЗИ реализует изменение атрибутов безопасности авторизованным пользователям;
- СЗИ реализует отображение атрибутов безопасности объектов доступа на экране монитора и при выводе информации на печать.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.32.

Таблица ПЗ.32 – 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 РС2 от имени и с правами пользователя Admin . Создать документы с произвольным содержимым: C:\1\print1.docx, C:\2\print2.docx	Создание документов с указанными именами
1.2	От имени и с правами пользователя Администратор на РС1 в консоли администрирования СЗИ:	
	<ul style="list-style-type: none"> • перейти в окно «Менеджер иерархий»; • в окне «менеджер иерархий» выбрать РС2; • перейти в вкладку «Настройки»; • выбрать «Контроль печати»; 	Настройки контроля печати установлены

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> • установить тумблер «Механизм включён»; • установить флаги для параметров «Выполнять аудит успешной печати из процессов, добавленных в список», «Выполнять аудит отказа печати из процессов, не добавленных в список»; • установить флаг «Шаблоны» для всех процессов; • сохранить сделанные изменения 	
1.3	<ul style="list-style-type: none"> • нажать кнопку «Настроить шаблон печати»; • в окне «Редактирование шаблона печати» выбрать все маркеры, отметив флажками соответствующие поля и ввести необходимые описания; • сохранить сделанные изменения. 	<p>Отображение окна «Редактирование шаблона печати».</p> <p>Отображение произведенных настроек</p>
1.4	<ul style="list-style-type: none"> • перейти в вкладку «Мандатный доступ»; • установить тумблер «Механизм включен»; • каталогу с файлом print1.docx присвоить иерархическую мандатную метку 1; • каталогу с файлом print2.docx – присвоить иерархическую мандатную метку 2; • установить флаги «Аудит»; • сохранить сделанные изменения. 	<p>Успешное сопоставление иерархических мандатных меток каталогам</p>
1.5	<ul style="list-style-type: none"> • в вкладке «Мандатный доступ» выбрать меню «Разделяемые файлы» добавить следующие файлы: <ul style="list-style-type: none"> - текстовый редактор Winword (C:\Program Files\Microsoft Office\Office14\Winword.exe); - приложение Wordicon.exe (C:\Program Files\Microsoft Office\Office14\Wordicon.exe); - C:\Blockhost\PrintControl\BlockHost.dot; - C:\Users\user1\AppData\Roaming\Microsoft\Шаблоны\Normal.dotm - C:\Users\user2\AppData\Roaming\Microsoft\Шаблоны\Normal.dotm 	<p>Отображение произведенных настроек</p>
2	Вывод документов на печать	
2.1	Вход в ОС PC2 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 <i>print1.docx</i> и отправить документ на печать	<p>Документ доступен для записи, чтения и печати.</p> <p>В верхнем и нижнем колонтитулах печатного листа отражены данные, указанные при настройке шаблона печати пользователя User1</p>
2.4	Запустить приложение Winword.exe и попытаться открыть файл <i>print2.docx</i> для последующей печати	Невозможность открытия файла print2.doc
2.5	Вход в ОС PC2 от имени и с правами пользователя User1 и мандатной меткой 2	Загрузка рабочего стола
2.6	Открыть с помощью приложения Winword.exe документ	Документ доступен для чтения.

№ п/п	Действия	Ожидаемый результат
	<i>print1.doc</i> и отправить документ на печать	Запрет печати документа
2.7	Запустить приложение Winword.exe и попытаться открыть файл <i>print2.doc</i> для последующей печати	Документ доступен для чтения и печати. В верхнем и нижнем колонтитулах печатного листа отражены данные, указанные при настройке шаблона печати пользователя User1
2.8	От имени и с правами пользователя Администратор на РС1 в консоли администрирования СЗИ: <ul style="list-style-type: none"> • перейти в окно «Менеджер иерархий»; • в окне «менеджер иерархий» выбрать РС2; • перейти в вкладку «Настройки»; • выбрать «Контроль печати»; • удалить из списка «Все процессы» с правом на печать • сохранить сделанные изменения. 	Настройки контроля печати установлены
2.9	Вход в ОС РС2 от имени и с правами пользователя User2 и мандатной меткой 1	Загрузка рабочего стола
2.1 0	Включить все макросы в настройках MS Office в пункте меню Файл → Параметры → Центр управления безопасностью → Параметры центра управления безопасностью → Параметры макросов	Успешное включение макросов
2.1 1	Запустить приложение Winword.exe и попытаться открыть файл <i>print2.doc</i> для последующей печати	Невозможность открытия файла <i>print2.doc</i>
2.1 2	Вход в ОС РС2 от имени и с правами пользователя User2 и мандатной меткой 2	Загрузка рабочего стола
2.1 3	Запустить приложение Winword.exe и попытаться открыть файл <i>print2.doc</i> для последующей печати	Документ доступен для чтения. Запрет печати документа
3	Просмотр событий аудита	
3.1	Запустить консоль «Системы развертывания и аудита» В окне выбрать «Мониторинг» выбрать РС2, нажать кнопку Выполнить запрос	Отображение сообщений, фиксирующих успешные и неудачные попытки вывода информации на печать
4	Выполнить указанные в пунктах 1 – 3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Требования по контролю печати и 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.

2.8 Проверка защиты ввода и вывода информации на отчуждаемый физический носитель

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

Описание проверки:

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

При вводе с «помеченного» устройства (вывода на «помеченное» устройство) СЗИ обеспечивает соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

Изменения в назначении и разметке устройств и должны осуществляются только под контролем СЗИ.

Выполняемые действия:

Проверка выполняется на основе действий, выполняемых в п. 2.4.1. Действия выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.33.

Таблица ПЗ.33 – 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	Подключить к РС8 USB-носитель (Flash drive 1)	Определение подключенного к РС8 USB-носителя средствами ОС
2	Войти на РС1 от имени и справами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС8;	В окне настройки мандатного доступа подключенный USB-носитель отражается в «Устройствах хранения данных»

№ п/п	Действия	Ожидаемый результат
	3) перейти на вкладку «Настройки»; 4) выбрать вкладку «Мандатный доступ»; 5) перейти на вкладку «Устройства»; 6) добавить USB-носитель Flash drive 1; 7) установить флаг на «Аудит»	
3	Назначить USB-носителю Flash drive 1 мандатную метку 4 «Секретно»	Присвоение объекту доступа Flash drive 1 иерархической мандатной метки 4
4	Нажать кнопку «Применить» для сохранения выполненных изменения	Сохранение настроек
5	Перейти в вкладку «События» РС8 и нажать кнопку «Поиск»	Появление сообщений, фиксирующих изменение настроек
6	Восстановить начальные настройки	Настройки СЗИ восстановлены

Критерии оценки:

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»).

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

Описание проверки:

В качестве подключаемых носителей рассматриваются внешние устройства хранения данных, подключаемые по USB-интерфейсу: съемные USB-накопители (флеш-накопители) или внешние съемные жесткие диски.

Все объекты относятся к неиерархической категории «Документы общего пользования».

В СЗИ предусмотрен ввод-вывод информации на МНИ для субъекта только в случае, если значение иерархической метки в классификационном уровне субъекта меньше или равно значению иерархической метки объекта с неиерархической категорией «Документы общего пользования».

Вывод информации на МНИ должен быть невозможен для субъекта в случае, если значение иерархической метки в его классификационном уровне выше значения иерархической метки объекта, вне зависимости от назначенной МНИ иерархической метки.

Выполняемые действия:

Субъектами доступа выступают локальные и доменные пользователи с назначенными иерархическими метками, а также доменный пользователь User4_AD с мандатной меткой назначаемой по умолчанию.

Объектами доступа являются каталоги на ЖМД компьютера, с вложенными в них файлами и подключенные USB-носители. Каталог C:\Test_label и USB-носителю Flash Drive4 принудительно мандатные иерархические метки не назначаются.

СЗИ идентифицирует МНИ по VID, PID-кодам и серийному номеру.

В процессе проверки субъекты доступа будут пытаться осуществлять попытки доступа к каталогам и копировать их на USB-носители.

Схема проверки представлена на рисунке П3.8.

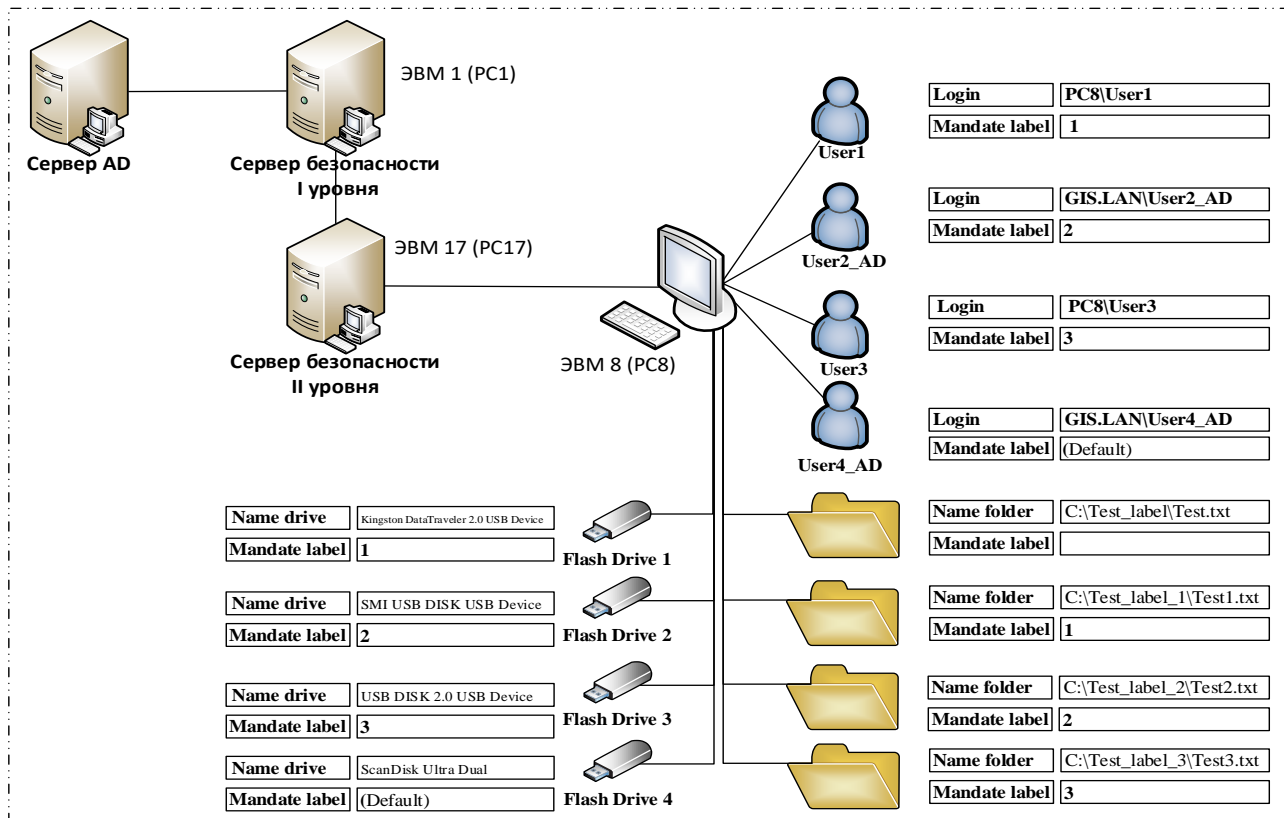


Рисунок П3.8 – Схема проверки

Иерархические метки для субъектов и объектов доступа назначаются в соответствии с таблицей Таблица П3.34.

Таблица ПЗ.34 – Матрица доступа к МНИ

СУБЪЕКТЫ		ОБЪЕКТЫ						
Имя носителя	Мандатная метка	МНИ (МНИ)				Файловые объекты		
		Flash Drive 1	Flash Drive 2	Flash Drive 3	Flash Drive 4	Атрибуты	Имя каталога и файла	Мандатная метка
		1	2	3	(Default)			
ID		1	RW	-	-	RW		
User1	1 2	RW	-	-	RW	RW	C:\Test_label\Test.txt	
		-	-	-	-	RW	C:\Test_label_1\Test1.txt	1
		-	-	-	-	-	C:\Test_label_2\Test2.txt	2
User2_AD	2 3	R	-	-	R	R	C:\Test_label\Test.txt	
		-	RW	-	-	R	C:\Test_label_1\Test1.txt	1
		-	-	-	-	RW	C:\Test_label_2\Test2.txt	2
User3	3 (Default)	R	-	-	R	R	C:\Test_label\Test.txt	
		-	R	-	-	R	C:\Test_label_1\Test1.txt	1
		-	-	RW	-	R	C:\Test_label_2\Test2.txt	2
User4_AD	(Default)	RW	-	-	RW	RW	C:\Test_label_3\Test3.txt	3
		-	-	-	-	RW	C:\Test_label_1\Test1.txt	1
		-	-	-	-	-	C:\Test_label_2\Test2.txt	2
							C:\Test_label_3\Test3.txt	3

Подробные действия, выполняемые при проверке, приведены в таблице ПЗ.35.

Таблица ПЗ.35 – Действия, выполняемые при проверке принципа сопоставления классификационных меток каждого субъекта и каждого объекта

№ п/п	Действия	Ожидаемый результат
1	Войти в ОС PC8 от имени и с правами пользователя Admin	Загрузка рабочего стола
2	Создание объектов файловой системы	
2.1	Создать каталоги с вложенными файлами: C:\Test_label\Test.txt C:\Test_label_1\Test1.txt C:\Test_label_2\Test2.txt C:\Test_label_3\Test3.txt	Созданы каталоги с вложенными файлами
3	Определение иерархического классификационного уровня мандатных меток для субъектов доступа	
3.1.	Войти на PC17 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать PC8; 3) перейти на вкладку «Настройки», «Мандатный доступ», «Пользователи»; 4) включить тумблер «Механизм включен»; 5) установить уровень доступа согласно ПЗ.34, для	Мандатные метки для субъектов доступа установлены

№ п/п	Действия	Ожидаемый результат
	пользователей: <ul style="list-style-type: none"> • User1 • User2_AD • User3 6) Применить сделанные изменения	
4	Определение иерархического классификационного уровня мандатных меток для объектов доступа	
4.1	1) выбрать PC8 и перейти по пути «Настройки», «Мандатный доступ», «Каталоги»; 2) установить уровень доступа согласно ПЗ.34, для каталогов: <ul style="list-style-type: none"> • C:\Test_label_1 • C:\Test_label_2 • C:\Test_label_3 3) Сохранить сделанные изменения	Мандатные метки для каталогов установлены
4.2	4) выбрать PC8 и перейти по пути «Настройки», «Мандатный доступ», «Устройства»; 5) установить уровень доступа согласно ПЗ.34, для USB-устройств: <ul style="list-style-type: none"> • Flash drive1 • Flash drive2 • Flash drive3 6) Сохранить сделанные изменения	Мандатные метки для USB - устройств установлены
5	Проверка осуществления санкционированных и несанкционированных попыток доступа к объектам доступа	
5.1	Выполнить вход в систему от имени и с правами пользователя User1 со значением мандатной метки 1	
5.1.1	Операции с файлом Test.txt	
	Чтение C:\Test_Label\Test.txt	Успешно
	Изменение C:\Test_Label\Test.txt	Успешно
	Копирование C:\Test_Label\Test.txt копирование на Flash Drive1	Успешно
	Копирование C:\Test_Label\Test.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование C:\Test_Label\Test.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование C:\Test_Label\Test.txt копирование на Flash Drive4	Успешно
5.1.2	Операции с файлом Test1.txt	
	Чтение C:\Test_Label_1\Test1.txt	Успешно
	Изменение C:\Test_Label_1\Test1.txt	Успешно
	Копирование C:\Test_Label_1\Test1.txt копирование на Flash Drive1	Успешно
	Копирование C:\Test_Label_1\Test1.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование C:\Test_Label_1\Test1.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование C:\Test_Label_1\Test1.txt копирование на Flash Drive4	Успешно

№ п/п	Действия		Ожидаемый результат
5.1.3	Операции с файлом Test2.txt		
	Чтение	C:\Test_Label_2\Test2.txt	Отказ в доступе
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
5.1.4	Операции с файлом Test3.txt		
	Чтение	C:\Test_Label_3\Test3.txt	Отказ в доступе
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
5.1.5	Завершить сеанс пользователя User1.		Появление приглашения для входа в систему
	5.2 Выполнить вход в систему от имени и с правами пользователя User2_AD со значением мандатной метки 2		
5.2.1	Операции с файлом Test.txt		
	Чтение	C:\Test_Label\Test.txt	Успешно
	Изменение	C:\Test_Label\Test.txt	Неуспешно
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive1	Неуспешно
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
5.2.2	Операции с файлом Test1.txt		
	Чтение	C:\Test_Label_1\Test1.txt	Успешно
	Изменение	C:\Test_Label_1\Test1.txt	Неуспешно
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive1	Неуспешно
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
5.2.3	Операции с файлом Test2.txt		
	Чтение	C:\Test_Label_2\Test2.txt	Успешно
	Изменение	C:\Test_Label_2\Test2.txt	Успешно

№ п/п	Действия		Ожидаемый результат
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive1 (Kingston DataTraveler 2.0 USB Device)	Неуспешно (Отказ в доступе)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive2	Успешно
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive4	Отказ в доступе (устройство недоступно)
5.2.4	Операции с файлом Test3.txt		
	Чтение	C:\Test_Label_3\Test3.txt	Отказ в доступе
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive4	Отказ в доступе (устройство недоступно)
5.2.5	Завершить сеанс пользователя User2.		Появление приглашения для входа в систему
5.3	Выполнить вход в систему от имени и с правами пользователя User3 co значением мандатной метки 3		
5.3.1	Операции с файлом Test.txt		
	Чтение	C:\Test_Label\Test.txt	Успешно
	Изменение	C:\Test_Label\Test.txt	Неуспешно
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive1	Отказ в доступе
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive2	Отказ в доступе
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive3	Отказ в доступе
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive4	Отказ в доступе
5.3.2	Операции с файлом Test1.txt		
	Чтение	C:\Test_Label_1\Test1.txt	Успешно
	Изменение	C:\Test_Label_1\Test1.txt	Неуспешно
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive1	Отказ в доступе
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive2	Отказ в доступе
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive3	Отказ в доступе
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive4	Отказ в доступе
5.3.3	Операции с файлом Test2.txt		
	Чтение	C:\Test_Label_2\Test2.txt	Успешно
	Изменение	C:\Test_Label_2\Test2.txt	Неуспешно
	Копирование	C:\Test_Label_2\Test2.txt копирование на	Отказ в доступе

№ п/п	Действия		Ожидаемый результат
		Flash Drive1	
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive2	Отказ в доступе
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive3	Отказ в доступе
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive4	Отказ в доступе
5.3.4	Операции с файлом Test3.txt		
	Чтение	C:\Test_Label_3\Test3.txt	Успешно
	Изменение	C:\Test_Label_3\Test3.txt	Успешно
	Копирование	C:\Test_Label\Test3.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive3	Успешно
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive4	Отказ в доступе
5.3.5	Завершить сеанс пользователя User3.		Появление приглашения для входа в систему
5.4	Выполнить вход в систему от имени и с правами пользователя User4_AD без значения мандатной метки, стандартным способом аутентификации		
5.4.1	Операции с файлом Test.txt		
	Чтение	C:\Test_Label\Test.txt	Успешно
	Изменение	C:\Test_Label\Test.txt	Успешно
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label\Test.txt копирование на Flash Drive4	Успешно
5.4.2	Операции с файлом Test1.txt		
	Чтение	C:\Test_Label_1\Test1.txt	Успешно
	Изменение	C:\Test_Label_1\Test1.txt	Успешно
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_1\Test1.txt копирование на Flash Drive4	Успешно
5.4.3	Операции с файлом Test2.txt		
	Чтение	C:\Test_Label_2\Test2.txt	Отказ в доступе
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)

№ п/п	Действия		Ожидаемый результат
		Flash Drive2	недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_2\Test2.txt копирование на Flash Drive4	Отказ в доступе (устройство недоступно)
5.4.4	Операции с файлом Test3.txt		
	Чтение	C:\Test_Label_3\Test3.txt	Отказ в доступе
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive1	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive2	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive3	Отказ в доступе (устройство недоступно)
	Копирование	C:\Test_Label_3\Test3.txt копирование на Flash Drive4	Отказ в доступе (устройство недоступно)
5.4.5	Завершить сеанс пользователя User4_AD.		Появление приглашения для входа в систему
6	Просмотр событий аудита		
6.1	Войти в ОС PC1 от имени и с правами пользователя Admin		Загрузка рабочего стола
6.2	Запустить консоль «Системы развертывания и аудита». В окне выбрать « Мониторинг » выбрать PC17. Нажать кнопку « Выполнить запрос »		Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
6.3	Выполнить указанные в пунктах 1 – 6 действия для рабочих станций ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows		Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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

- обеспечивается вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных при совпадении маркировки;
- средства СЗИ обеспечивают надежную регистрацию всех событий, связанных с попытками получения доступа к контролируемым МНИ.

