

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

Руководство администратора безопасности

Часть 1. Управление политиками

Санкт-Петербург, 2024

### Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» (далее по тексту – СЗИ от НСД «Блокхост-Сеть 4», СЗИ или средство).

В документе приведены назначение и состав СЗИ, реализованные функции защиты, сведения об аппаратных и программных требованиях для установки СЗИ; описаны интерфейс СЗИ и основные приемы работы с ним, порядок управления подчиненными серверами, группами и клиентскими рабочими станциями, настройка клиентских и серверных политик безопасности.

Важнейшей частью документа являются разделы по настройке СЗИ: построение иерархии серверов, групп и клиентских рабочих станций в сети, настройка параметров серверов и клиентских рабочих станций и т.д.

GIS ГАЗИНФОРМ СЕРВИС

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

### Содержание

Введен	ие	6
1	Назначение, задачи и состав СЗИ от НСД «Блокхост-Сеть 4»	7
1.1	Назначение СЗИ от НСД «Блокхост-Сеть 4»	7
1.2	Состав СЗИ от НСД «Блокхост-Сеть 4»	8
2	Условия применения СЗИ от НСД «Блокхост-Сеть 4»	. 11
2.1	Требования к программной и аппаратной конфигурации	.11
2.2	Пакеты для функционирования СЗИ под управлением ОС Linux	.13
2.3	Изменение уровня контроля UAC	. 14
2.4	Отключение запуска консоли восстановления ОС	. 15
2.5	Устранение проблем совместимости с антивирусным ПО	. 18
2.6	Постановка на КЦ программных модулей СЗИ в ОС Linux	.19
3	Основные элементы интерфейса	. 21
4	Общие принципы работы	. 24
4.1	Управление иерархией	.24
4.2	Общее описание политик	. 30
4.3	Принудительное наследование	.31
4.4	Пересечение прав	.43
5	Вкладка «Общее»	. 47
6	Управление политиками	. 51
6.1	Создание политик	.51
6.2	Назначение политик группе	. 53
6.3	Изменение политик	. 56
6.4	Удаление политик	. 57
6.5	Экспорт/импорт политик	. 58
6.6	Примеры наследования политик	.61
6.7	Синхронизация политик	.64
7	Описание клиентских политик	. 66
7.1	Управление