2.8.3 Проверка возможности изменения в назначении и разметке устройств только под контролем СЗИ от НСД «Блокхост-Сеть 4»

Описание проверки:

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

При вводе с «помеченного» устройства (вывода на «помеченное» устройство) СЗИ обеспечивает соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

Изменения в назначении и разметке устройств и каналов осуществляются только под контролем СЗИ.

Выполняемые действия:

Проверка выполняется на основании действий, выполняемых в п. 2.8.2. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.36.

Таблица ПЗ.36 – Действия при проверке возможности изменения в назначении и разметке устройств только под контролем СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия	Ожидаемый результат
1	Включить и загрузить ОС на РС8 от имени и с правами пользователя Администратор	ОС на РС8 загружена
2	Подключить к РС8 USB-накопитель	Идентификация накопителя средствами ОС
3	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС8 и перейти на вкладку «Настройки», «Мандатный доступ»; 3) включить механизм мандатного доступа, установив тумблер в положение «Механизм включен»; 4) перейти на вкладку «Устройства»; 5) нажать на кнопку «+Добавить» и добавить подключенное к РС8 устройство USB – устройство; 6) назначить уровень доступа 4 для USB – устройства; 7) сохранить сделанные изменения	Метка успешно присвоена
4	Войти на сервер безопасности II уровня РС17 от имени и с правами доменного пользователя User2_AD	Успешно вошли на сервер РС17
5	Попытаться запустить консоль управления СЗИ	Отказ в доступе «У пользователя недостаточно прав».
6	Выполнить выход из системы пользователя User2_AD	Выход выполнен
7	На РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) перейти в вкладку «События»; 3) нажать кнопку «Поиск»	Появление сообщений, фиксирующих выполненные пользователем Администратор назначения мандатных меток и попытки пользователя User2_AD войти на сервер безопасности РС17

Критерии оценки:

Испытания считаются успешными, если изменения в назначении мандатных меток устройствам и каналам осуществляется только под контролем СЗИ от НСД «Блокхост-Сеть 4».

2.9 Проверка сопоставления пользователя с устройством**2.9.1 Проверка возможности обеспечить вывод информации на запрошенное пользователем устройство****Описание проверки:**

СЗИ реализует контроль использования (запрет или разрешение) интерфейсов ввода (вывода) пользователям.

СЗИ реализует:

- регистрацию событий использования интерфейсов ввода (вывода);
- программное отключение запрещенных к использованию интерфейсов ввода (вывода).

СЗИ реализует контроль ввода (вывода) информации на машинные носители:

- запрещает действия по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации;
- регистрирует действия пользователей и событий по вводу (выводу) информации на машинные носители информации.

СЗИ реализует контроль подключения машинных носителей информации:

- позволяет определить типы носителей информации, подключение которых к информационной системе разрешено;
- позволяет определить категории пользователей, которым предоставлены полномочия по подключению носителей к информационной системе;
- запрещает подключения носителей информации, подключение которых к информационной системе не разрешено;
- регистрирует действия пользователей и событий по подключению к информационной системе носителей.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.37.

Таблица ПЗ.37 – Действия при проверке возможности обеспечить вывод информации на запрошенное пользователем устройство

№ п/п	Действия	Ожидаемый результат
1	Формирование разрешительной политики контроля устройств и интерфейсов	
1.1	На рабочих станциях ЭВМ1 – ЭВМ5 зарегистрировать учетную запись локального пользователя User1. На контроллере домена зарегистрировать учетную запись доменного пользователя GIS.LAN \User1_AD	Пользователи зарегистрированы
1.2	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»; 3) перейти на вкладку Windows, «Контроль устройств»; 4) включить механизм контроля устройств; 5) установить флаги для правил разрешения доступа для всех устройств и интерфейсов; 6) добавить в список следующих пользователей для устройств хранения данных и переносных устройств с разрешением на чтение и запись: <ul style="list-style-type: none"> • локального пользователя PC2\User1; • доменного пользователя GIS.LAN\User1_AD; 7) на вкладках «Аудит» для USB устройств, установить флаги «Выполнять аудит событий включения/выключения устройств», «Выполнять аудит успешных операций доступа к устройствам», «Выполнять аудит отказов на доступ к устройствам»; 8) сохранить внесенные изменения, нажав кнопку «Применить» 	Политика контроля устройств и интерфейсов сформирована
2	Проверка доступа локального пользователя PC2 \User1 к устройствам и интерфейсам	
2.1.	Войти на PC2 от имени и с правами пользователя User1 и выполнить следующие действия:	
	• Чтение файла с CD-ROM	Успешно
	• Печать на принтере (подключен к LPT-порту)	Успешно
	• Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	• Чтение/запись информации на подключенное к USB-порту устройство	Успешно
3	Проверка доступа доменного пользователя User1_AD к устройствам и интерфейсам	
3.1.	Войти на PC2 от имени и с правами пользователя User1_AD и выполнить следующие действия:	
	• Чтение файла с CD-ROM	Успешно
	• Печать на принтере (подключен к LPT-порту)	Успешно
	• Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	• Чтение/запись информации на подключенное к USB-порту устройство	Успешно
4	Формирование запретительной политики контроля устройств и интерфейсов	

№ п/п	Действия	Ожидаемый результат
4.1	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»; 3) выбрать раздел Windows, «Контроль устройств» и далее вкладки USB-устройства, «Устройства хранения данных»; 4) отключить флаг «Доступ разрешен»; 5) выбрать раздел Windows, «Контроль устройств» и далее вкладки USB-устройства, «Переносные устройства»; 6) отключить флаг «Доступ разрешен»; 7) выбрать вкладку «Другие устройства» и снять флаг «Доступ разрешен» с: <ul style="list-style-type: none"> • CD/DVD-приводы; • COM; • LPT. 8) сохранить внесенные изменения , нажав кнопку «Применить» 	<p>Запретительная политика контроля устройств и интерфейсов сформирована</p>
5	<p>Проверка доступа локального пользователя PC2\User1 к устройствам и интерфейсам при запретительной политике</p>	
	<p>Войти на PC2 от имени и с правами пользователя User1 и выполнить следующие действия:</p>	
5.1	Чтение файла с CD-ROM	Неудачно (устройство отсутствует в списке)
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно
6	<p>Проверка доступа доменного пользователя User1_AD к устройствам и интерфейсам</p>	
	<p>Войти на PC2 от имени и с правами пользователя User1_AD и выполнить следующие действия:</p>	
6.1	Чтение файла с CD-ROM	Неудачно (устройство отсутствует в списке)
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно
7	<p>Просмотр событий аудита</p>	
7.1	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, и перейти на вкладку «События»; 3) установить фильтр по типу событий «Контроль устройств»; 4) нажать кнопку «Поиск»; 5) убедиться, что присутствуют события о попытках доступа к контролируемым устройствам и интерфейсам 	<p>Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам</p>

№ п/п	Действия	Ожидаемый результат
8	Выполнить указанные в пунктах 1.2 – 7 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
Linux (РЕД ОС)		
9	Включить и загрузить ОС на PC18 от имени Администратора. Зарегистрировать учетную запись локального пользователя User1	Пользователь зарегистрирован
10	Войти на PC1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»; 3) перейти на вкладку Linux, «Контроль устройств»; 4) включить механизм контроля устройств; 5) установить флаги для правил разрешения доступа для всех устройств и интерфейсов; 6) добавить в список следующих пользователей для устройств хранения данных и переносных устройств с разрешением на чтение, запись и исполнение: <ul style="list-style-type: none"> • локального пользователя PC18\User1; • доменного пользователя GIS.LAN\User1_AD; 7) на вкладках «Аудит» для USB устройств, установить флаги «Выполнять аудит событий включения/выключения устройств», «Выполнять аудит успешных операций доступа к устройствам», «Выполнять аудит отказов на доступ к устройствам»; 8) сохранить внесенные изменения	Политика контроля устройств и интерфейсов сформирована
11	Проверка доступа локального пользователя PC18\User1 к устройствам и интерфейсам	
11.1	Войти на PC18 от имени и с правами пользователя User1 и выполнить следующие действия:	
	Чтение файла с CD-ROM	Успешно
	Печать на принтере (подключен к LPT-порту)	Успешно
	Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	Чтение/запись информации на подключенное к USB-порту устройство	Успешно
12	Проверка доступа доменного пользователя User1_AD к устройствам и интерфейсам	
12.1	Войти на PC18 от имени и с правами пользователя User1_AD и выполнить следующие действия:	
	• Чтение файла с CD-ROM	Успешно
	• Печать на принтере (подключен к LPT-порту)	Успешно
	• Чтение/запись информации на подключенное к COM-порту устройство	Успешно
	• Чтение/запись информации на подключенное к USB-порту устройство	Успешно
13	Формирование запретительной политики контроля устройств и интерфейсов	

№ п/п	Действия	Ожидаемый результат
13.1	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»; 3) выбрать раздел Linux, «Контроль устройств» и далее вкладки USB-устройства, «Устройства хранения данных»; 4) отключить флаг «Доступ разрешен»; 5) перейти на вкладку «Переносные устройства»; 6) отключить флаг «Доступ разрешен»; 7) выбрать вкладку «Другие устройства» и снять флаг «Доступ разрешен» с: <ul style="list-style-type: none"> • CD/DVD-приводы; • COM; • LPT. 8) сохранить внесенные изменения 	<p>Запретительная политика контроля устройств и интерфейсов сформирована</p>
14	<p>Проверка доступа локального пользователя PC18\User1 к устройствам и интерфейсам при запретительной политике</p>	
14.1	<p>Войти на PC18 от имени и с правами пользователя User1 и выполнить следующие действия:</p>	
	Чтение файла с CD-ROM	Неудачно (устройство отсутствует в списке)
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно
15	<p>Проверка доступа доменного пользователя User1_AD к устройствам и интерфейсам</p>	
	<p>Войти на PC18 от имени и с правами пользователя User1_AD и выполнить следующие действия:</p>	
15.1	Чтение файла с CD-ROM	Неудачно (устройство отсутствует в списке)
	Печать на принтере (подключен к LPT-порту)	Неудачно
	Чтение/запись информации на подключенное к COM-порту устройство	Неудачно
	Чтение/запись информации на подключенное к USB-порту устройство	Неудачно
16	<p>Просмотр событий аудита</p>	
16.1	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC17 и перейти на вкладку «События»; 3) установить фильтр по типу событий «Контроль устройств»; 4) нажать кнопку «Поиск»; 5) убедиться, что присутствуют события о попытках доступа к контролируемым устройствам и интерфейсам 	<p>Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым устройствам и интерфейсам</p>

Критерии оценки:

Проверка считается успешной, если пользователю обеспечен ввод/вывод информации:

- на произвольно используемое устройство;
- на идентифицированное устройство.

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

Описание проверки:

СЗИ реализует контроль использования (запрет или разрешение) интерфейсов ввода (вывода) пользователям.

СЗИ реализует:

- регистрацию событий использования интерфейсов ввода (вывода);
- программное отключение запрещенных к использованию интерфейсов ввода (вывода).

Выполняемые действия:

Проверка выполняется согласно и на основании действий, выполненных в п. 2.9.1. В данном пункте сформирована политика запрещения доступа всех пользователей к «Устройствам хранения данных». Для проведения проверки в качестве объектов доступа используются 4 USB Flash drive, а в качестве субъектов доступа, локальный и доменные пользователи.

Для доступа пользователей формируется политика «доверенного списка» устройств и ассоциированного с ним списка санкционированных пользователей, с явными разрешениями и запретами приведенных в таблице ПЗ.38. При этом СЗИ должно идентифицировать каждое из устройств.

Четвертый носитель не будет входить в список доверенных устройств.

Таблица ПЗ.38 – Матрица доступа к устройствам

№	Имя	User1		User1_AD		User2_AD	
1	Flash drive 1	Доверенное устройство		Доверенное устройство			
		Чтение	Запись	Чтение	Запись	Чтение	Запись
		+		+			
		+			-		
2	Flash drive 2	Доверенное устройство		Доверенное устройство			

№	Имя	User1		User1_AD		User2_AD	
		Чтение	Запись	Чтение	Запись	Чтение	Запись
3	Flash drive 3	Чтение	Запись	Чтение	Запись	Чтение	Запись
		+		+			
			-	+			
				Доверенное устройство		Доверенное устройство	
4	Flash drive 4	Чтение	Запись	Чтение	Запись	Чтение	Запись
					-	+	
					-	+	

Подробный порядок действий при проверке и ожидаемые результаты приведены в таблице ПЗ.39.

Таблица ПЗ.39 – Действия при проверке механизма сопоставления пользователя с устройством, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству

№ п/п	Действия	Ожидаемый результат
1	Формирование разрешительной политики контроля устройств и интерфейсов	
1.1	На контроллере домена зарегистрировать доменных пользователей GIS.LAN\User1_AD и GIS.LAN\User2_AD. На рабочих станциях ЭВМ1 – ЭВМ5 Windows/Linux (ПЕД ОС) зарегистрировать локального пользователя User1	Пользователи зарегистрированы
1.2	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»; 3) выбрать раздел Windows и вкладку «Управление входом в ОС»; 4) перейти на вкладку «Список пользователей»; 5) добавить пользователей User1_AD, User2_AD и USER1 с разрешением «Аутентификации Windows»; 6) выбрать раздел Windows и вкладку «Контроль устройств»; 7) перейти на вкладку «Доверенный список»; 8) добавить устройства и установить политику согласно матрице доступа, представленной в таблице ПЗ.38, для следующих пользователей: • добавить локального пользователя PC2\User1 • добавить доменных пользователей GIS.LAN\User1_AD и GIS.LAN\User2_AD; 9) сохранить внесенные изменения	Политика контроля устройств и интерфейсов сформирована
1.3	Создать файлы C:\iotest1.txt с произвольным содержимым и read.txt	Создание файлов
1.4	Создать файл read.txt с произвольным содержанием и скопировать его на Flash drive 1, Flash drive 2, Flash drive 3	Файл создан и скопирован
2	Проверка доступа локального пользователя PC2\User1 к устройствам	

2.1.	Войти на PC2 от имени и с правами пользователя User1 и выполнить следующие действия:	
	• Скопировать файл C:\iotest1.txt на Flash drive 1	Успешно
	• Скопировать файл C:\iotest1.txt на Flash drive 2	Неуспешно. Ошибка
	• Открыть read.txt на Flash drive 2	Успешно
	• Скопировать файл C:\iotest1.txt на Flash drive 3	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл C:\iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе
3	Проверка доступа доменного пользователя User1_AD к устройствам	
3.1	Войти на PC2 от имени и с правами пользователя User1_AD и выполнить следующие действия:	
	• Скопировать файл C:\iotest1.txt на Flash drive 1	Неуспешно
	• Открыть read.txt на Flash drive 1	Успешно
	• Скопировать файл C:\iotest1.txt на Flash drive 2	Успешно
	• Открыть read.txt на Flash drive 2	Успешно
	• Скопировать файл C:\iotest1.txt на Flash drive 3	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл C:\iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе
4	Проверка доступа доменного пользователя User2_AD к устройствам	
4.1	Войти на PC2 от имени и с правами пользователя User2_AD и выполнить следующие действия:	
	• Скопировать файл C:\iotest1.txt на Flash drive 1	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл C:\iotest1.txt на Flash drive 2	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл C:\iotest1.txt на Flash drive 3	Успешно
	• Открыть read.txt на Flash drive 3	Успешно
	• Скопировать файл C:\iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе
5	Просмотр событий аудита	
5.1	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, вкладку «События»; 3) установить фильтр по категории «Контроль устройств»; 4) нажать кнопку «Поиск»; 5) убедиться в том, что присутствуют события о попытке доступа к контролируемым объектам	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам
6	Выполнить указанные в пунктах 1.2 – 5 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
Linux (РЕД ОС)		
7	Формирование разрешительной политики контроля устройств и интерфейсов	
7.1	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, «Политики», «Политика клиента по умолчанию»;	Политика контроля устройств и интерфейсов сформирована

	<p>3) выбрать раздел Linux и вкладку «Управление входом в ОС»;</p> <p>4) перейти на вкладку «Список пользователей»;</p> <p>5) добавить пользователей User1_AD, User2_AD и USER1 с разрешением «Аутентификации ОС»;</p> <p>6) выбрать раздел Linux и вкладку «Контроль устройств»;</p> <p>7) перейти на вкладку «Доверенный список»;</p> <p>8) добавить устройства и установить политику согласно матрице доступа, представленной в таблице ПЗ.38 для следующих пользователей:</p> <ul style="list-style-type: none"> • добавить локального пользователя PC18\User1 • добавить доменных пользователей GIS.LAN\User1_AD и GIS.LAN\User2_AD; <p>9) сохранить внесенные изменения</p>	
7.2	Создать файл iotest1.txt с произвольным содержимым	Создание файла
7.3	Создать файл read.txt с произвольным содержимым b скопировать его на Flash drive 1, Flash drive 2, Flash drive 3	Файл скопирован
8	Проверка доступа локального пользователя PC18\User1 к устройствам	
	Войти на PC18 от имени и с правами пользователя User1 и выполнить следующие действия:	
8.1.	• Скопировать файл iotest1.txt на Flash drive 1	Успешно
	• Скопировать файл iotest1.txt на Flash drive 2	Неуспешно. Ошибка
	• Открыть read.txt на Flash drive 2	Успешно
	• Скопировать файл iotest1.txt на Flash drive 3	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе
9	Проверка доступа доменного пользователя User1_AD к устройствам	
	Войти на PC18 от имени и с правами пользователя User1_AD и выполнить следующие действия:	
9.1	• Скопировать файл iotest1.txt на Flash drive 1	Неуспешно
	• Открыть read.txt на Flash drive 1	Успешно
	• Скопировать файл iotest1.txt на Flash drive 2	Успешно
	• Открыть read.txt на Flash drive 2	Успешно
	• Скопировать файл iotest1.txt на Flash drive 3	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе
10	Проверка доступа доменного пользователя User2_AD к устройствам	
	Войти на PC18 от имени и с правами пользователя User2_AD и выполнить следующие действия:	
10.1	• Скопировать файл iotest1.txt на Flash drive 1	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл iotest1.txt на Flash drive 2	Неуспешно. Ошибка. Отказано в доступе
	• Скопировать файл iotest1.txt на Flash drive 3	Успешно
	• Открыть read.txt на Flash drive 3	Успешно
	• Скопировать файл iotest1.txt на Flash drive 4	Неуспешно. Ошибка. Отказано в доступе

11	Просмотр событий аудита	
11.1	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, вкладку «События»; 3) установить фильтр по категории «Контроль устройств»; 4) нажать кнопку «Поиск»; 5) убедиться в том, что присутствуют события о попытке доступа к контролируемым объектам 	<p>Появление сообщений, фиксирующих произведенные попытки доступа к контролируемым объектам</p>

Критерии оценки:

Проверка считается успешной, если:

- СЗИ реализует формирование политики и передачу её на защищаемые компьютеры по иерархии серверов безопасности;
- политики могут переопределяться на подчиненных серверах безопасности, если нет запрета на переопределение на головном сервере;
- реализует сопоставление пользователя с устройством (МНИ) и установку разрешений к нему;
- средства СЗИ обеспечивают идентификацию USB-устройств (по серийному номеру);
- средства СЗИ позволяют задавать явные права на доступ для каждой пары «пользователь – устройство доступа» (формировать матрицу доступа к устройствам);
- СЗИ регистрирует события безопасности, связанные с контролем портов.

2.10 Проверка идентификации и аутентификации пользователей

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

Идентификация и аутентификация пользователя при его доступе на ПК в составе СЗИ предназначена для защиты от несанкционированного доступа к защищаемой информации на ПК незарегистрированных пользователей или пользователей не имеющих установленных прав доступа к защищаемой информации.

Механизм осуществляет проверку подлинности идентификатора субъекта – аутентификацию, и препятствует входу неидентифицированных пользователей или пользователей, чья подлинность при аутентификации не подтвердилась.

Идентификация и аутентификация пользователей осуществляются после

инициализации механизмов защиты СЗИ. При этом в СЗИ отключена возможность загрузки ОС в защищенном режиме для всех пользователей, за исключением администратора безопасности.

Предусмотрены следующие возможные виды входа пользователя в систему, описанные в таблице ПЗ.40.

Таблица ПЗ.40 – Возможные виды входа пользователя в систему

Аутентификация	Описание	Возможные виды входа	Комментарий
По токену: - с записанным паролем или безопасный вход по паролю (БВПП); - с сертификатом.	Аутентификация возможна только с использованием токена, назначенного пользователю с помощью подсистемы управления токенами СЗИ	<ul style="list-style-type: none"> • вход по сертификату на токене; • вход по паролю на токене. 	При входе пользователя СЗИ выполняет проверку принадлежности токена пользователю
По паролю	Аутентификация с помощью пароля, вводимого пользователем вручную	<ul style="list-style-type: none"> • вход по паролю, вводимому вручную. 	При входе пользователя СЗИ выполняет проверку введенного пароля с паролем пользователя, хранящимся в БД
Аутентификация Windows/Linux	Аутентификация пользователя, предполагающая полное доверие проверкам входа, выполняемым средствами ОС	любой возможный вид входа, поддерживаемый средствами ОС	При входе пользователя идентификационные данные пользователя проверяются средствами операционной системы, СЗИ только осуществляет проверку в своей базе наличия учетной записи пользователя, выполняющего вход в ОС

При аутентификации осуществляются следующие проверки позволяющие или запрещающие в конечном итоге вход пользователя в ОС:

- проверка не является ли пользователь встроенным администратором;
- проверка режима функционирования рабочей станции (включен/отключен «мягкий» режим работы) и проверка наличия лицензии у клиентской рабочей станции;
- проверка соответствия введенных аутентификационных данных требованиям сложности, установленным в политике аутентификации;
- проверка наличия учетной записи пользователя в списке клиентской политики в разделе «Управление входом в ОС»;
- при предъявлении токена выполняется проверка разрешен ли пользователю вход по токену, и в случае разрешения:
 - принадлежит ли токен пользователю;

- валиден ли токен.
- при предъявлении пользователем пароля выполняется:
 - проверка установки у пользователя типа аутентификации «Доверять аутентификации Windows/Linux»;
 - проверка разрешения у учетной записи пользователя входа по паролю и наличия пользователя в списке настроек в разделе «Проверка пароля в СЗИ» (в случае отсутствия доверия аутентификации Windows/Linux);
 - сверка введенного пароля с копией в локальной базе данных клиента СЗИ (в случае разрешенной аутентификации пользователя по паролю);
- при включенном механизме, ограничивающим вход на клиентскую рабочую станцию, выполняется проверка наличия учетной записи пользователя в списке раздела «Пользователи с разрешением на вход в ОС».

Подробная схема проверок при аутентификации пользователя приведена на рисунке ПЗ.9.

Если все проверки завершены успешно, пользователю разрешается вход в операционную систему.

Механизм аутентификации действует параллельно с политиками безопасности, действующими в домене (в ОС локальной рабочей станции), и параметрами безопасности драйверов аппаратных идентификаторов, используемых в качестве персональных идентификаторов пользователей. Таким образом, параметры идентификации пользователя, для его корректного входа в ОС, должны удовлетворять всем политикам, действующим на рабочей станции.

Описание проверки:

СЗИ реализует:

- идентификация и аутентификация пользователей, являющихся работниками оператора, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей;
- пользователи однозначно идентифицируются и аутентифицируются для всех видов доступа.
- обеспечивается многофакторная (двухфакторная) аутентификация для локального доступа с правами привилегированных учетных записей (администраторов);
- обеспечивается многофакторная (двухфакторная) аутентификация для локального доступа с правами непривилегированных учетных записей (пользователей).

Защита обратной связи при вводе аутентификационной информации путем исключения отображения для пользователя действительного значения аутентификационной информации с заменой вводимых символов пароля условным знаком «•».

СЗИ реализует ограничение количества неуспешных попыток входа и блокирование СВТ при их превышении.

СЗИ реализует блокирование ресурсов СВТ до полной загрузки компонентов СЗИ.

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству.

Управление средствами аутентификации, инициализация, блокирование средств аутентификации.

- изменение аутентификационной информации (средств аутентификации),

заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;

- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля:
 - сложность пароля, определяемая требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
 - количество измененных символов при создании новых паролей;
 - время действия пароля;
 - запрет использования заданного количества последних сохраненных паролей.
- блокирование (прекращение действия) средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля).

Механизм многофакторной аутентификации, основанный на пароле, должен обладать следующими характеристиками:

- длина пароля;
- количество неуспешных попыток аутентификации;
- блокирование программно-технического средства или учетной записи пользователя при превышении предела количества неуспешных попыток аутентификации.

Выполняемые действия:

Проверка состоит из ряда взаимосвязанных последовательных проверок.

2.10.1.1 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

Проверяемые требования:

Управление средствами аутентификации, инициализация, блокирование средств аутентификации:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;
- генерация и выдача начальной аутентификационной информации (начальных

значений средств аутентификации);

- установление характеристик пароля:
 - сложность пароля, определяемая требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
 - количество измененных символов при создании новых паролей;
 - время действия пароля;
 - запрет использования заданного количества последних сохраненных паролей.
- блокирование (прекращение действия) средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля).

Выполняемые действия:

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

Таблица ПЗ.41 – Проверка управления идентификаторами, в том числе, создание, присвоение, уничтожение идентификаторов

№ п/п	Действия	Ожидаемый результат
1	Присвоение токена доменному пользователю GIS.LAN\User2_AD	
1.1	Войти на PC1, сервер безопасности I уровня, от имени и с правами пользователя Администратор. Подключить к PC1 USB-токен	Загрузка рабочего стола
1.2	От имени и с правами Администратор загрузить консоль управления СЗИ и выполнить следующие действия: <ul style="list-style-type: none"> • в «Менеджере иерархий» консоли управления СЗИ, нажать на пиктограмму «Управление токенами»; • в окне «Управление токенами» перейти на вкладку «Пользователи»; • в строке поиска ввести User2 и выполнить поиск; • выбрать из найденного списка, пользователя GIS.LAN\User2_AD и открыть «Карточку пользователя»; • в «Карточке пользователя» нажать на пиктограмму «+Выпустить»; • в открывшемся меню выбрать «Для безопасного входа по паролю»; • в окне «Выпуск токена для безопасного входа по паролю» выбрать подключенный токен и нажать «Далее»; • в окне «Выпуск токена для безопасного входа по паролю» активировать тумблер «Инициализировать» и нажать кнопку «Далее»; • в открывшемся окне ввести PIN-код для Администратора и 	Токен инициализирован

№ п/п	Действия	Ожидаемый результат
	<p>Пользователя;</p> <ul style="list-style-type: none"> • нажать кнопку «Применить»; • для инициализации токена ввести PIN-код администратора и нажать кнопку «ОК»; • после завершения инициализации токена, снять флаг «Сменить PIN-код при первом входе в ОС по токену (средствами Блокхост-Сеть)»; • нажать кнопку «Закрыть» 	
1.3	Убедиться в том, что токен выпущен доменному пользователю GIS.LAN\User2_AD	Токен присвоен пользователю
1.4	<ul style="list-style-type: none"> • на строке активного токена в «Карточке пользователя» User2_AD, открыть контекстное меню; • нажать кнопку контекстного меню «Изъять»; • в открывшемся окне «Изъятия устройства» нажать кнопку «Да» 	Токен изъят у пользователя
2	Выполнить указанные действия пунктов 1.1-1.4 для доменного пользователя FreeIPA.local\User1_IPA	Совпадение полученных результатов с приведенными выше результатами
3	Присвоение токена локальному пользователю PC8\User1	
3.1	Войти в ОС PC8 от имени и с правами пользователя User1	Загрузка рабочего стола
3.2	Подключить к PC8 токен	Токен подключен
3.3	Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор	Загрузка рабочего стола
3.4	<p>От имени и с правами Администратор загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • выбрать PC8; • перешли на вкладку «Пользователь»; • нажать на пиктограмму «+Выпустить»; • в открывшемся меню выбрать выпуск токена для «Безопасного входа по паролю»; • в окне «Выпуск токена для безопасного входа по паролю» выбрать токен и нажать кнопку «Далее»; • в окне «Выпуска токена для безопасного входа по паролю» нажать кнопку «Применить»; • ожидайте ввода PIN-кода пользователем; • перейти на PC8 в окно ввода PIN-кода; • от имени пользователя User1 ввести три раза некорректный PIN-код; • убедилась, в невозможности задать PIN-код не соответствующий политике безопасности для токена; • ввести верный PIN-код и нажать кнопку «Применить»; • вернуться в консоль управления на PC17 	Токен инициализирован
3.5	Убедиться, что выполнен успешный выпуск токена для пользователя User1. Нажать кнопку «Закрыть»	Токен присвоен пользователю PC8\User1
3.6	<p>В консоли управления СЗИ, перейти на вкладку управления токенами и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть «Карточку пользователя» User1; • на строке с присвоенным токеном в «Карточке пользователя» 	Токен изъят у пользователя

№ п/п	Действия	Ожидаемый результат
	User1, открыть контекстное меню; <ul style="list-style-type: none"> • нажать кнопку «Изъять»; • в открывшемся окне «Изъятия устройства» нажать кнопку «Да» 	
3.7	Выполнить указанные в пунктах 3.1–3.6 действия на PC15 для ОС Astra Linux SE, PC16 для ОС Альт 8 СП и PC18 для РЕД ОС и остальных ОС Windows	Совпадение полученных результатов с приведенными выше результатами
4	Просмотр событий аудита	
4.1	<p>Войти на PC1 от имени и справами пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ PC1, вкладку «События» 3) установить фильтр по типу событий «Управление жизненным циклом токенов» 4) нажать кнопку «Поиск» 5) выбрать сервер СЗИ PC17; 6) перейти на вкладку «События»; 7) установить фильтр по типу событий «Управление жизненным циклом токенов»; 8) нажать кнопку «Поиск»; 9) убедиться в появлении событий управления жизненным циклом токенов 	Появление сообщений, фиксирующих Управление жизненным циклом токенов

Критерии оценки:

Результаты проверки считаются положительным, если:

- СЗИ позволяет управлять жизненным циклом токенов;
- СЗИ регистрирует события безопасности, связанные с управлением жизненным циклом токенов.

2.10.1.2 Проверка требования применения установленной политики аутентификации

Описание проверки:

СЗИ предоставляет возможность идентификации и аутентификации пользователей при удаленном доступе на ПК (с использованием механизма удаленного доступа MS Windows - RDP)

АБ СЗИ при помощи средств консоли администрирования имеет возможность устанавливать и изменять следующие параметры политики аутентификации с использованием PIN-кода персональных электронных идентификаторов пользователей (токенов):

- минимальную длину PIN-кода (не менее 6 буквенно-цифровых символов);
- соответствие PIN-кода требованиям сложности (PIN-код должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы);

Выполняемые действия:

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

Таблица ПЗ.42 – Проверка применения установленной политики аутентификации

№ п/п	Действия	Ожидаемый результат
1	Формирование парольной политики	
1.1	Войти на РС1, сервер безопасности I уровня, от имени и с правами пользователя Администратор	Загрузка рабочего стола
1.2	От имени и с правами Администратор загрузить консоль управления СЗИ и выполнить следующие действия: 1) выбрать РС1, «Политики», «Политика клиента по умолчанию», Windows, «Сложность паролей»; 2) Установить флаги на параметрах для пароля пользователя: <ul style="list-style-type: none"> • минимальное количество символов – 6; • срок действия пароля (дней) – 42; • количество новых символов при смене пароля – 1; • запретить использование последних паролей – 1; • проверить пароль на соответствие требованиям сложности; • заблокировать использование популярных паролей; 3) Установить флаги на параметрах для PIN-кода токена: <ul style="list-style-type: none"> • минимальное количество символов - 6; • срок действия PIN-кода (дней) – 45; • количество новых символов при смене PIN-кода – 1; • проверить PIN-код на соответствие требованиям сложности; 4) Установить флаги и время блокирования в разделе «Аутентификация»: <ul style="list-style-type: none"> • количество попыток входа – 3; • заблокировать пользователя при неправильном вводе паролей на (минут)» - 5; 5) Сохранить выполненные изменения; 6) Перейти на вкладку Linux, «Сложность паролей»; 7) Выполнить настройки «Сложность паролей» для Linux, аналогичные параметрам, установленным для Windows; 8) Сохранить выполненные изменения; 9) Выполнить принудительное наследование параметров для «Сложности паролей»; 10) синхронизировать политику для всех компьютеров используя контекстное меню	Парольная политика сформирована
2	Проверка применения сформированной парольной политики	
2.1	Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор От имени и с правами Администратор загрузить консоль управления СЗИ и выполнить следующие действия: <ul style="list-style-type: none"> • выбрать последовательно РС17, «Политики», «Политика клиента по умолчанию», Windows, «Сложность паролей»; • сверить загруженные параметры; • перейти на вкладку Linux, «Сложность паролей»; 	Парольная политика применена на защищаемые ПК

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> сверить загруженные параметры 	
3	Просмотр событий аудита	
3.1	<p>Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия:</p> <ol style="list-style-type: none"> запустить консоль управления СЗИ; выбрать сервер СЗИ РС1, вкладку «События»; нажать кнопку «Поиск» 	Появление сообщений аудита, фиксирующих изменение параметров работы СЗИ

Критерии оценки:

Результаты проверки считаются положительным, если СЗИ позволяет применять установленные политики аутентификации для пользователей.

2.10.1.3 Проверка идентификации и аутентификации пользователя при входе в систему

Описание проверки:

СЗИ от НСД «Блокхост-Сеть 4» реализует:

- идентификация и аутентификация пользователей, являющихся работниками оператора, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей;
- пользователи однозначно идентифицируются и аутентифицируются для всех видов доступа;
- должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа с правами привилегированных учетных записей (администраторов);
- должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа с правами непривилегированных учетных записей (пользователей).

СЗИ реализует ограничение количества неуспешных попыток входа и блокирование средства вычислительной техники (далее – СВТ) при их превышении.

СЗИ реализует автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток выхода, с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль).

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблицах ПЗ.43 и ПЗ.44.

Таблица ПЗ.43 – Проверка идентификации и аутентификации пользователя при входе в систему с ОС MS Windows

№ п/п	Действия	Ожидаемый результат
1	Проверка идентификации и аутентификации пользователей	
2	Войти в систему на РС8, от имени и с правами пользователя Администратор . Создать пользователя User1 и задать пароль для первого входа. Подключить к USB-разъёму компьютера токен.	Пользователь создан. Токен подключен
3	Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор , запустить консоль управления СЗИ и выполнить следующие действия: <ul style="list-style-type: none"> • выбрать РС8 и перейти на вкладку «Пользователь»; • нажать на кнопку «+Выпустить»; • выпустить пользователю User1 токен для безопасного входа по паролю; • в консоли управления СЗИ выбрать РС17; • перейти во вкладку «Политики», «Политика клиента по умолчанию»; • выбрать раздел Windows и вкладку «Управление входом в ОС»; • нажать пиктограмму «+» и добавить локального пользователя РС8\User1; • установить флаг «Разрешить» напротив «Аутентификация Windows»; • установить флаг в «Разрешить» напротив «По токену»; • сохранить выполненные изменения 	Токен зарегистрирован. Установлен тип аутентификации по токену
4	Выполнить попытку входа в систему РС8 от имени и с правами санкционированного пользователя User1	Сообщение о требовании поменять пароль пользователя
5	Нажать клавишу «Ок» и в окне смены пароля и попытаться ввести и подтвердить новый пароль со следующими параметрами: <ul style="list-style-type: none"> • попытаться ввести пароль, не удовлетворяющий требованиям сложности; • ввести пароль, удовлетворяющий всем требованиям сложности, но не содержащий символы в нижнем регистре; • ввести пароль, удовлетворяющий всем требованиям сложности, но не содержащий символы в верхнем регистре; • ввести пароль, удовлетворяющий всем требованиям сложности, но не содержащий специальные символы; • ввести пароль, удовлетворяющий всем требованиям сложности, но не содержащий цифры; 	Пароль не изменен. Пароль не удовлетворяет требованиям сложности. Пароль должен содержать символы в нижнем регистре. Пароль должен содержать символы в верхнем регистре. Пароль должен содержать специальные символы. Пароль должен содержать цифры Пароль не удовлетворяет требованиям длины пароля! Пароль не должен содержать меньше 6 символов

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> • ввести пароль, удовлетворяющий всем требованиям сложности, но содержащий меньше 6 символов 	
6	Ввести и подтвердить пароль, соответствующий парольной политике (таблица ПЗ.42 п. 1.2)	Пароль изменен. Загрузка рабочего стола
7	Перезагрузить компьютер и выполнить попытку входа в систему PC8 от имени и с правами уполномоченного пользователя User1 Указать: 1) неверный пароль; 2) назначенную мандатную метку; 3) верный PIN-код идентификатора входа.	Запрет входа в систему
8	Выполнить попытку входа в систему PC8 от имени и с правами уполномоченного пользователя User1 . Указать: 1) верный пароль; 2) мандатную метку выше допустимой; 3) верный PIN-код идентификатора входа.	Запрет входа в систему Выбранный мандат входа пользователя превышает максимально допустимый!
9	Выполнить попытку входа в систему PC8 от имени и с правами уполномоченного пользователя User1 . Указать: 1) верный пароль; 2) назначенную мандатную метку; 3) неверный PIN-код идентификатора входа.	Запрет входа в систему. Блокировка пользователя на 5 мин.
10	Перезагрузить компьютер и выполнить попытку входа в систему PC8 от имени и с правами уполномоченного пользователя User1 . Указать: 1) верный пароль; 2) назначенную мандатную метку; 3) верный PIN-код идентификатора входа.	Запрет входа в систему. (Время блокировки не истекло)
11	Подождать 5 минут. Выполнить попытку входа в систему PC8 от имени и с правами уполномоченного пользователя User1 . Указать: 1) верный пароль; 2) назначенную мандатную метку; 3) неверный PIN-код идентификатора входа.	Запрет входа в систему. Ошибка входа на токен! Неверный ПИН-код.
12	Выполнить попытку входа в систему PC8 от имени и с правами санкционированного пользователя User1 . Указать: 1) верный пароль; 2) назначенную мандатную метку; 3) верный PIN-код идентификатора входа.	Вход в систему

Таблица ПЗ.44 – Проверка идентификации и аутентификации пользователя при входе в систему с ОС Linux

№ п/п	Действия	Ожидаемый результат
1	Проверка идентификации и аутентификации пользователей	
2	Войти в систему на PC15, от имени и с правами пользователя Администратор . Создать пользователя User1 и задать пароль для первого	Пользователь создан

№ п/п	Действия	Ожидаемый результат
	входа не соответствующий парольной политике.	
3	<p>Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • выбрать РС17; • перейти во вкладку «Политики», «Политика клиента по умолчанию»; • выбрать раздел Linux и вкладку «Управление входом в ОС»; • нажать пиктограмму «+» и добавить локального пользователя РС15\User1; • установить флаг «Разрешить» напротив «Аутентификация ОС»; • установить флаг «Запретить» напротив «По токену»; • сохранить сделанные изменения. 	Установлен тип аутентификации по токену
4	Перезагрузить РС15 и выполнить попытку входа в систему РС15 от имени и с правами уполномоченного пользователя User1 с паролем не соответствующим заданной политике сложности для пароля	Сообщение о требовании поменять пароль пользователя
5	<p>Нажать клавишу «Ок» и в окне смены пароля и попытаться ввести и подтвердить новый пароль со следующими параметрами:</p> <ul style="list-style-type: none"> • ввести пароль, не удовлетворяющий требованиям сложности; • ввести пароль, удовлетворяющий требованиям сложности, но не содержащий символы в нижнем регистре; • ввести пароль, удовлетворяющий требованиям сложности, но не содержащий символы в верхнем регистре; • ввести пароль, удовлетворяющий требованиям сложности, но не содержащий специальные символы; • ввести пароль, удовлетворяющий требованиям сложности, но не содержащий цифры; • ввести пароль, удовлетворяющий требованиям сложности, но содержащий меньше 6 знаков 	<p>Пароль не изменен. Пароль не удовлетворяет требованиям сложности. Пароль должен содержать символы в нижнем регистре. Пароль должен содержать символы в верхнем регистре. Пароль должен содержать специальные символы. Пароль должен содержать цифры Пароль не удовлетворяет требованиям длины пароля! Пароль не должен содержать меньше 6 символов</p>
6	Ввести и подтвердить пароль, соответствующий парольной политике (таблица ПЗ.42 п. 1.2)	Пароль изменён. Загрузка рабочего стола
7	Перезагрузить РС15 и выполнить попытку входа в систему РС15 от имени и с правами уполномоченного пользователя User1 введя 3 раза некорректный пароль	Сообщение о блокировке пользователя на 5 минут
8	Подождать 5 минут и ввести корректный пароль	Загрузка рабочего стола
9	Подключить к РС15 токен	Токен подключен
10	Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор ,	Установлен тип аутентификации по токену

№ п/п	Действия	Ожидаемый результат
	загрузить консоль управления СЗИ и выполнить следующие действия: <ul style="list-style-type: none"> • выбрать PC15 и перейти на вкладку «Пользователь»; • нажать пиктограмму «+» и выпустить токен для безопасного входа по паролю, пользователю PC15\User1; • выбрать PC17; • перейти на вкладку «Политики», «Политика клиента по умолчанию»; • выбрать раздел Linux и вкладку «Управление входом в ОС»; • выбрать локального пользователя PC15\User1; • установить флаг «Запретить» напротив «Аутентификация ОС»; • установить флаг «Разрешить» напротив «По токену»; • сохранить изменения 	
11	Перезагрузить PC15 и выполнить попытку входа в систему PC15 от имени и с правами уполномоченного пользователя User1	
12	В окне ввести и подтвердить новый PIN-код, удовлетворяющий всем требованиям безопасности, но не соответствующий требованиям длины	Длина PIN-кода не удовлетворяет требованиям безопасности
13	В окне смены ввести и подтвердить новый PIN-код, соответствующий всем требованиям безопасности	PIN-код установлен Выполнен вход в систему PC15
14	Перезагрузить компьютер и выполнить попытку входа в систему PC15 от имени и с правами уполномоченного пользователя User1 Указать: 1) неверный PIN-код идентификатора входа 3 раз	Ошибка. Блокировка пользователя на 5 минут
15	Подождать 5 минут	
16	Выполнить попытку входа в систему PC15 от имени и с правами пользователя User1 , указав верный PIN-код токена	Успешный вход в систему
17	Выполнить указанные в пунктах 1–16 действия для остальных ОС Linux	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Результаты проверки считаются положительным, если СЗИ позволяет:

- осуществлять проверку идентификации и аутентификации пользователя;
- применять установленные политики аутентификации для пользователей;
- при назначении токена для входа пользователя по паролю, при первом входе пользователя на ПК с использованием токена, должен быть сгенерирован пароль пользователя и записан на токен.

2.10.1.4 Проверка возможности самостоятельного изменения паролей и PIN-кодов пользователем

Описание проверки:

СЗИ позволяет пользователям ИС возможность при помощи средств ОС самостоятельно изменять пароли или PIN-коды персональных электронных идентификаторов (токенов) в зависимости от вида аутентификации.

При аутентификации пользователя с использованием персонального электронного идентификатора для безопасного входа по паролю, при первом входе пользователя на ПК с использованием токена, средствами СЗИ сгенерирован и записан на токен безопасный пароль.

Выполняемые действия:

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

Таблица ПЗ.45 – Проверка возможности самостоятельного изменения PIN-кодов

№ п/п	Действия	Ожидаемый результат
1	Установка требований к сложности PIN-кода пользователей	
1.1	<p>Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • выбрать РС17; • перейти во вкладку «Политики», «Политика клиента по умолчанию»; • выбрать раздел Windows и вкладку «Сложность паролей»; • установить все флаги в параметрах PIN-кода токена; • выбрать раздел Linux и вкладку «Сложность паролей»; • установить все флаги в параметрах PIN-кода токена; • сохранить выполненные изменения 	Политика установлена
1.2	<p>В консоли управления СЗИ выполнить следующие действия:</p> <ul style="list-style-type: none"> • выбрать РС8; • перейти во вкладку «Пользователь» и открыть карточку пользователя User1; • выбрать токен и открыть контекстное меню; • выбрать сменить PIN-код пользователя и установить галочку на параметре «Изменить PIN-код при первом входе»; • нажать кнопку «Сменить PIN-код»; • после успешной смены PIN-кода пользователем нажать кнопку «Ок» 	

№ п/п	Действия	Ожидаемый результат
2	Смена PIN-кода токена пользователем	
2.1	Выполнить попытку входа в систему РС8 от имени и с правами санкционированного пользователя User1 , введя правильный первичный PIN-код токена	Появление сообщения о том, что «Срок действия PIN-кода истек. Смените PIN-код»
2.2	Нажать кнопку «Ок» и попытаться ввести новый ПИН-код: <ul style="list-style-type: none"> • ввести PIN-код не удовлетворяющий требованиям сложности; • ввести PIN-код не содержащий символы в нижнем регистре; • ввести PIN-код не содержащий символы в верхнем регистре; • ввести PIN-код не содержащий специальные символы 	Ошибка. PIN-код не удовлетворяет требованиям сложности. PINкод должен содержать символы в нижнем регистре. PIN-код должен содержать символы в верхнем регистре. PIN-код должен содержать специальные символы.
2.3	От имени и с правами пользователя User1 выполнить смену PIN-кода, в соответствии с установленной парольной политикой.	PIN-код изменён пользователем. Выполнен вход в ОС
2.4	Выполнить указанные в пунктах 1.2–2.3 действия на рабочих станциях для всех остальных установленных операционных систем MS Windows/Linux	Совпадение полученных результатов с приведенными выше результатами
3	Смена пароля пользователем	
3.1	Войти в систему РС8 от имени и с правами пользователя User2 . Нажать комбинацию клавиш <Ctrl>+<Alt>+	Появление диалога выбора действий ОС Windows
3.2	Заполнить поля диалога: <ul style="list-style-type: none"> • выбрать «Изменить пароль»; • в поле ввода «Пароль» ввести текущий пароль; • в поле ввода «Новый пароль» ввести новый пароль (длиной 8 символов и удовлетворяющий парольной политике); • повторить ввод нового пароля в поле ввода «Повторите новый пароль»; • нажать клавишу «Enter» 	Пароль изменен. Загрузка рабочего стола.
3.3	Войти в систему РС18 от имени и с правами пользователя user_test.	Вход в систему
3.4	Открыть терминал и выполнить терминальную команду: sudo passwd. Выполнить указанные действия: <ul style="list-style-type: none"> • ввести пароль текущего пользователя; • ввести новый пароль (длиной 8 символов и удовлетворяющий парольной политике); • повторить ввод нового пароля; • нажать клавишу «Enter»; • выйти из системы 	Пароль изменен.
3.5	Войти в систему от имени и с правами пользователя user_test введя новый пароль пользователя	Вход в систему
4	Просмотр событий аудита	
4.1	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ;	Появление сообщений, фиксирующих Управление входом в ОС

№ п/п	Действия	Ожидаемый результат
	2) выбрать сервер СЗИ РС17, вкладку «События»; 3) установить фильтр по категории «Управление входом в ОС»; 4) нажать кнопку «Поиск»	

Критерии оценки:

Результаты проверки считаются положительным, если СЗИ позволяет:

- пользователям самостоятельно изменять пароли и PIN-коды токенов.

2.10.1.5 Проверка возможности управления параметрами механизмов защиты средства доверенной загрузки (СДЗ) «SafeNode System Loader»

Описание проверки:

СЗИ от НСД «Блокхост-Сеть 4» обеспечивает управление параметрами механизмов защиты (управление входом, управление аутентификацией в домене, управление сложностью паролей, контроль целостности) средства доверенной загрузки «SafeNode System Loader» на клиентских рабочих станциях.

Выполняемые действия:

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

Таблица ПЗ.46 – Управление параметрами механизмов защиты средства доверенной загрузки «SafeNode System Loader»

№ п/п	Действия	Ожидаемый результат
1	Взятие под управление СДЗ «SafeNode System Loader»	
1.1	Выполнить установку СДЗ «SafeNode System Loader» на рабочие станции ЭВМ2 – ЭВМ5 в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке»	Выполнена установка СДЗ на рабочие станции
1.2	Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия: <ul style="list-style-type: none"> • открыть «Менеджер иерархий»; • убедиться в том, что на рабочих станциях ЭВМ2 – ЭВМ5, отображается информационное сообщение «Модуль доверенной загрузки» установлен на компьютере, но не управляется из Блокхост-Сеть; • перейти в подсистему «Развертывание»; • перейти на вкладку «Задачи» и сконфигурировать задачу «Взятие под управление модуля доверенной 	СДЗ «SafeNode System Loader» взят под управление Блокхост-Сеть

№ п/п	Действия	Ожидаемый результат
	<p>загрузки «SafeNode System Loader» со следующими параметрами:</p> <ul style="list-style-type: none"> ○ перейти на вкладку «Компьютеры»; ○ добавить компьютеры; ○ перейти на вкладку «Пароли администраторов»; ○ добавить в список пароли администраторов от всех добавленных компьютеров; ○ перейти на вкладку «Планировщик»; ○ задать тип запуска – Вручную; ○ сохранить внесенные изменения; ● нажать на кнопку «Запустить»; ● убедиться в успешном завершении задачи; ● перейти в «Менеджер иерархий»; ● убедиться в том, что иконки компьютеров с взятыми под управление модуля доверенной загрузки «SafeNode System Loader», отображаются черным цветом; ● убедиться, что исчезло информационное сообщение о том, что модуль «Доверенной загрузки» установлен на компьютере, но не управляется из Блокхост-Сеть 	
1.3	<p>Перезагрузить PC6 и войти в ОС от имени Администратора. Выполнить следующие действия:</p> <ul style="list-style-type: none"> ● загрузить локальную консоль СДЗ «SafeNode System Loader» с правами администратора; ● убедиться, что присутствуют информационные сообщения: <ul style="list-style-type: none"> ○ «SafeNode System Loader» работает в режиме управления из Блокхост-Сеть»; ○ функции локального администратора неактивны, настройка СЗИ осуществляется из консоли Блокхост-Сеть»; ○ для локального управления функциями безопасности необходимо выйти из режима управления; ○ убедиться, что активна кнопка: «Выход из режима управления Блокхост-Сеть» 	СДЗ «SafeNode System Loader» находится под управлением Блокхост-Сеть
1.4	Выполнить указанные в пункте 1.3 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
2	Управление настройкой входа и аутентификацией пользователей в СДЗ «SafeNode System Loader»	
2.1	На контроллере домена зарегистрировать учетные записи пользователей user1_ad и user2_ad. Зарегистрировать учетную запись пользователя user1 на рабочих станциях ЭВМ2 – ЭВМ5 с ОС Windows/Linux	Учетные записи пользователей зарегистрированы
2.2	Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор. Подключить USB-токен к PC17. Загрузить консоль управления СЗИ и выполнить следующие действия:	Включена политика управления аутентификацией пользователей. Добавлены учетные записи

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> • открыть подсистему «Управления токенами»; • перейти на вкладку «Токены»; • выбрать подключенный токен; • нажать на кнопку «Зарегистрировать» для регистрации токена; • нажать на кнопку «Выпустить»; • выбрать «Выпуск токена для безопасного входа по паролю»; • в окне «Выпуск токена для безопасного входа по паролю» нажать кнопку «Выбрать»; • добавить учетную запись пользователя user2_ad; • сохранить выполненные изменения; • введите PIN-код токена; • закройте окно «Выпуска токена для безопасного входа по паролю»; • перейти в подсистему «Менеджер иерархий»; • открыть «Политику клиента по умолчанию» для изменения; • зарегистрировать доменного пользователя: user1_ad с разрешением аутентификации Windows и с разрешением аутентификации ОС (для Linux); • зарегистрировать пользователя: user1 с разрешением аутентификации Windows и с разрешением аутентификации ОС (для Linux); • сохранить внесенные изменения; • открыть «Политику SafeNode System Loader по умолчанию»; • перейти на вкладку «Настройка входа»; • установить аутентификацию средствами «Блокхост-Сеть»; • перейти на вкладку «Управление аутентификацией»; • включить механизм аутентификации пользователей; • перейти на вкладку «Дополнительные настройки»; • установить флаги на механизмах «Проверки пароля в SafeNode» и «Пользователи с разрешением на вход в ОС» на клиентских компьютерах; • перейти на вкладку «Список пользователей»; • добавить учетные записи пользователей, созданных в п.2.1 настоящей таблицы; • сохранить внесенные изменения 	<p>пользователей</p>
<p>2.3</p>	<p>Перезагрузить РС6 и войти в ОС от имени доменного пользователя user1_ad;</p> <ul style="list-style-type: none"> • убедиться, что аутентификация выполняется средствами «Блокхост-Сеть»; • загрузить локальную консоль СДЗ «SafeNode System Loader» от имени и с правами администратора; • убедиться в том, что учетные записи user1_ad и user1 добавлены в СДЗ «SafeNode System Loader»; • убедиться в том, что учетная запись user2_ad с 	<p>Аутентификация выполняется средствами «Блокхост-Сеть». Учетные записи пользователей добавлены в СДЗ «SafeNode System Loader»</p>

№ п/п	Действия	Ожидаемый результат
	зарегистрированным токеном добавлены в СДЗ «SafeNode System Loader»	
2.4	Выполнить указанные в пункте 2.3 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
2.5	<p>Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть подсистему «Менеджер иерархий»; • перейти на вкладку «Политики»; • открыть «Политику SafeNode System Loader по умолчанию» на изменение; • перейти на вкладку «Настройка входа»; • установить аутентификацию средствами «SafeNode System Loader» и «Блокхост-Сеть»; • сохранить внесенные изменения 	Установлена аутентификация пользователей средствами «SafeNode System Loader» и «Блокхост-Сеть»
2.6	<p>Перезагрузить РС6 и войти в ОС от имени локального пользователя user1:</p> <ul style="list-style-type: none"> • убедиться, что аутентификация выполняется средствами СДЗ «SafeNode System Loader» и «Блокхост-Сеть» 	Аутентификация выполняется средствами СДЗ «SafeNode System Loader» и «Блокхост-Сеть»
2.7	Выполнить указанные в пункте 2.6 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
3	Управление парольной политикой пользователей, СДЗ «SafeNode System Loader»	
3.1	<p>Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть подсистему «Менеджер иерархий»; • перейти на вкладку «Политики»; • открыть «Политику SafeNode System Loader по умолчанию» на изменение; • перейти на вкладку «Настройка входа»; • установить аутентификацию средствами: «Блокхост-Сеть»; • перейти на вкладку «Сложность пароля», «Пароль пользователя»; • установить флаги и задать значения на следующих параметрах: <ul style="list-style-type: none"> ○ «Минимальное количество символов» - 8; ○ «Контроля сложности пароля», установить флаги на следующих параметрах: Цифры, Заглавные буквы, Строчные буквы; ○ «Срок действия пароля (дней)» – 40; ○ «Минимальное число уникальных символов» - 1. • перейти на вкладку «Пароль администратора»; • установить флаги и задать значения на следующих параметрах: <ul style="list-style-type: none"> ○ «Минимальное количество символов» - 10; 	Установлена сложность пароля и дополнительные настройки для пользователей и администратора

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> ○ «Контроля сложности пароля», установить флаги на следующих параметрах: Цифры, Заглавные буквы, Строчные буквы; ○ «Срок действия пароля (дней)» – 30; ○ «Минимальное число уникальных символов» - 1; • перейти на вкладку «Дополнительно»; • установить флаги и задать значения дополнительных настроек для следующих параметров: <ul style="list-style-type: none"> ○ «Количество попыток входа» – 5; ○ «Блокировать при неудачной попытке входа (мин)» – 15; ○ «Запретить использование последних паролей» - 5; • сохранить внесенные изменения 	
3.2	<p>Перезагрузить РС6 и войти в ОС от имени администратора. Загрузить локальную консоль администратора СДЗ «SafeNode System Loader»:</p> <ul style="list-style-type: none"> • убедиться в том, что парольная политика аутентификации пользователей заданная средствами Блокхост-Сеть, была передана в СДЗ «SafeNode System Loader» в соответствии с п.3.1 настоящей таблицы 	<p>Парольная политика аутентификации пользователей (admin policy, user policy) заданная средствами Блокхост-Сеть, передана в СДЗ «SafeNode System Loader»</p>
3.3	<p>Выполнить указанные в пункте 3.2 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux</p>	<p>Совпадение полученных результатов с приведенным выше результатом</p>
4	Настройка подключения к домену	
4.1	<p>Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть подсистему «Менеджер иерархий»; • перейти на вкладку «Политики» и открыть «Политику SafeNode System Loader по умолчанию» для изменения; • перейти на вкладку «Настройки подключения к домену»; • включить механизм, установив переключатель в положение «Механизм включен»; • перейти на вкладку krb5.conf и нажать на кнопку «Задать значения по умолчанию»; • ввести в окне «Задание значения по умолчанию», имя основного контроллера домена, домен и IP адрес контроллера домена; • проверить наличие заданных значений на вкладках krb5.conf, ldap.conf, host; • сохранить внесенные изменения 	<p>Выполнена настройка подключения к домену</p>
4.2	<p>Перезагрузить РС6 и войти в ОС от имени Администратора.</p> <ul style="list-style-type: none"> • загрузить локальную консоль СДЗ «SafeNode System Loader» от имени и с правами администратора; • перейти на вкладку «Основные настройки» и развернуть «Настройки LDAP»; • убедиться в том, что настройки krb5.conf, ldap.conf и 	<p>Настройки подключения к домену заданные средствами Блокхост-Сеть, переданы в СДЗ «SafeNode System Loader»</p>

№ п/п	Действия	Ожидаемый результат
	host переданы в модуль доверенной загрузки «SafeNode System Loader» в соответствии с заданными значениями в п. 4.1	
4.3	Выполнить указанные в пункте 4.2 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
5	Настройка сетевого адаптера UEFI	
5.1	<p>Войти в ОС на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть подсистему «Менеджер иерархий»; • перейти на вкладку «Политики»; • открыть «Политику SafeNode System Loader по умолчанию» на изменение; • перейти на вкладку «Сетевой адаптер UEFI»; • включить механизм настройки сетевого адаптера UEFI, установив переключатель в положение «Механизм включен»; • выбрать режим «Получать IP-адрес автоматически»; • сохранить внесенные данные 	Установлен режим получения IP-адреса автоматически
5.2	<p>Войти в ОС на PC6</p> <ul style="list-style-type: none"> • загрузить локальную консоль СДЗ «SafeNode System Loader» от имени и с правами администратора; • убедиться в том, что в настройке LDAP выключена сетевая подсистема использования статического IP-адреса 	Убедились, что в настройке LDAP выключена сетевая подсистема использования статического IP-адреса
5.3	Выполнить указанные в пункте 5.2 действия на рабочих станциях ЭВМ2 ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
5.4	<p>Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор. Выполнить следующие действия:</p> <ul style="list-style-type: none"> • загрузить консоль управления СЗИ: • открыть «Менеджер иерархий»; • перейти на вкладку «Политики»; • открыть «Политику SafeNode System Loader по умолчанию» на изменение; • перейти на вкладку «Сетевой адаптер UEFI»; • включить механизм настройки сетевого адаптера UEFI, установив переключатель в положение «Механизм включен»; • выбрать режим «Статический IP-адрес»; • сохранить внесенные изменения; • перейти в «Менеджере иерархий»; • выбрать рабочую станцию PC6 и перейти во вкладку «Настройки»; • выбрать «Сетевой адаптер UEFI»; • включить механизм настройки сетевого адаптера, установив переключатель в положение «Настроить 	Установлен режим задания статического IP-адреса

№ п/п	Действия	Ожидаемый результат
	сетевой адаптер»; • задать сетевые параметры рабочей станции: IP-адрес, маску подсети и шлюз (параметры устанавливаются в соответствии с требованиями теста)	
5.5	Войти в ОС на РС6. • загрузить локальную консоль СДЗ «SafeNode System Loader» от имени и с правами администратора; • убедиться в том, что в настройке LDAP, установлены галочки на «Использовании сетевой подсистемы» и «Использовании статического IP-адреса»; • убедиться в том, что параметры, заданные в п. 5.4 настоящей таблицы соответствуют заданным: IP-адрес, маска подсети и основной шлюз	Убедились, что режим использования статического IP-адреса и установленные параметры, заданные политикой Блокхост-Сеть, переданы в СДЗ «SafeNode System Loader»
5.6	Выполнить указанные в пунктах 5.4 - 5.5 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенным выше результатом
6	Управление механизмами контроля целостности СДЗ политикой сервера	«SafeNode System Loader» через
6.1	Войти на РС17, сервер безопасности II уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия: • открыть «Менеджер иерархий»; • перейти на вкладку «Политики»; • открыть «Политику SafeNode System Loader по умолчанию» на изменение; • выбрать «Контроль целостности» и выполнить следующие действия: • перейти на вкладку «Файловая система»; • включить механизм контроля файлов; • добавить произвольные файлы для контроля («Файлы Windows»«Файлы Linux»); • перейти на вкладку «Реестр»; • включить механизм контроля реестра; • добавить рекомендованные ключи; • перейти на вкладку «Загрузочные сектора»; • включить контроль целостности загрузочных секторов; • перейти на вкладку «UEFI»; • включить контроль UEFI; • добавить контролируемые объекты: переменные UEFI, драйверы UEFI и системные таблицы UEFI; • перейти на вкладку «Аппаратная среда»; • включить механизм контроля изменений аппаратной среды; • установить флаги на процессоры, оперативная память (ОЗУ), жесткие диски, PCI-устройства, USB-устройства; • перейти на вкладку «Другие параметры» и установить:	Выполнена настройка политики контроля целостности

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> ○ алгоритм хеширования: SHA-512; ○ реакция на нарушения: Запись в журнал аудита; ● сохранить внесенные изменения в политику 	
6.2	<p>Войти на РС6 от имени Администратора и выполнить следующие действия:</p> <ul style="list-style-type: none"> ● загрузить локальную консоль СДЗ SafeNode System Loader от имени и с правами администратора; ● нажать на кнопку «Расширенный режим»; ● убедиться в том, что все объекты поставленные на контроль целостности, средствами Блокхост-Сеть в п.6.1 настоящей таблицы, были переданы в СДЗ «SafeNode System Loader» 	<p>Все параметры контроля целостности, установленные в Блокхост-Сеть, переданы в СДЗ «SafeNode System Loader»</p>
6.3	<p>Выполнить указанные в пункте 6.2 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux</p>	<p>Совпадение полученных результатов с приведенным выше результатом</p>
7	Сбор событий аудита СДЗ SafeNode System Loader	
7.1	<p>Войти на РС1, сервер безопасности I уровня, от имени и с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> ● открыть «Менеджер иерархий»; ● открыть «Политику SafeNode System Loader по умолчанию» на изменение; ● перейти на вкладку «Настройка входа»; ● установить аутентификацию средствами «SafeNode System Loader» и «Блокхост-Сеть»; ● сохранить внесенные изменения 	<p>Включена политика аутентификацией пользователей средствами «SafeNode System Loader» и «Блокхост-Сеть»</p>
7.2	<p>Перезагрузить РС6 и дождаться загрузки компьютера:</p> <ul style="list-style-type: none"> ● убедиться в том, что у пользователя запрашивается логин и пароль СДЗ «SafeNode System Loader»; ● ввести логин и пароль незарегистрированного пользователя; ● убедиться в появлении ошибки аутентификации; ● ввести правильный логин и неправильный пароль зарегистрированного пользователя; ● убедиться в появлении ошибки аутентификации; ● ввести правильные пароль и логин; ● войти в систему 	<p>Выполнен вход пользователя в систему с использованием СДЗ «SafeNode System Loader» и «Блокхост-Сеть»</p>
7.3	<p>Перезагрузить РС15 и дождаться загрузки компьютера:</p> <ul style="list-style-type: none"> ● убедиться в том, что у пользователя запрашивается логин и пароль СДЗ «SafeNode System Loader»; ● ввести логин и пароль незарегистрированного пользователя; ● убедиться в появлении ошибки аутентификации; ● ввести правильный логин и неправильный пароль зарегистрированного пользователя; ● убедиться в появлении ошибки аутентификации; ● ввести правильные пароль и логин; ● войти в систему 	<p>Выполнен вход пользователя в систему с использованием СДЗ «SafeNode System Loader» и «Блокхост-Сеть»</p>
7.4	<p>Войти на РС1, сервер безопасности I уровня, от имени и</p>	<p>Отражены события обо всех</p>

№ п/п	Действия	Ожидаемый результат
	<p>с правами пользователя Администратор, загрузить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть «Менеджер иерархий»; • выполнить на сервере РС1 загрузку событий аудита, для этого в контекстном меню «Запустить внеплановую загрузку событий аудита» и указать «С клиентских компьютеров»; • перейти во вкладку «События» и в разделе «Фильтры» указать следующие параметры: <ul style="list-style-type: none"> ○ системы: «СДЗ (Средство доверенной загрузки)»; ○ уровни важности: все уровни; ○ компьютеры: изменить на РС8 и РС15; • выполнить поиск; • убедиться, что в разделе события отражаются все события неудачного и успешного входа пользователя на компьютеры РС8 и РС15 	<p>действиях пользователей</p>
8	Управление мягким режимом	
8.1	<p>Войти на РС1 от имени и с правами пользователя администратор и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть «Менеджер иерархий»; • перейти на вкладку «Политики» и открыть «Политику SafeNode System Loader по умолчанию» на изменение; • установить переключатель в положение «Мягкий режим»; • сохранить внесенные изменения 	<p>Включен «Мягкий режим»</p>
8.2	<p>Перезагрузить РС6:</p> <ul style="list-style-type: none"> • убедиться в том, что появляется окно СДЗ «SafeNode System Loader» с сообщением: «СДЗ работает в режиме установки»; • войти в ОС от имени Администратора; • загрузить локальную консоль модуля доверенной загрузки SafeNode System Loader от имени и с правами администратора; • перейти на вкладку «Основные настройки»; • убедиться, что установлен флаг на параметре «Режим установки» 	<p>Убедились, что СДЗ работает в режиме установки</p>
8.3	<p>Выполнить указанные в пунктах 8.2 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux</p>	<p>Совпадение полученных результатов с приведенными выше результатами</p>

Критерии оценки:

Результаты проверки считаются успешными, если СЗИ позволяет:

- управлять параметрами механизмов защиты модуля доверенной загрузки «SafeNode System Loader» на клиентских рабочих станциях.

2.10.2 Проверка идентификации и аутентификации пользователей при удалённом доступе RDP

Описание проверки:

СЗИ предоставляет возможность идентификации и аутентификации пользователей при удаленном доступе на ПК (с использованием механизма удаленного доступа MS Windows - RDP)

Выполняемые действия:

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

Таблица ПЗ.47 – Управление идентификации и аутентификации пользователей при удалённом доступу MS Windows – RDP

№ п/п	Действия	Ожидаемый результат
1	Отключение групповых парольных политик AD	
1.1	Войти в ОС на Ser2008AD с правами «Администратор» и выполнить следующие действия:	Вход в систему
1.2	<ul style="list-style-type: none"> • открыть раздел «Управление групповой политикой»; • открыть лес доменов (GIS.LAN); • выбрать «Default Domain Policy»; • через контекстное меню выбрать «Редактор управления групповыми политиками»; • перейти по иерархическому списку «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Политики учетных записей» → «Политика паролей» 	Открыто окно редактора групповых политик
1.3	Изменить параметр политики «Минимальная длина пароля» с установленного по умолчанию значения 7 знаков на 6 знаков	Параметр политики установлен
1.4	Установить параметр политики «Пароль должен отвечать требованиям сложности» с положения «Включен» в положение «Отключен»	Параметр политики установлен
2	Создание пользователя User3_AD	
2.1	Создать пользователя User3_AD с правами «Пользователь» и с паролем «123456»	
3	Настройка удаленного доступ на PC8	
3.1	<p>Войти в ОС PC8 от имени и с правами пользователя «Администратор» и выполнить следующие действия:</p> <ul style="list-style-type: none"> • перейти по пути «Панель управления», «Система и безопасность», «Система», «Настройка удалённого доступа»; • выбрать вкладку «Удалённый доступ»; • выбрать параметр «Разрешить удалённые подключения к этому компьютеру»; • нажать кнопку «Выбрать пользователей...» и добавить пользователя домена User3_AD; • сохранить сделанные изменения 	
4	Попытка подключения пользователя User3_AD с паролем, не соответствующим установленным парольным политикам	

№ п/п	Действия	Ожидаемый результат
4.1	Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор и выполнить следующие действия:	Загрузка рабочего стола
4.2	<ul style="list-style-type: none"> • запустить «Подключение к удалённому рабочему столу»; • в поле «Компьютер» набрать IP-адрес PC8; • нажать кнопку «Подключить»; • в открывшемся окне «Безопасность Windows» нажать ссылку «Больше вариантов»; • ввести имя и пароль пользователя User3_AD; • нажать кнопку «ОК» 	Ошибка. Недопустимые учетные данные.
5	Попытка подключения пользователя User3_AD с паролем, соответствующим установленным парольным политикам	
5.1	Войти на PC8 от имени и с правами пользователя User3_AD и установить пароль, соответствующий установленным парольным политикам	Загрузка рабочего стола. Пароль изменён
5.2	Выйти из ОС	
5.3	Войти на PC17, сервер безопасности II уровня, от имени и с правами пользователя Администратор и выполнить следующие действия:	
5.4	<ul style="list-style-type: none"> • запустить «Подключение к удалённому рабочему столу»; • в поле «Компьютер» набрать IP-адрес PC8; • нажать кнопку «Подключить»; • в открывшемся окне «Безопасность Windows» нажать ссылку «Больше вариантов»; • ввести имя и пароль пользователя User3_AD; • нажать кнопку «ОК» 	Загрузка рабочего стола.

Критерии оценки:

Результаты проверки считаются положительным, если СЗИ предоставляет возможность идентификации и аутентификации пользователей на ПК с использованием механизма MS Windows RDP

2.10.3 Проверка возможности аутентификации пользователей с использованием цифровых сертификатов

Описание проверки:

В СЗИ предусмотрена возможность двухфакторной аутентификации пользователей средствами СЗИ при входе в ОС с использованием цифровых сертификатов пользователей.

Выполняемые действия:

В качестве центра сертификации используется контроллер домена MS Active Directory. Добавление ролей и компонентов проводится средствами «Диспетчера

сервера».

Средствами мастера добавления ролей выбираются элементы, их компоненты и устанавливаются значения, приведенные в таблице ПЗ.48.

Таблица ПЗ.48 – Перечень устанавливаемых ролей, компонентов и их значений

№	Роль	Значение	
1	Роли сервера		
	-	Web Server (IIS) («Веб-сервер IIS»)	
	-	Application Server («Сервер приложений»)	
	-	Active Directory Certificate Services («Служба сертификации Active Directory»)	
2	Сервер приложений		
2.1	Службы ролей		
	-	Платформа.NET Framework	
	-	Поддержка веб-сервера (IIS)	
	-	Активация по HTTP	
3	Службы сертификации AD		
3.1	Службы ролей		
	-	Центр сертификации	
	-	Служба регистрации в центре сертификации через Интернет	
3.2		Вариант установки	Предприятие («Enterprise»)
3.3		Тип ЦС	Корневой ЦС
3.4		Закрытый ключ	Создать новый закрытый ключ (Create a new private key)
3.4.1		Шифрование	
	-	Поставщик	Crypto-Pro GOST R 34.10-2012
	-	Алгоритм шифрования	ГОСТ Р 34.11-2012 Cryptographic Service provider
	-	Длина ключа	512
	-	Флаг	Разрешить взаимодействие с администратором, если центр сертификации обращается к закрытому ключу
3.4.2		Имя ЦС	
	-	Общее имя для этого ЦС	По умолчанию
	-	Суффикс различающегося имени	По умолчанию
3.4.3		Срок действия	5 лет
3.5		База данных сертификатов	По умолчанию
4	Веб-сервер IIS		
4.1		Службы ролей	По умолчанию

В консоли «Диспетчер сервера» необходимо пройти по ветке «Роли» – «Службы сертификации Active Directory» – (имя Центра сертификации) – «Шаблоны сертификатов».

Через контекстное меню выбирать команду «Управление» и в открывшемся окне «Консоль шаблонов сертификатов» скопировать (дублировать) шаблон «Вход со смарт-картой» (при запросе версии шаблона установить параметр «Windows Server 2003 Enterprise»).

В окне свойств шаблона установить параметры, указанные в таблице ПЗ.49.

Таблица ПЗ.49 – Параметры шаблона сертификата

№	Вкладка	Параметр	Значение
1	Общие		
1.1		Отображаемое имя	Вход со смарт картой ГОСТ
2	Обработка запроса		
2.1.		Цель	Вход с подписью и смарт-картой
3	Шифрование		
3.1.		Минимальный размер ключа	512
3.2		Поставщики	Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
4	Расширения		
4.1		Использование ключа	Цифровая подпись
			Разрешить обмен ключами только с шифрованием ключей
			Считать расширение критическим
4.2		Политика применения	Вход со смарт-картой
			Проверка подлинности клиента
5	Безопасность		
5.1		Администратор домена	Чтение, Запись, Заявка
5.2		Администратор предприятия	Чтение, Запись, Заявка

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

Таблица ПЗ.50 – Проверка возможности аутентификации пользователей с использованием цифровых сертификатов

№ п/п	Действия	Ожидаемый результат
1	Настройка центра сертификации	
1.1	Настроить ЦС в соответствии с таблицей ПЗ.48 и таблицей ПЗ.49 настоящего документа	ЦС настроен
2	Получение сертификата пользователя	
2.1	От имени и с правами пользователя Администратор войти на РС1 запустить консоль управления СЗИ и выполнить следующие действия:	
	<ul style="list-style-type: none"> • подключить токен к РС1; • открыть раздел «Управление токенами»; 	В карточке пользователя User1_AD отображается токен

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> • перейти на вкладку «Пользователи»; • в строке поиска набрать «User1_AD»; • в найденном списке выбрать доменного пользователя User1_AD; • перейти в карточку пользователя; • нажать кнопку «+Выпустить» и в контекстном меню выбрать «Для входа по управляемому сертификату Microsoft»; • выбрать подключенный токен; • нажать кнопку «Далее» и для продолжения нажать кнопку «Применить»; • ввести PIN-код пользователя и нажать кнопку «ОК»; • дождаться окончания выпуска токен для входа по управляемому сертификату и нажать кнопку «Закрыть»; • кликнуть на ячейке «Сертификаты»; • убедиться, что статус сертификата «Действительный»; • закрыть окно «Карточка пользователя» 	с сертификатом.
3	Настройка политики аутентификации	
3.1	<p>От имени и с правами пользователя Администратор на PC1 в консоли администрирования СЗИ:</p> <ul style="list-style-type: none"> • перейти в окно «Менеджер иерархий»; • выбрать сервер безопасности PC1; • перейти на вкладку «Политики»; • выбрать «Политика клиента по умолчанию», Windows; • выбрать вкладку «Управление входом в ОС»; • добавить доменного пользователя «User1_AD»; • в списке пользователей для доменного пользователя «User1_AD» установить флаг разрешить аутентификацию «По токену» и запретить «Аутентификацию Windows»; • перейти на вкладку Linux, «Управление входом в ОС»; • добавить доменного пользователя «User1_AD»; • в списке пользователей для доменного пользователя «User1_AD» установить флаг разрешить «Аутентификацию по токену» и запретить «Аутентификацию ОС»; • сохранить сделанные изменения 	Политика аутентификации создана
4	Проверка аутентификации пользователя по токену с сертификатом	
4.1	Перезагрузить PC4 и подключить токен	Токен подключен
4.2	Войти в ОС PC4 от имени и с правами доменного пользователя User1_AD	Загрузка рабочего стола
4.3	Завершить работу пользователя User1_AD	Выполнен выход пользователя
4.4	Выполнить указанные в пунктах 4.1 – 4.3 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенными выше результатами
5	Выключение токена пользователя	
5.1	<p>От имени и с правами пользователя Администратор войти на PC1 запустить консоль управления СЗИ и выполнить следующие действия:</p> <ul style="list-style-type: none"> • открыть раздел «Управление токенами»; • перейти на вкладку «Пользователи»; 	Токен пользователя временно отключен

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> в строке поиска набрать «User1_AD»; в найденном списке выбрать доменного пользователя User1_AD; нажать кнопку «Выключить»; в открывшемся окне «Выключение устройства» нажать кнопку «Да»; убедиться, что токен пользователя User1_AD временно выключен 	
6	Проверка аутентификации пользователя с временно отозванным токеном содержащим сертификатом	
6.1	От имени и с правами доменного пользователя User1_AD войти в ОС PC4	Ошибка. «Вы не можете войти с данным токеном, т.к. он заблокирован администратором»
6.2	Выполнить указанные в пункте 6.1 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенными выше результатами
7	Отзыв сертификата пользователя	
	От имени и с правами пользователя Администратор войти на PC1, запустить консоль управления СЗИ и выполнить следующие действия:	
7.1	<ul style="list-style-type: none"> открыть раздел «Управление токенами»; перейти на вкладку «Токены»; в списке выбрать доменного пользователя User1_AD; нажать кнопку «Включить»; убедиться, что токен доменного пользователя User1_AD включен;	Токен пользователя включён
	<ul style="list-style-type: none"> Нажать кнопку «Отозвать»; В открывшемся окне «Отзыв устройства» нажать кнопку «Да»; убедиться, что сертификат отозван	Сертификат отозван
8	Проверка аутентификации пользователя с токеном с отозванным сертификатом	
8.1	От имени и с правами доменного пользователя User1_AD войти в ОС PC4	Ошибка. «Вы не можете войти с данным токеном, т.к. он заблокирован администратором»
8.2	Выполнить указанные в пункте 8.1 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Windows/Linux	Совпадение полученных результатов с приведенными выше результатами
9	Проверка нахождения сертификата пользователя User1_AD в каталоге «Отозванных сертификатов»	
9.1	Войти в контроллер домена GIS.LAN от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> загрузить «Центр сертификации» перейдя по ветке «Пуск» - «Все программы» – «Администрирование» – «Центр сертификации»; выбрать сертификат пользователя User1_AD перейдя по ветке «Центр сертификации» - «GIS-SER2008AD-CA» - 	Сертификат пользователя User1_AD находится в списке отозванных

№ п/п	Действия	Ожидаемый результат
	«Отозванные сертификаты»	
10	Просмотр событий аудита	
10.1	Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать сервер СЗИ РС1, вкладку «События» • установить фильтр по категории «Управление жизненным циклом токенов»; • нажать кнопку «Поиск» 	Появление сообщений, фиксирующих Управление жизненным циклом токенов

Критерии оценки:

Результаты проверки считаются положительным, если СЗИ предоставляет возможность двухфакторной аутентификации пользователей с использованием цифровых сертификатов.

2.10.4 Проверка функционирования политики безопасности аутентификации в контроллере домена с использованием СЗИ от НСД «Блокхост-Сеть 4»

Описание проверки:

При использовании СЗИ от НСД «Блокхост-Сеть 4» по варианту поставки № 2, СЗИ реализует собственные политики безопасности на защищаемых ПК в сети, использующей службу каталогов Active Directory для ПК под управлением ОС MS Windows и FreeIPA для ПК под управлением ОС Linux с действующими групповыми политиками.

Цель проверки заключается в том, что при организации защищенного сегмента сети СЗИ выполняет функции по формированию политик безопасности, в частности, политик идентификации и аутентификации, которые в защищенном сегменте сети доминируют над политиками, устанавливаемыми Microsoft Active Directory под управлением ОС MS Windows и FreeIPA под управлением ОС Linux.

Для пользователей СЗИ реализуются отдельные политики безопасности.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблицах ПЗ.51 и ПЗ.52.

Таблица ПЗ.51 – Управление политикой безопасности Microsoft Active Directory через консоль администрирования СЗИ

№	Действия	Ожидаемый результат
1	Войти в контроллер домена с правами «Администратор»	Вход в систему
2	<ul style="list-style-type: none"> • Открыть раздел «Управление групповой политикой»; 	Открыто окно редактора

№	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> Открыть лес доменов (GIS.LAN); Выбрать «Default Domain Policy»; Через контекстное меню выбрать «Редактор управления групповыми политиками»; Перейти по иерархическому списку «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Политики учетных записей» → «Политика паролей» 	групповых политик
3	Изменить параметр политики «Минимальная длина пароля» с установленного по умолчанию значения 7 знаков на 8 знаков	Параметр политики установлен
4	Установить параметр политики «Пароль должен отвечать требованиям сложности» с положения «Включен» в положение «Отключен»	Параметр политики установлен
5	<p>Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия:</p> <ul style="list-style-type: none"> запустить консоль управления СЗИ; открыть «Политику клиента по умолчанию»; выбрать Windows и перейти в «Управление входом в ОС»; на вкладке «Список пользователей» добавить доменного пользователя User1_AD; разрешить доменному пользователю User1_AD тип входа в ОС «Аутентификацию Windows»; выбрать Linux и перейти в «Управление входом в ОС»; на вкладке «Список пользователей» добавить доменного пользователя User1_AD; <p>разрешить доменному пользователю User1_AD тип входа в ОС «Аутентификацию ОС»</p>	Разрешение аутентификации установлено
6	Войти на PC8 (ОС Windows) с правами доменного пользователя User1_AD	Рабочий стол загружен
7	Нажать комбинацию клавиш <Ctrl>+<Alt>+	Появление диалога выбора действий ОС Windows
8	Нажать ссылку «Изменить пароль»	Появление диалога «Смена пароля»
9	<p>Заполнить поля диалога:</p> <ul style="list-style-type: none"> 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». 	Появление сообщения с описанием ошибки смены пароля.
10	<p>Заполнить поля диалога:</p> <ul style="list-style-type: none"> в поле ввода «Старый пароль» ввести текущий пароль; в поле ввода «Новый пароль» ввести новый пароль (длиной 8 символов, но не удовлетворяющий сложности пароля: Буквы/цифры/специальные символы); повторить ввод нового пароля в поле ввода «Подтвердите пароль». 	Появление сообщения с описанием ошибки смены пароля.
11	<p>Заполнить поля диалога:</p> <ul style="list-style-type: none"> в поле ввода «Старый пароль» ввести текущий пароль; в поле ввода «Новый пароль» ввести новый пароль (длиной 8 символов и удовлетворяющий сложности пароля); 	Пароль изменен. Загрузка рабочего стола.

№	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> повторить ввод нового пароля в поле ввода «Подтвердите пароль». 	
12	Войти на РС15 с правами доменного пользователя User1_AD	Рабочий стол загружен
13	Открыть терминал и выполнить терминальную команду passwd. Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 7 символов); повторить ввод нового пароля; нажать клавишу «Enter» 	Появление сообщения с описанием ошибки смены пароля.
14	Еще раз выполнить терминальную команду passwd. Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 8 символов не удовлетворяющий сложности пароля: Буквы\цифры\спец символы); повторить ввод нового пароля; нажать клавишу «Enter» 	Появление сообщения с описанием ошибки смены пароля.
15	Еще раз выполнить терминальную команду passwd. Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 8 символов и удовлетворяющий парольной политике); повторить ввод нового пароля; нажать клавишу «Enter»; выйти из системы 	Пароль изменен.
16	Войти в систему от имени и с правами пользователя User1_AD введя новый пароль пользователя	Вход в систему

Таблица ПЗ.52 – Управление политикой безопасности FreeIPA через консоль администрирования СЗИ

№	Действия	Ожидаемый результат
1	Войти в веб-интерфейс контроллер домена freeipa.local с правами «admin»	Вход в систему
2	Открыть раздел «Политика», «Политики паролей»	Открыто окно редактора групповых политик
3	Изменить параметр политики «Минимальная длина пароля» с установленного по умолчанию значения 7 знаков на 6 знаков	Параметр политики установлен
4	Установить параметр политики «Пароль должен отвечать требованиям сложности» с положения «Включен» в положение «Отключен»	Параметр политики установлен
5	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> запустить консоль управления СЗИ; открыть «Политику клиента по умолчанию»; выбрать Windows и перейти в «Управление входом в ОС»; на вкладке «Список пользователей» добавить доменного пользователя freeipa.local User_IPA; разрешить доменному пользователю User_IPA тип входа в ОС «Аутентификацию Windows»; выбрать Linux и перейти в «Управление входом в ОС»; 	Разрешение аутентификации установлено

№	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> на вкладке «Список пользователей» добавить доменного пользователя freeipa.local User_IPA; разрешить доменному пользователю User_IPA тип входа в ОС «Аутентификацию ОС» 	
6	Войти на РС8 с правами User_IPA домена freeipa.local	Рабочий стол загружен
7	Нажать комбинацию клавиш <Ctrl>+<Alt>+	Появление диалога выбора действий ОС Windows
8	Нажать ссылку «Изменить пароль»	Появление диалога «Смена пароля»
9	Заполнить поля диалога: <ul style="list-style-type: none"> 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». 	Появление сообщения с описанием ошибки смены пароля.
10	Заполнить поля диалога: <ul style="list-style-type: none"> в поле ввода «Старый пароль» ввести текущий пароль; в поле ввода «Новый пароль» ввести новый пароль (длиной 8 символов, но не удовлетворяющий сложности пароля: Буквы\цифры\спец символы); повторить ввод нового пароля в поле ввода «Подтвердите пароль». 	Появление сообщения с описанием ошибки смены пароля.
11	Заполнить поля диалога: <ul style="list-style-type: none"> в поле ввода «Старый пароль» ввести текущий пароль; в поле ввода «Новый пароль» ввести новый пароль (длиной 8 символов и удовлетворяющий сложности пароля); повторить ввод нового пароля в поле ввода «Подтвердите пароль». 	Пароль изменен. Загрузка рабочего стола.
12	Войти на РС15 с правами User_IPA домена freeipa.local	Рабочий стол загружен
13	Открыть терминал и выполнить терминальную команду <code>passwd</code> . Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 7 символов); повторить ввод нового пароля; нажать клавишу «Enter». 	Появление сообщения с описанием ошибки смены пароля.
14	Еще раз выполнить терминальную команду <code>passwd</code> . Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 8 символов не удовлетворяющий сложности пароля: Буквы\цифры\спец символы); повторить ввод нового пароля; нажать клавишу «Enter». 	Появление сообщения с описанием ошибки смены пароля.
15	Еще раз выполнить терминальную команду <code>passwd</code> . Выполнить указанные действия: <ul style="list-style-type: none"> ввести пароль текущего пользователя; ввести новый пароль (длиной 8 символов и удовлетворяющий парольной политике); повторить ввод нового пароля; нажать клавишу «Enter»; 	Пароль изменен.

№	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> выйти из системы 	
16	Выйти из системы и войти в систему от имени и с правами пользователя User_IPA введя новый пароль пользователя	Вход в систему

Критерии оценки:

Результаты проверки считаются положительным, если сервер безопасности СЗИ обеспечивает применение установленной «политики безопасности» для пользователей СЗИ.

2.10.5 Проверка возможности идентификации и аутентификации пользователей в сети с иерархией серверов безопасности без контроллера домена

Описание проверки:

СЗИ от НСД «Блокхост-Сеть 4» реализует возможность идентификации и аутентификации пользователей СЗИ в сети без использования службы каталогов Active Directory, FreeIPA и регистрации событий безопасности связанных с действиями пользователей.

Выполняемые действия:

Для проведения теста необходимо добавление пользователей средствами СЗИ указанных в таблице ПЗ.53 в виртуальной сети, не использующей AD и FreeIPA.

Таблица ПЗ.53 – Список пользователей

№	Имя	Пользователь	Права в ОС	Полномочия в СЗИ	
				Администратор	Аудитор
1	PC1	Test1	Пользователь	-	-
2	PC2	Test2	Пользователь	-	-
3	PC3	Test3	Пользователь	-	-
4	PC4	Test4	Пользователь	-	-
5	PC5	Test5	Пользователь	-	-
6	PC6	Test6	Пользователь	-	-
7	PC7	Test7	Пользователь	-	-
8	PC8	Test8	Пользователь	-	-
9	PC9	Test9	Пользователь	-	-
10	PC10	Test10	Пользователь	-	-
11	PC11	Test11	Пользователь	-	-
12	PC12	Test12	Пользователь	-	-
13	PC13	Test13	Пользователь	-	-
14	PC14	Test14	Пользователь	-	-
15	PC15	Test15	Пользователь	-	-
16	PC16	Test16	Пользователь	-	-
17	PC18	Test18	Пользователь	-	-

Дальнейшие действия, выполняемые при проверке, и ожидаемые результаты приведены в таблице ПЗ.54.

Таблица ПЗ.54 – Действия при проверке аутентификации пользователей СЗИ

№ п/п	Действия	Ожидаемый результат
1	Загрузить виртуальную сеть с иерархией серверов	Виртуальная сеть загружена
2	Войти в ОС на ЭВМ1 от имени и с правами Администратора	Вход в систему
3	Загрузить консоль управления головного сервера безопасности СЗИ	Консоль управления СЗИ
4	Добавить пользователей согласно таблице ПЗ.51 и разрешить тип входа в ОС для добавленных пользователей «Аутентификация Windows» и «Аутентификация ОС»	Пользователи и разрешения добавлены
5	Войти на РС2 от имени и с правами пользователя Test2	Загрузка рабочего стола
6	Войти на РС3 от имени и с правами пользователя Test3	Загрузка рабочего стола
7	Войти на РС4 от имени и с правами пользователя Test4	Загрузка рабочего стола
8	Войти на РС5 от имени и с правами пользователя Test5	Загрузка рабочего стола
9	Войти на РС6 от имени и с правами пользователя Test6	Загрузка рабочего стола
10	Войти на РС7 от имени и с правами пользователя Test7	Загрузка рабочего стола
11	Войти на РС8 от имени и с правами пользователя Test8	Загрузка рабочего стола
12	Войти на РС9 от имени и с правами пользователя Test9	Загрузка рабочего стола
13	Войти на РС10 от имени и с правами пользователя Test10	Загрузка рабочего стола
14	Войти на РС11 от имени и с правами пользователя Test11	Загрузка рабочего стола
15	Войти на РС12 от имени и с правами пользователя Test12	Загрузка рабочего стола
16	Войти на РС13 от имени и с правами пользователя Test13	Загрузка рабочего стола
17	Войти на РС14 от имени и с правами пользователя Test14	Загрузка рабочего стола
18	Войти на РС15 от имени и с правами пользователя Test15	Загрузка рабочего стола
19	Войти на РС16 от имени и с правами пользователя Test16	Загрузка рабочего стола
20	Войти на РС18 от имени и с правами пользователя Test17	Загрузка рабочего стола
21	Войти в ОС на РС1 от имени и с правами Администратора	Вход в систему
22	Запустить консоль «Система развертывания и аудита» и выполнить действия: 1) Перейти в раздел «События»; 2) Установить следующие параметры фильтра: системы- Windows/Linux, тип события – «Управление входом в ОС»; 3) Нажать кнопку «Поиск»	Информация о событиях безопасности загружена

Критерии оценки:

Проверка считается положительной, если:

- СЗИ осуществляет свою аутентификацию пользователя по паролю;
- СЗИ реализует регистрацию событий аутентификации пользователей.

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

Описание проверки:

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

Выполняемые действия:

Проверка выполняется на основании действий, выполняемых в п.п.2.4.1 и 2.10.1 проверки содержания необходимой информации о действиях пользователя.

Критерии оценки:

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

2.11 Проверка регистрации

2.11.1 Проверка регистрации использования идентификационного и аутентификационного механизмов

Описание проверки:

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Проверка выполняется на основании действий, выполненных в п. 2.10.1 и путем проверки журнала, содержащего информацию об идентификации и аутентификации

[72410666.00063-04 95 01-01](#)

пользователей (дата и время, субъект, тип события, успешно ли осуществилось событие).

Критерии оценки:

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).

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

Описание проверки:

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Проверка выполняется после совокупности выполненных действий, описанных в испытаниях:

- п. 2.3.1 «Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа»;
- п. 2.4.1 «Проверка принципа сопоставления классификационных меток каждого

субъекта и каждого объекта при реализации мандатных ПРД»;

- п. 2.3.4 «Проверка контроля запуска процессов по модели разрешенных процессов»;
- п. 2.3.5 «Проверка контроля запуска программ и файлов (аудит доступа к медиафайлам)»;
- п. 2.3.6 «Проверка контроля запуска исполняемого файла по маске его имени (аудит запуска приложений)»;

Дальнейшие действия проверки и ожидаемые результаты приведены в таблице ПЗ.55.

Таблица ПЗ.55 – Действия при проверке регистрации запроса на доступ к защищаемому ресурсу

№ п/п	Действия	Ожидаемый результат
1	Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать сервер СЗИ РС17, вкладку «События»; 3) нажать кнопку «Поиск»	Появление сообщений, фиксирующих произведенные попытки доступа к контролируемому объектам

Критерии оценки:

Результаты проверки считаются положительными, если:

- журнал регистрации событий безопасности содержит информацию о запросах на доступ к защищаемому ресурсу;
- в зарегистрированных событиях регистрируется следующая информация:
 - дата и время;
 - субъект, осуществляющий регистрируемое действие;
 - тип события;
 - успешно ли осуществилось событие (обслужен запрос на доступ или нет).

2.11.3 Проверка регистрации создания и уничтожения объекта

Описание проверки:

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;

- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Проверка выполняется на основании действий, выполненных в п. 2.3.1.

Критерии оценки:

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).

2.11.4 Проверка регистрации действий по изменению ПРД

Описание проверки:

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Проверка выполняется согласно действиям, описанным в испытаниях:

- п. 2.3.1 «Проверка контроля доступа наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.) с использованием дискреционных правил разграничения доступа»;
- п. 2.3.3 «Проверка предоставления прав санкционировано изменять ПРД выделенным субъектам (администрации, службе безопасности и т.д.), в том числе изменения списка пользователей СВТ2»;
- п. 2.4.4 «Проверка возможности изменения классификационных уровней субъектов и объектов специально выделенными субъектами при реализации мандатных ПРД»

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

Критерии оценки:

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).

2.11.5 Проверка наличия средств выборочного ознакомления с регистрационной информацией**Описание проверки:**

СЗИ обеспечивает возможности просмотра и анализа информации о действиях отдельных пользователей.

Механизм регистрации событий безопасности предоставляет пользователю с привилегированной учетной записью и ролью в СЗИ «Аудитор» или «Администратор» возможность просмотра информации о действиях отдельных пользователей.

Пользователю с привилегированной учетной записью и ролью в СЗИ «Аудитор» или «Администратор» предоставляется возможность выборочного просмотра событий безопасности на основе задаваемых критериев.

СЗИ содержит средства выборочного ознакомления с регистрационной информацией.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.56.

Таблица ПЗ.56 – Действия при проверке наличия средств выборочного ознакомления с регистрационной информацией в консоли администрирования СЗИ

№ п/п	Действия	Ожидаемый результат
1	Войти на РС1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) открыть вкладку «События»; 3) нажать кнопку «Поиск»	Отображение сообщений аудита о работе модулей СЗИ.
2	В вкладке «События» последовательно установить фильтры:	
2.1	1) «Типы событий» (в выпадающем списке) выбрать категорию:	
2.1.1	• «Контроль печати». Нажать кнопку «Поиск»,	Отображение сообщений аудита о по категории «Контроль печати»
2.1.2	• «Контроль устройств». Нажать кнопку «Поиск».	Отображение сообщений аудита о по категории «Контроль портов»
2.1.3	Сбросить установленные фильтры.	Фильтры сброшены
2.2	2) «Уровни важности»	
2.2.1	• Установить флаг в строке «Сведения». Нажать кнопку «Поиск».	Отображение сообщений аудита с уровнем важности «Сведения»
2.2.2	• Установить флаг в строке «Предупреждения». • Нажать кнопку «Поиск».	Отображение сообщений аудита с уровнем важности «Предупреждения»
2.2.3	• Установить флаг в строке «Ошибки». Нажать кнопку «Поиск»	Отображение сообщений аудита с уровнем важности «Ошибка»
2.2.4	Очистить установленные фильтры	
2.3	3) «Типы событий»	
2.3.1	В окне «Выбор событий фильтра», установить флаг в строках: • «Локальный вход в систему» из «Управления входом в ОС»; • «Изменение политики» из «Администрирования»; • нажать кнопку «ОК» для сохранения изменений	В окне выбора событий отображены события по типам
2.3.2	Нажать кнопку «Поиск»	Отображение событий по типам событий
2.3.3	Сбросить установленные фильтры	Фильтры сброшены
2.4	4) «Компьютеры»	
2.4.1	На вкладке «События», выполнить следующие действия: • в строке «Компьютеры» нажать кнопку «Выбрать»; • в окне «Выберите компьютеры» установить флаг на РС6; • нажать кнопку «ОК» для сохранения изменений	Отображение событий по выбранным компьютера
2.4.2	Нажать кнопку «Поиск»	Отображение событий по выбранным компьютера

№ п/п	Действия	Ожидаемый результат
2.4.3	Повторить действия с п.2.4.1 по п.2.4.2 (настоящей таблицы) для РС8, РС16	Отображение событий по выбранным компьютера
2.4.4	Сбросить установленные фильтры	Фильтры сброшены
2.5	5) «По подстроке»	
2.5.1	На вкладке «События», выполнить следующие действия: <ul style="list-style-type: none"> • в строке «по подстроке» нажать кнопку «+»; • в поле набрать слово «клиент»; • нажать кнопку «Поиск» 	Отображение событий по содержащие искомый текст
2.5.2	Сбросить установленные фильтры	Фильтры сброшены
2.6	6) «По времени»	
2.6.1	На вкладке «События», выполнить следующие действия: <ul style="list-style-type: none"> • в строке «по времени» нажать кнопку «+»; • установить параметры по времени • нажать кнопку «Поиск» 	Отображение событий по в заданном интервале дат
2.6.2	Сбросить установленные фильтры	Фильтры сброшены
2.7	7) «За последние (дней)»	
2.7.1	На вкладке «События», выполнить следующие действия: <ul style="list-style-type: none"> • в строке «По времени» нажать кнопку «Последние дни»; • в активированном окне выбора дней установить цифру «2»; • нажать кнопку «Поиск» 	Отображение в заданном интервале дней
2.7.2	Сбросить установленные фильтры	Фильтры сброшены
2.7.3	На вкладке «События», выполнить следующие действия: <ul style="list-style-type: none"> • в строке «по времени» нажать кнопку «Период»; • установить флаг в поле «От начала сбора событий» и указать период; • нажать кнопку «Поиск» 	Отображение событий от указанного периода
2.7.4	Сбросить установленные фильтры	Фильтры сброшены
2.7.5	На вкладке «События», выполнить следующие действия: <ul style="list-style-type: none"> • в строке «по времени» нажать кнопку «Период»; • установить флаг в поле «По текущее время» и указать время: До: дата и время; • нажать кнопку «Поиск» 	Отображение событий по текущее время
3	В окне события аудита выбрали пункты и критерии, согласно которым будет выполнена фильтрация. Нажали кнопку «Поиск»	В Основной панели настроек клиентов будут отображены только сообщения, которые отвечают критериям фильтра

Критерии оценки:

Результаты проверки считаются положительными, если:

- СЗИ содержит средства выборочного ознакомления с регистрационной информацией.

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

Описание проверки:

В СЗИ предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

Выполняемые действия:

Проверка выполняется согласно действиям, выполняемым в пп. 2.3.1, 2.4.1 и 2.10.1.1. Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.57.

Таблица ПЗ.57 – Действия при проверке регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.)

№ п/п	Действия	Ожидаемый результат
ОС Windows		
1	Выполнить вход в ОС на РС8 от имени и с правами пользователя Администратор	Загрузка рабочего стола
2	<ul style="list-style-type: none"> • Зарегистрировать локальных пользователей User1 и User2; • Создать на РС8 директорию C:\LogTest с поддиректориями 1 и 2 • Создать файлы: C:\LogTest\1\test1.txt и C:\LogTest\2\test2.txt 	Пользователи, директория и поддиректории с файлами созданы
3	Войти в систему на РС17 от имени и с правами пользователя Администратор и запустить консоль управления СЗИ	Загрузка рабочего стола Выполнен запуск консоли управления
4	На РС17 в консоли управления СЗИ, выбрать РС8, в окне «Настройки» выбрать пункт «Мандатный доступ» . Включить механизм мандатного доступа. Добавить и назначить иерархические мандатные метки с ведением аудита для каталогов: <ul style="list-style-type: none"> • C:\LogTest\1 – мандатную метку 1; • C:\LogTest\2 – мандатную метку 2 	Правила разграничения доступа для мандатного разграничения заданы
5	В окне «Настройки» для пользователя РС8\User1 задать дискреционные ПРД с аудитом: <ul style="list-style-type: none"> • C:\LogTest\1\test1.txt – Просмотр/Изменение; • C:\LogTest\2\test2.txt – Просмотр/Изменение В окне «Настройки» для пользователя РС8\User2 задать дискреционные ПРД с аудитом: <ul style="list-style-type: none"> • C:\LogTest\1\test1.txt – Просмотр/Изменение; • -C:\LogTest\2\test2.txt – -/-. 	Правила разграничения доступа для дискреционного доступа заданы
6	Сохранить произведенные настройки	Сохранение настроек

№ п/п	Действия	Ожидаемый результат
7	Перезагрузить РС8	Появление интерфейса СЗИ от НСД «Блокхост-Сеть 4»
8	Войти в систему от имени и с правами пользователя User1	Загрузка рабочего стола
9	Открыть файл <i>C:\LogTest\1.test1.txt</i>	Открытие файла
10	Открыть файл <i>C:\LogTest\2\test2.txt</i>	Отказано в доступе
11	Выйти из системы или перезагрузить РС8	
12	Войти в систему от имени и с правами User2	Загрузка рабочего стола
13	Открыть файл <i>C:\LogTest\1\test1.txt</i>	Открытие файла
14	Открыть файл <i>C:\LogTest\2\test2.txt</i> .	Отказано в доступе
15	Выйти из системы или перезагрузить РС8	
16	Войти на РС17 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • выбрать сервер РС17, вкладку «События»; • нажать кнопку «Поиск» 	Отображены сведения обо всех действиях пользователей и для каждого события содержит дату и время, субъект, тип, статус
17	Выполнить указанные в пунктах 1–16 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
РЕД ОС (РС18)		
1	Выполнить вход в ОС на РС18 от имени и с правами пользователя Администратор	Загрузка рабочего стола
2	- Зарегистрировать локальных пользователей User1 и User2; - Создать на РС18 директорию <i>~/LogTest</i> с поддиректориями 1 и 2 Создать файлы: - <i>~/LogTest/1/test1.txt</i> ; - <i>~/LogTest/2/test2.txt</i>	Пользователи, директория и поддиректории с файлами созданы
3	Войти в систему на РС17 от имени и с правами пользователя Администратор и запустить консоль управления СЗИ	Загрузка рабочего стола Выполнен запуск консоли управления
4	В окне «Настройки» для пользователя РС18\User1 задать дискреционные ПРД с аудитом: - <i>/LogTest/1/test1.txt</i> – Просмотр/Изменение ; - <i>/LogTest/2/test2.txt</i> – Просмотр/Изменение В окне «Настройки» для пользователя РС18\User2 задать дискреционные ПРД с аудитом: - <i>/LogTest/1/test1.txt</i> – Просмотр/Изменение ; - <i>/LogTest/2/test2.txt</i> – -/- .	Правила разграничения доступа для дискреционного доступа заданы
5	Сохранить произведенные настройки	Сохранение настроек
6	Перезагрузить РС18	Появление интерфейса СЗИ от НСД «Блокхост-Сеть 4»
7	Войти в систему от имени и с правами пользователя User1	Загрузка рабочего стола
8	Открыть файл <i>/LogTest/1.test1.txt</i>	Открытие файла
9	Открыть файл <i>/LogTest/2/test2.txt</i>	Отказано в доступе
10	Выйти из системы или перезагрузить РС18	

№ п/п	Действия	Ожидаемый результат
11	Войти в систему от имени и с правами User2	Загрузка рабочего стола
12	Открыть файл /LogTest/1/test1.txt	Открытие файла
13	Открыть файл /LogTest/2/test2.txt.	Отказано в доступе
14	Выйти из системы или перезагрузить PC18	
15	Войти на PC17 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none">• запустить консоль управления СЗИ;• выбрать PC18, вкладку «События»;• нажать кнопку «Поиск»	Отображены сведения обо всех действиях пользователей и для каждого события содержит дату и время, субъект, тип, статус

Критерии оценки:

Результаты проверки считаются положительными, если СЗИ регистрирует все попытки доступа, все действия оператора и выделенных пользователей (администраторов защиты и т.п.).

2.11.7 Проверка функциональных возможностей механизма регистрации событий безопасности

Проверяемые требования:

СЗИ реализует регистрацию событий:

- вход (выход), а также попытки входа субъектов доступа и загрузки (останова) операционной системы;
- подключение МНИ;
- попытки доступа программных средств к внешним устройствам, программам, томам, каталогам, файлам;
- попытки удаленного входа (по сети).
- регистрируются действия от имени привилегированных учетных записей (администраторов);
- регистрируются события, связанные с изменением привилегий учетных записей.

В СЗИ обеспечивается определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

Состав и содержание событий безопасности приведены в таблице П3.58.

Таблица ПЗ.58 – Состав событий безопасности

№	Наименование	Дата и время события	Результат	Идентификатор субъекта доступа	Протокол доступа	Интерфейс доступа	Спецификация объекта доступа (логическое имя, тип, номер)
1	Регистрации входа (выхода) субъектов доступа и загрузки (останова) операционной системы	+	+	+			
2	Регистрации подключения машинных носителей информации	+		+			
3	Регистрации запуска (завершения) программ и процессов	+	+	+			
4	Регистрации попыток доступа программных средств к защищаемым файлам	+	+	+			+
5	Регистрации попыток доступа программных средств к защищаемым объектам доступа	+	+	+			+
6	Регистрации попыток удаленного доступа	+	+	+	+	+	

СЗИ реализует сбор, запись и хранение информации о событиях безопасности, централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

В случае возникновения сбоев при регистрации событий безопасности СЗИ в режиме реального времени, сигнализирует администраторам о возникших проблемах, сообщениями в журнале событий и странице мониторинга. Иерархия серверов, групп компьютеров оснащена цветовой индикацией.

Администраторы имеют возможность устранить сбой путем изменения параметров сбора.

На странице мониторинга администраторам предоставляется информация с процентными и цифровыми показателями по разделам:

- «Распределение клиентов по типу аутентификации»;
- «Режим работы клиентов»;
- «Состояние клиентов».

В разделе «События для рассмотрения» отражается информация о наличии неактивных шаблонов клиентов и ошибок при синхронизации политик.

СЗИ реализует интеграцию результатов мониторинга (записей регистрации) из разных источников с возможностью передачи в SIEM-систему для последующей корреляции и выявления инцидентов безопасности.

СЗИ реализует синхронизацию меток системного времени, включающих дату и время, используемых для генерации записей регистрации (аудита) событий безопасности.

Защита информации о событиях безопасности реализуется предоставлением доступа к механизму регистрации событий и к его настройке администраторам безопасности.

- обеспечивается резервное копирование записей регистрации (аудита);
- доступ к записям о регистрации событий безопасности (аудиту) предоставляется привилегированным учетным записям с ролью в СЗИ «Аудитор» или «Администратор».

Механизм регистрации событий безопасности предоставляет пользователю с привилегированной учетной записью и ролью в СЗИ «Аудитор» или «Администратор» возможность просмотра информации о действиях отдельных пользователей.

Пользователю с привилегированной учетной записью и ролью в СЗИ «Аудитор» или «Администратор» предоставляется возможность выборочного просмотра событий безопасности на основе задаваемых критериев.

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице П3.59.

Таблица П3.59 – Функциональные возможности консоли «Система развертывания и аудита»

№ п/п	Действия	Ожидаемый результат
1	Войти в систему РС1 от имени и с правами пользователя Администратор	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> запустить консоль управления СЗИ; выбрать PC1; «Политики», «Политика сервера по умолчанию», «Доступ к серверу»; добавить пользователя Admin с разрешениями на «Просмотр» и «Изменение»; сохранить сделанные изменения; выйти из консоли управления СЗИ 	
2	Запустить консоль управления на PC1 от имени и с правами пользователя Admin с разрешениями на «Просмотр» и «Изменение»	Загрузка консоли управления
3	Определение списка событий, подлежащих регистрации	
3.1	<ul style="list-style-type: none"> запустить консоль управления СЗИ; выбрать PC1; «Политики», «Политика сервера по умолчанию», «Сбор событий по иерархии», «Windows/Linux»; нажать кнопку «Выбрать все» и кнопку «Проставить все»; сохранить сделанные изменения 	Список регистрируемых событий сформирован
3.2	Войти на PC17 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> запустить консоль управления СЗИ; выбрать PC17; «Политики», «Политика сервера по умолчанию», «Сбор событий по иерархии», «Windows/Linux»; убедиться, что политика сбора событий аудита применена 	Применение политики сбора аудита на подчинённых серверах безопасности
4	Настройка автоархивации событий	
4.1	Войти на корневой сервер безопасности I уровня PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> запустить консоль управления СЗИ; в окне «Менеджер иерархии» выбрать PC1; перейти в вкладку «Настройки»; выбрать раздел «Автоархивация событий»; включить тумблер «Механизм включён»; включить флаг «Перемещать события в архив» - «только события, старше (дни)» - 30 дней; указать каталог для «Создать архивы событий в каталоге»; сохранить сделанные изменения. 	Параметры автоархивации заданы
4.2	Перевести системное время на 29 дней вперед	Установлено время на 29 дней вперед
4.3	Проверить наличие записей о событиях безопасности	Наличие записей о событиях безопасности
4.4	Перевести системное время на 30 дней вперед	Установлено время на 30 дней вперед
4.5	Проверить наличие созданного архива записей о событиях безопасности	Наличие архива записей о событиях безопасности
5	Централизованная загрузка событий безопасности	
5.1	Войти на корневой сервер безопасности I уровня PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> запустить консоль управления СЗИ; 	Информация о событиях безопасности загружена

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> в окне «Менеджер иерархии» выбрать РС1; через контекстное меню выбрать команду «Запустить внеплановую загрузку событий аудита» – «с клиентских компьютеров»; через контекстное меню выбрать команду «Запустить внеплановую загрузку событий аудита» – «С подчинённых серверов». 	
5.2	Зафиксировать время запуска	Консоль запущена
5.3	<ul style="list-style-type: none"> повторить «внеплановую загрузку» зарегистрированных событий безопасности; выбрать категорию событий «События сервера СЗИ»; нажать кнопку «Поиск»; закрыть консоль управления СЗИ 	Время события и время, зарегистрированное в журнале аудита идентично
5.4	Перевести системное время на РС1 на 1 час вперед	Изменено системное время на 1 час вперед
5.5	Запустить консоль управления СЗИ и зафиксировать время запуска	Консоль запущена
5.6	<ol style="list-style-type: none"> Повторить внеплановую загрузку событий аудита с подчиненных серверов и с клиентских компьютеров; Перейти во вкладку «События»; Выбрать тип событий «События сервера СЗИ»; Нажать кнопку «Поиск» 	Время события и время, зарегистрированное в журнале аудита идентично
6	Архивирование информации о событиях безопасности	
5.1	В консоли консоль управления СЗИ выполнить действия: <ol style="list-style-type: none"> Перейти в раздел «Архивы»; Нажать кнопку «Выбрать»; Выбрать файл архива. Нажать кнопку «Выполнить запрос» 	Информация о событиях безопасности загружена из выбранного архива
7	Определение состава событий безопасности	
7.1	<ol style="list-style-type: none"> В загруженных событиях безопасности отобразить события, соответствующие критериям: <ul style="list-style-type: none"> регистрации входа (выхода) субъектов доступа и загрузки (останова) операционной системы; регистрации подключения машинных носителей информации; регистрации запуска (завершения) программ и процессов; регистрации попыток доступа программных средств к защищаемым файлам; регистрации попыток доступа программных средств к защищаемым объектам доступа; регистрации попыток удаленного доступа. Двойным щелчком мыши открыть окно «Подробная информация» 	Состав событий безопасности соответствует требуемым
8	Мониторинг	
8.1	Войти на корневой сервер безопасности I уровня РС1 от имени и справками пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none"> запустить консоль управления СЗИ; в окне «Менеджер иерархии» выбрать РС1; 	Во вкладках отражается информация с цифровыми показателями по категориям

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none">перейти на вкладку «Статистика»	
8.2	Войти в систему РС2 от имени и с правами пользователя Admin с ролью в СЗИ «Администратор»	Загрузка рабочего стола
8.3	Перейти с «Панель управления» – «Администрирование» – «Службы». Остановить службу аудита изделия «GIS.Client.AuditSystem»	Служба «GIS.Client.AuditSystem» выключена
8.4	Войти на сервер безопасности I уровня РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: <ul style="list-style-type: none">запустить консоль управления СЗИ;в окне «Менеджер иерархии» выбрать РС1;перейти в раздел «События»;нажать кнопку «Поиск»	Убедиться, что в разделе события отображается событие об остановке механизма сбора событий безопасности.
9	Повторить указанные действия консоли управления на других операционных системах	Ожидаемые результаты совпадают

Критерии оценки:

Результаты проверки считаются положительными, если:

- в механизме архивации реализована возможность сбора событий безопасности во временном диапазоне;
- СЗИ реализует синхронизацию меток системного времени;
- содержание и состав событий безопасности соответствуют требуемым;
- механизм регистрации событий безопасности реализует централизованный сбор, управление сбором и хранение информации;
- на вкладке «События» отражается сводная статистика;
- СЗИ реализует возможность реагирования на события безопасности;
- СЗИ обеспечивает выдачу предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации.

2.11.8 Проверка аудита событий, возникающих при задании/изменении настроек аудита

Проверяемые требования:

СЗИ должно осуществлять следующие функции аудита:

- сбор сообщений аудита;
- регистрацию сообщений аудита в журнал аудита (на клиентах СЗИ, клиенте управления и СБ СЗИ);
- чтение сообщений аудита из журнала аудита (из БД аудита на СБ СЗИ);
- фильтрацию событий безопасности при выборке записей из журнала аудита по

заданным параметрам (из БД аудита на СБ СЗИ);

- передачу сообщений аудита из БД аудита ПК на СБ СЗИ.

При регистрации сообщений аудита в журнале аудита в каждое сообщение аудита должны добавляться «метки точного времени», полученные от внутренних системных часов на ПК.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.60.

Таблица ПЗ.60 – Функциональные возможности подсистемы развертывания и аудита»

№ п/п	Действия	Ожидаемый результат
1	Войти в систему РС1 от имени и с правами пользователя Admin с ролью в СЗИ «Администратор» и «Аудитор»	Загрузка рабочего стола
2	Изменение списка событий, подлежащих регистрации	
2.1	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС1; «Политики», «Политика сервера по умолчанию», «Сбор событий по иерархии», «Windows/Linux»; 3) Снять флаги с событий «Контроль устройств»; 4) Применить сделанные изменения	Список регистрируемых событий изменён
3	Проверка регистрации изменении настроек аудита	
3.1	Перейти во вкладку «События» и нажать кнопку «Поиск»	Информация о событиях безопасности загружена в категории «Действия Администратора СЗИ» отображается событие «Изменения параметров работы СЗИ».

Критерии оценки:

Результаты проверок считаются положительными, если СЗИ регистрирует событие «Изменение параметров работы СЗИ».

2.11.9 Проверка регистрации в автономном варианте СЗИ от НСД «Блокхост-Сеть 4»

Настройка СЗИ в автономном варианте осуществляется через «Консоль клиента Блокхост-Сеть 4».

Механизм регистрации событий безопасности в автономном варианте (вариант использования №1) и в варианте с удалённым управлением (вариант использования

№2) реализован идентично.

Описание функций изложено в пунктах:

- п. 2.11.1 «Проверка регистрации использования идентификационного и аутентификационного механизмов»;
- п. 2.11.2 «Проверка регистрации запроса на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)»;
- п. 2.11.3 «Проверка регистрации создания и уничтожения объекта»;
- п. 2.11.4 «Проверка регистрации действий по изменению ПРД»;
- п. 2.11.5 «Проверка наличия средств выборочного ознакомления с регистрационной информацией»;
- п. 2.11.6 «Проверка регистрации всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).»

Описание проверки:

СЗИ осуществляет регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выполняемые действия:

Перед проведением проверок автономного варианта необходимо перевести его из сетевого режима в автономный. Для этого достаточно отключить сетевой интерфейс у сервера безопасности.

При проведении вышеуказанных проверок выполняются аналогичные действия с учетом функциональных особенностей автономного варианта СЗИ.

Для просмотра журнала аудита СЗИ от НСД «Блокхост-Сеть 4» потребуется перейти

по цепочке «Панель управления» – «Администрирование» – «Просмотр событий».

Журнал аудита «Блокхост-Сеть» находится в каталоге «Журнал приложений и служб».

Критерии оценки:

Результаты проверок считаются положительными, если они совпадают с изложенными в выше перечисленных тестах.

2.11.10 Проверка передачи собранных событий безопасности с головного сервера СЗИ в SIEM-систему

Описание проверки:

СЗИ обеспечивает передачу собранных СЗИ данных аудита (событий безопасности), получаемых от каждого ПК ИС, на внешнюю программную систему («ANKEY SIEM»), осуществляющую сбор, регистрацию и хранение всех данных аудита, возникающих в ИС, которая защищена СЗИ.

Процесс сбора и передачи собранных СЗИ данных аудита, осуществляется по многоуровневой иерархии серверов безопасности СЗИ, развернутых в корпоративной сети защищаемой ИС.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.61.

Таблица ПЗ.61 – Действия при проверке передачи событий безопасности в SIEM-систему

№ п/п	Действия	Ожидаемый результат
1	Запустить виртуальную тестовую среду	Виртуальные ЭВМ запущены
2	Настройка головного сервера безопасности БХС	
2.1	Войти на РС1 от имени и с правами пользователя Администратор	Загрузка рабочего стола
2.2.	Выполнить следующие действия: <ul style="list-style-type: none"> • запустить консоль управления СЗИ; • в окне «Менеджер иерархий» выбрать РС1; • выбрать меню «Настройки», «Экспорт событий в SIEM»; включить тумблер «Передавать события аудита»;	Параметры установлены. Активны поля: <ul style="list-style-type: none"> • IP-адрес SIEM сервера, • Порт SIEM сервера, • Протокол.
2.3	<ul style="list-style-type: none"> • установить параметры подключения к SIEM-системе; • нажать кнопку «События...»; • выбрать все и нажать кнопку «Ок»; • сохранить выполненные изменения 	Параметры установлены, все события выбраны
3	Настройка представления активного канала в консоли SIEM-системы	
3.1	Запустить в браузере пользовательский веб-интерфейс Ankey	Авторизация успешна

№ п/п	Действия	Ожидаемый результат
	SIEM NG	
3.1.1	В окне авторизации ввести данные для входа	
4	Проверка передачи событий аудита от головного сервера БХС в SIEM-систему	
4.1	Перейти на «Все события»	События безопасности отображаются в SIEM-системе

Критерии оценки:

Проверка считается успешной если, осуществляется передача событий аудита вверх по иерархии серверов вплоть до головного сервера с последующей передачей в SIEM-систему.

2.12 Проверка надежного восстановления

2.12.1 Проверка полного восстановления свойств СЗИ от НСД «Блокхост-Сеть 4» после сбоев и отказов оборудования при использовании процедур восстановления

Описание проверки:

СЗИ обеспечивает восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения.

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

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.62.

Таблица ПЗ.62 – Действия при проверке полного восстановления свойств СЗИ от НСД «Блокхост-Сеть 4» после сбоев и отказов оборудования при использовании процедур восстановления

№ п/п	Действия	Ожидаемый результат
1	Включить РС1	Появление интерфейса СЗИ
2	Войти в систему от имени и с правами Администратор	Загрузка рабочего стола
3	Проверить работоспособность СЗИ	Механизмы защиты СЗИ функционируют
4	Выключить питания РС1 и включить ее вновь для имитирования отказа оборудования	Появление интерфейса СЗИ
5	Войти в систему от имени и с правами	Загрузка рабочего стола

№ п/п	Действия	Ожидаемый результат
	пользователя Администратор	
6	Проверить работоспособность СЗИ	Механизмы защиты СЗИ функционируют
7	Выполнить указанные в пунктах 1 – 6 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех установленных операционных систем	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка процедуры надежного восстановления считается успешной, если:

- в результате ее применения произошло полное восстановление свойств СЗИ.

2.13 Проверка целостности СЗИ от НСД «Блокхост-Сеть 4»

Контроль целостности СЗИ от НСД «Блокхост-Сеть 4» осуществляется:

- на уровне аппаратной среды;
- на уровне среды функционирования;
- на уровне доступа к файлам.

2.13.1 Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4»

Описание проверки:

СЗИ осуществляет проверку целостности программных компонентов СЗИ, а также выполнять надежное восстановление поврежденных программных компонентов СЗИ, используя эталонные файлы СЗИ.

В СЗИ реализован контроль целостности программных модулей СЗИ, не подлежащих изменению в процессе функционирования СЗИ.

Проверка целостности программных компонентов СЗИ осуществляется при помощи расчета контрольных сумм программных модулей СЗИ и их сравнения с эталонным значением в защищенной ветке реестра на ПК. Расчет контрольных сумм программных модулей СЗИ должен выполняться с помощью алгоритма вычисления хеша SHA1.

При обнаружении нарушений контрольных сумм программных компонентов, СЗИ выполняет автоматическое восстановление программных модулей из резервных копий, без привлечения администратора безопасности.

Реализуется контроль целостности по контрольным суммам в процессе загрузки и динамически в процессе работы для:

- программного обеспечения;
- компонентов программного обеспечения;

- программного обеспечения СЗИ.

Контроль целостности СЗИ выполняется по контрольным суммам всех компонентов СЗИ, в процессе загрузки и динамически в процессе работы.

Реализуется блокировка автоматизированного рабочего места, сервера, в случае обнаружения нарушения контроля целостности программного обеспечения.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.63.

Таблица ПЗ.63 – Действия при проверке наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4»

№ п/п	Действия	Ожидаемый результат
1	Периодический контроль целостности СЗИ после перезагрузки ОС (Windows)	
1.1	Войти в систему на PC2 от имени и с правами Администратора	Загрузка рабочего стола
1.2	Создать документ C:\test.txt с произвольным содержимым	Документ создан и сохранен на диск
1.3	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать PC2; 3) перейти на вкладку «Настройки»; 4) выбрать «Контроль целостности файлов с восстановлением»; 5) включить тумблер «Механизм включен»; 6) ввести период проверки, каждые 5 мин.; 7) установить флаг в поле «Формировать события аудита при нарушении целостности файлов» «Блокировать сессию пользователя, если не удалось восстановить файл»	Механизм контроля целостности включен и установлена периодичность контроля равная 5 мин.
1.4	Добавить «Контролируемые файлы» , для этого нажать кнопку «+» и добавить следующий файл для контроля целостности и восстановления: C:\ test.txt	Файл поставлен на контроль.
1.5	Сохранить произведенные настройки	Изменения сохранены
1.6	Войти в систему на PC2, от имени пользователя, с правами Администратора	Загрузка операционной системы
1.7	Внести изменения в файл: C:\ test.txt и сохранить изменения	Изменения внесены и сохранены
1.8	Перезагрузить PC2 и войти в систему от имени пользователя, с правами администратора	Загрузка операционной системы
1.9	Открыть файл C:\ test.txt и убедиться, что файл восстановлен	В файле не содержатся внесенных изменений
2	Периодический контроль целостности во время сеанса работы	
2.1	Войти в систему на PC2 от имени и с правами пользователя User1	Загрузка рабочего стола
2.2	Выполнить следующие действия 1) Внести изменения в файл test.txt, 2) Подождать 5 минут	Изменения внесены и сохранены

№ п/п	Действия	Ожидаемый результат
	3) Открыть файл test.txt и убедиться, что файл восстановлен	В файле не содержится внесенных изменений
2.3	Войти на PC1 от имени и справками пользователя Администратор и выполнить следующие действия: 1) Запустить консоль управления СЗИ; 2) Выбрать PC2; 3) Перейти на вкладку «События»; 4) Выбрать тип событий «Контроль целостности файлов»; 5) Нажать кнопку «Поиск»	Наличие событий о нарушении целостности файла и события об успешном восстановлении
2.4	Выполнить указанные в пунктах 1.1 – 2.3 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами
3	Периодический контроль целостности файлов (Linux)	
3.1	Войти в систему на PC18 от имени и с правами Администратора	Загрузка рабочего стола
3.2	Создать файл test1 с произвольным содержимым	Документ создан и сохранен на диск
3.3	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать «Все компьютеры» в «Менеджере иерархий»; 3) убедиться в наличии построения иерархии серверов и доступности PC18 (при необходимости создать иерархию серверов и добавить PC18); 4) перейти на вкладку «Политики» и открыть для изменения «Политику клиента по умолчанию»; 5) в окне «Изменение клиентской политики: Политика клиента по умолчанию», выбрать последовательно Linux и «Контроль целостности файлов»; 6) включить тумблер «Механизм включен»; 7) выбрать вкладку «Настройки» и задать интервал выполнения построения отчета каждые 5 минут; 8) установить флаг на «Формировать события аудита при обнаружении изменения файлов»; 9) перейти на вкладку «Файлы и исключения» и добавить следующий файл на контроль: test1	Механизм контроля целостности включен и установлена периодичность контроля равная 5 мин. Файл поставлен на контроль.
3.4	Сохранить произведенные настройки	Изменения сохранены
3.5	Войти на PC18 от имени пользователя, с правами Администратора	Загрузка рабочего стола
3.6	Открыть файловый менеджер и внести произвольные изменения в файл: test1; Сохранить внесенные изменения в файл	Изменения внесены и сохранены
3.7	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) в окне «Менеджер иерархий» выбрать PC18; 3) перейти на вкладку «События»; 4) установить следующие параметры фильтра: • Системы – Linux; • Уровни важности – Все уровни;	Наличие зарегистрированных событий о внесении изменений в файл

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none"> Типы событий: Контроль целостности файлов; По времени: За последние (Дней) – 1. Выполнить «Поиск»; 5) убедиться в наличии зарегистрированных событий, об изменении файла	
3.8	Выполнить указанные в пунктах 3.1 – 3.7 действия на рабочих станциях для всех остальных установленных операционных систем Linux	Совпадение полученных результатов с приведенными выше результатами
4	Управление механизмом контроля целостности файлов из локальной консоли управления (Linux)	
4.1	Включить рабочую станцию PC18 и загрузить операционную систему от имени пользователя user	Загружена ОС
4.2	Убедитесь, что локальная консоль управления не находится под управлением сервера (при необходимости отключить механизм управления локальной консолью управления сервером)	Убедились, что редактирование доступно
4.3	Загрузить локальную консоль управления от имени и с правами Администратора	Загружена локальная консоль
4.4	Запустить терминал на рабочей станции PC18 и создать каталог test с файлами test1.txt и test2.txt с произвольным содержимым	Каталог и файлы созданы
4.5	Открыть локальную консоль управления от имени и с правами Администратора и выполнить следующие действия: <ol style="list-style-type: none"> перейти на вкладку «Контроль целостности файлов»; включить механизм КЦ файлов, установив переключатель в положение «Механизм контроля целостности включен»; перейти на вкладку «Файлы и исключения» и добавить на контроль целостности файлы, созданные в п.4.4 настоящей таблицы; перейти на вкладку «Настройки»: <ul style="list-style-type: none"> задать периодичность построения отчета каждые 5 минут; установить галочку на поле «Формировать события аудита при обнаружении изменения файлов»; перейти на вкладку «Отчет» и убедиться, что в нем отображаются все файлы, установленные на контроль; сохранить выполненные изменения 	Механизм КЦ файлов включен Файлы для КЦ добавлены
4.6	На рабочей станции PC18 от имени пользователя user выполнить следующие действия: <ul style="list-style-type: none"> в файл test1.txt внести произвольные изменения; удалить файл test2.txt 	Изменения выполнены
4.7	Открыть локальную консоль управления от имени и с правами Администратора и выполнить следующие действия: <ul style="list-style-type: none"> перейти во вкладку «Контроль целостности файлов» и далее на вкладку «Отчет»; установить переключатель в положение «Только нарушения»; перестроить отчет; 	Убедились, что в отчете отображен статус всех изменений

№ п/п	Действия	Ожидаемый результат
	<ul style="list-style-type: none">убедиться, что в отчете отображен статус всех изменений, выполненных в п.4.6 настоящей таблицы.	
4.8	<ul style="list-style-type: none">перейти на вкладку «События аудита»;выбрать период: «День»;обновить события;убедиться, что в журнале событий аудита отображены все изменения, выполненные в п. 4.6 настоящей таблицы.	Убедились, что в журнале событий аудита отображены все изменения, выполненные в п. 4.7 настоящей таблицы
4.9	Выполнить указанные в пунктах 4.1 – 4.8 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех установленных операционных систем Linux	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка считается успешной, если:

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

2.13.2 Проверка наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4» с блокировкой доступа пользователя при нарушении целостности**Проверяемые требования:**

Реализуется контроль целостности по контрольным суммам в процессе загрузки и динамически в процессе работы для:

- программного обеспечения;
- компонентов программного обеспечения;
- программного обеспечения СЗИ.

Контроль целостности СЗИ выполняется по контрольным суммам всех компонентов СЗИ, в процессе загрузки и динамически в процессе работы.

Реализуется блокировка автоматизированного рабочего места, сервера, в случае обнаружения нарушения контроля целостности программного обеспечения.

В СЗИ предусмотрены средства периодического контроля за целостностью программной и информационной части СЗИ.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.64.

Таблица ПЗ.64 – Действия при проверке наличия периодического контроля целостности СЗИ от НСД «Блокхост-Сеть 4» с блокировкой доступа пользователя при нарушении целостности

№ п/п	Действия	Ожидаемый результат
	Периодический контроль целостности СЗИ с блокировкой пользователя после перезагрузки ОС	
1	Войти в РС2 от имени и с правами пользователя Администратор	Загрузка рабочего стола
2	Создать документ test.txt с произвольным содержимым	Документ создан и сохранен на диск
3	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС2; 3) выбрать вкладку «Настройки», «Контроль целостности файлов с восстановлением»; 4) включить тумблер «Механизм включен»; 5) установить флаг «Блокировать сессию пользователя, если не удалось восстановить файл»; 6) задать интервал выполнения построения отчета каждые 5 минут; 7) в окне «Контролируемые файлы» добавить файл - test.txt; 8) сохранить выполненные изменения	Механизм контроля целостности включен, установлена периодичность контроля равная 5 мин. и установлено блокирование сеанса пользователя
4	Перезагрузить РС2	Загрузка операционной системы
5	Войти на РС2 от имени и с правами пользователя Администратор и внести изменения в файл: - test.txt и сохранить изменения. Изменения наступят через пять минут после внесения.	Изменения внесены и сохранены
6	Отобразить права на изменения/запись на файл test.txt.	Доступно только чтение файла.
7	Перезагрузить РС2	Загрузка операционной системы
8	Попытка входа в систему РС2 пользователем User1	Вход в систему заблокирован, нарушена целостность файла
	Периодический контроль целостности СЗИ с блокировкой пользователя во время сеанса работы	
9	Войти в систему на РС2 от имени и с правами пользователя Администратор	Загрузка рабочего стола
10	Вернуть права на изменения/запись на файл test.txt	Восстановлен полный доступ к файлу
11	Войти на РС2 от имени и с правами пользователя User1 , и внести изменение в файл test.txt.	Изменения внесены и сохранены
12	Установить для файла test.txt атрибут «Только чтение»	Права на действия с файлом ограничены
13	Ожидание установленного времени Периодичности контроля равное 5 минутам	Сеанс работы пользователя прерывается.

№ п/п	Действия	Ожидаемый результат
14	Попытка входа в систему PC2 пользователем User1	Вход в систему заблокирован, не удалось восстановить целостность критичных файлов
15	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать PC2; 3) открыть вкладку «События»; 4) выбрать тип событий «Контроль целостности файлов»; 5) нажать кнопку «Поиск»; 6) убедиться в наличии событий о нарушении целостности файла, о невозможности восстановить файл из резервной копии и отказе на вход пользователя	Наличие записей о нарушении целостности файла, о невозможности восстановить файл из резервной копии и отказе на вход пользователя
16	Выполнить указанные в пунктах 1 – 15 действия на рабочих станциях ЭВМ2 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

Проверка считается успешной, если:

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

2.13.3 Проверка регистрации событий, связанных с изменением целостности среды

Проверяемые требования:

Механизм контроля программной среды СЗИ отслеживает установку и удаление на ПК следующих видов программных компонентов:

- программ (приложений);
- служб;
- драйверов.

СЗИ осуществляет контроль изменений каталогов общего доступа на защищаемых ПК. АБ может выполнять включение или выключение контроля целостности каталогов общего доступа на выбранном ПК.

При обнаружении нарушений контроля целостности программно-аппаратной среды, в системном журнале СЗИ регистрируется соответствующее событие аудита об изменении:

- аппаратной среды;
- перечня каталогов общего доступа;

а также при установке/удалении:

- драйверов;
- служб;
- программ.

Загрузка и выполнение прикладного программного обеспечения, поддерживающего возможность «тихой» (скрытой) установки, с доступных для чтения МНИ и контроль целостности данного ПО.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.65.

Таблица ПЗ.65 – Проверка контроля целостности среды

№ п/п	Действия	Ожидаемый результат
1	Настройки целостности среды	
1.1	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС1; 3) перейти на вкладку «Политики»; 4) открыть «Политику клиента по умолчанию»; 5) выбрать Windows, «Контроль целостности среды»; 6) на вкладке «Контроль целостности среды» установить флаги на параметрах контроля: • «Аппаратной среды»; • «Изменения перечня каталогов общего доступа»; • «Установки/удаления драйверов»; • «Установки/удаления служб»; • «Установки/удаления программ»; 7) сохранить сделанные изменения	Политика контроля целостности среды установлена
2	Проверка регистрации событий безопасности	
2.1	Перезагрузить РС2	Загрузка операционной системы
2.2	Войти в систему от имени и с правами Admin и установить драйвер для Tokena	Драйвер установлен
2.3	Создать папку общего доступа	Папка общего доступа создана
2.4	Удалить драйвер для Tokena	Драйвер удален
2.5	Отключить папку общего доступа	Папка общего доступа отключена

2.6	Войти на РС1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать РС1; 3) выбрать вкладку «События»; 4) выбрать тип событий «Контроль целостности среды»; 5) нажать кнопку «Поиск»; 6) убедиться в появлении событий об установке и удалении приложения, об изменении перечня каталогов общего доступа	Появление сообщений, об установке и удалении приложения, а также об изменении перечня каталогов общего доступа
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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

2.13.4 Проверка регистрации событий, связанных с изменением аппаратной среды

Описание проверки:

СЗИ осуществляет контроль за изменениями состава аппаратных средств и установленного программного обеспечения на защищаемых ПК.

СЗИ осуществляет контроль за изменениями состава аппаратных устройств, отслеживая изменения по списку установленных на контроль аппаратных средств на ПК.

При последующих загрузках клиента СЗИ на ПК, СЗИ отслеживает изменения состава аппаратных устройств, установленных на ПК, сравнивая их идентификационную информацию с идентификационной информацией, хранящейся в эталонном списке аппаратных устройств.

СЗИ осуществляет контроль за изменениями состава программного обеспечения, отслеживая изменения файлов по списку программных компонентов на ПК.

Выполняемые действия:

Выполняемые при проверке действия и ожидаемые результаты приведены в таблице ПЗ.66.

Таблица ПЗ.66 – Проверка контроля аппаратной среды

№ п/п	Действия	Ожидаемый результат
1	Настройки целостности среды	
1.1	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: 1) запустить консоль управления СЗИ; 2) выбрать PC1; 3) перейти на вкладку «Политики»; 4) открыть «Политику клиента по умолчанию»; 5) выбрать Windows, «Контроль целостности среды»; 6) на вкладке «Контроль целостности среды» установить флаги на параметрах контроля: • «Аппаратной среды»; 7) сохранить выполненные изменения	Политика контроля целостности среды установлена
2	Проверка	
2.1	отключить станцию PC2	PC2 отключена
2.2	Подключить в PC2 новый CD-ROM	Новое устройство подключено
2.3	Запустить PC2 и войти в систему пользователем User1	PC2 включена, загрузка ОС
2.4	Войти на PC1 от имени и с правами пользователя Администратор и выполнить следующие действия: • запустить консоль управления СЗИ; • выбрать PC1; • выбрать вкладку «События»; • выбрать тип событий «Контроль целостности среды»; • нажать кнопку «Поиск»; • убедиться в появлении событий об отсутствии изменения аппаратной среды	Появление сообщений, фиксирующих о целостности аппаратной среды
3	Выполнить указанные в пунктах 1 – 2 действия на рабочих станциях ЭВМ1 – ЭВМ5 для всех остальных установленных операционных систем MS Windows	Совпадение полученных результатов с приведенными выше результатами

Критерии оценки:

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

2.14 Проверки работы с токенами (управление ЖЦ токенов)

Описание проверки:

СЗИ предоставляет возможность АБ СЗИ управления (администрирования) ЖЦ токенов пользователей на защищаемых ПК, а также на СБ СЗИ.

СЗИ обеспечивает хранение списка токенов пользователей в БД СЗИ и возможность работы с ним АБ СЗИ. Учет токенов в списке должен осуществляться по их серийным номерам.

СЗИ осуществляет контроль состояний ЖЦ токенов:

- для входа по управляемому сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенным средствами подсистемы управления токенами);
- для входа по стороннему сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенным сторонними средствами);
- для безопасного входа по паролю (при использовании токена для аутентификации по паролю, записанному на устройство);
- для учета.

Приведены процедуры проверки работы с токенами (управления ЖЦ токенов), в соответствии с требованиями, приведенными в Технических условиях ТУ 58.29.40-063-72410666-2019 п. 1.2.16.15.

Проверка выпуска токена для безопасного входа по паролю выполнена в п. 2.10.1.1 «Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов».

Проверка выпуска токена для входа по сертификату выполнена в п. 2.10.3 «Проверка возможности аутентификации пользователей с использованием цифровых сертификатов».

Выполняемые действия:

Проверка (просмотр) состояний ЖЦ токена для входа по паролю представлена в таблице ПЗ.67.

Таблица ПЗ.67 – Проверка (просмотр) состояний ЖЦ токена для входа по паролю

№	Действия	Ожидаемый результат
1	Войти в систему РС1 от имени и с правами пользователя Admin	Загрузка рабочего стола пользователя Admin
2	Запустить консоль управления СЗИ	Открытие консоли администрирования СЗИ
3	Вставить токен в USB-порт на РС1. Посмотреть в диспетчере устройств Windows или при помощи собственного клиента драйвера, что устройство в рабочем состоянии	Устройство в рабочем состоянии
4	Выбрать пункт меню «Управление токенами» → пункт «Токены»	Просмотреть список токенов
5	Выбрать токен в списке	Просмотреть сведения о состоянии токене (перечень состояний приведен в таблице 6.7)
6	Выбрать «История токенов»	Просмотреть сведения о выпущенных Актах токена в списке Актов
7	Выбрать токен и через контекстное меню нажать «Просмотреть»	Просмотреть Акт токена
8	Закрыть Консоль СЗИ	Загрузка рабочего стола пользователя Admin

№	Действия	Ожидаемый результат
9	Завершить сеанс работы пользователя Admin	Завершение работы ОС

Проверка (просмотр) состояний ЖЦ токена для входа по сертификату представлена в таблице ПЗ.68.

Таблица ПЗ.68 – Проверка (просмотр) состояний ЖЦ токена для входа по сертификату

№	Действия	Ожидаемый результат
1	Войти в систему PC1 от имени и с правами пользователя Admin	Загрузка рабочего стола пользователя Admin
2	Запустить консоль сервера СЗИ	Открытие консоли администрирования СЗИ
3	Вставить токен в USB-порт на PC1. Посмотреть в диспетчере устройств Windows или при помощи собственного клиента драйвера, что устройство в рабочем состоянии	Устройство в рабочем состоянии
4	Выбрать пункт меню «Управление токенами», пункт «токены»	Просмотреть список токенов
5	Выбрать токен в списке	Просмотреть сведения о состоянии токене (перечень состояний приведен в таблице 6.8)
6	Выбрать «Историю актов»	Просмотреть сведения о выпущенных Актах токена в списке Актов
7	Выбрать разрешенное действие для выбранного токена	
8	Закрыть Консоль СЗИ	Загрузка рабочего стола пользователя Admin
9	Завершить сеанс работы пользователя Admin	Завершение работы Windows

Проверка возможности просмотра сертификатов на токене представлена в таблице ПЗ.69.

Таблица ПЗ.69 – Проверка (просмотр) сертификатов на токене

№	Действия	Ожидаемый результат
1	Войти в систему PC1 от имени и с правами пользователя Admin	Загрузка рабочего стола пользователя Admin
2	Запустить консоль сервера СЗИ	Открытие консоли администрирования СЗИ
3	Вставить токен в USB-порт на PC1. Посмотреть в диспетчере устройств Windows или при помощи собственного клиента драйвера, что устройство в рабочем состоянии	Устройство в рабочем состоянии
4	Выбрать пункт меню «Управление токенами» → «токены»	Просмотреть список состояния токен
5	В списке подключенных токенов выбрать токен	Просмотреть общие сведения о выбранном токене
5.1	<ul style="list-style-type: none"> кликнуть на ячейке «Сертификаты»; в открывшемся окне «просмотр содержимого Token», нажать кнопку «Подробнее» и просмотреть сертификат. 	Просмотр установленного сертификата
6	Закрыть Консоль СЗИ	Загрузка рабочего стола пользователя Admin
7	Завершить сеанс работы пользователя Admin	Завершение работы Windows

Перечень статусов ЖЦ токенов и доступные действия АБ СЗИ по управлению ЖЦ токенов представлены в таблице ПЗ.70.

Таблица ПЗ.70 – Состояния ЖЦ токенов и доступные действия АБ СЗИ по управлению ЖЦ токенов

№	Состояние	Описание состояния токена	Возможные действия
1	Не зарегистрирован	Подключен напрямую к ПК, но не зарегистрирован в СЗИ	- Добавление и регистрация токена в СЗИ
2	Зарегистрирован	Добавлен в СЗИ	- Назначение токена пользователю - Удаление токена из СЗИ
3	Используется	Назначен пользователю	- Синхронизация данных токена - Вывод токена из использования

Перечень состояния типов использования токенов приведен в таблице ПЗ.71.

Таблица ПЗ.71 – Состояния ЖЦ токенов, содержащих сертификат, и доступные действия АБ СЗИ по управлению ЖЦ токенов

№	Состояние	Описание состояния токена	Доступные действия с токеном
1	Не зарегистрирован	Подключен напрямую к ПК, но не зарегистрирован в СЗИ	- Добавление и регистрация токена в СЗИ
2	Зарегистрирован	Токен добавлен в СЗИ	- Назначение токена пользователю - Удаление токена из СЗИ
3	Используется	Токен назначен пользователю	- Приостановка использования токена (временное отключение) - Синхронизация данных на токене - Вывод токена из использования
4	Выключен	Использование токена временно приостановлено. Токен остается закреплен за пользователем.	- Возобновление использования токена - Синхронизация данных на токене - Вывод токена из использования
5	Отозван	Токен выведен из использования. Отозванный токен остается закреплен за пользователем.	- Возврат токена в эксплуатацию (токен можно вернуть в эксплуатацию с записью новых сертификатов)
6	Изъят	Токен изъят из эксплуатации. Привязка к пользователю удаляется и токен становится доступен для назначения.	- Доступен для назначения (токен можно вернуть в эксплуатацию с назначением пользователю и записью новых сертификатов)

Возможные действия АБ с токенами описаны в таблице ПЗ.72.

Таблица ПЗ.72 – Возможные действия АБ СЗИ с токенами в СЗИ

№	Действие	Описание действия
1	Добавление токена в СЗИ	Добавление токена в БД СЗИ с присвоением инвентарного номера (регистрации токена в СЗИ). АБ СЗИ может присваивать и изменять инвентарные номера токенов
2	Привязка токена к пользователю	Привязка или отвязка токена к пользователю при назначении токена пользователю или изъятии из обращения

3	Инициализация токена	При инициализации, все данные на токене удаляются (выполняется при вводе в эксплуатацию токена)
4	Создание профиля токена в СЗИ	АБ СЗИ может создавать и изменять в БД СЗИ профили для различных типов токенов
5	Запись (удаление) сертификатов на токене.	Создание и запись новых сертификатов на токен. (при назначении токена). Удаление сертификатов с токена. (при отзыве токена)
6	Синхронизация сертификатов на токене	Удаление старых сертификатов на токене, создание и запись новых сертификатов на токен. (Токен должен быть назначен пользователю (в состоянии Используется) или его использование приостановлено (в состоянии Выключен))
7	Удаление токена из СЗИ	Удаление токена из БД СЗИ. При удалении, токен должен быть в состоянии Изъят с отвязанным пользователем

Перечень возможных состояний сертификатов приведен в таблице ПЗ.73.

Таблица ПЗ.73 – Перечень возможных состояний сертификата

№	Состояние сертификата	Описание состояния сертификата
1	Действительный	Срок действия сертификата не истек. Сертификат пригоден для использования
2	Отозван	Сертификат отозван окончательно и более не пригоден для использования. Окончательный отзыв происходит в результате отзыва устройства или его изъятия.
3	Временно отозван	Действие сертификата приостанавливается на период выключения устройства. После включения устройства сертификат снова становится действительным.
4	Истекает	Срок действия сертификата подходит к концу. Необходимо выполнить обновление сертификата, если планируется его дальнейшее использование
5	Истек	Срок действия сертификата закончился. Сертификат не пригоден для использования.
6	Ошибка	Состояние сертификата не удалось определить. Центр сертификации недоступен. Сертификат не пригоден для использования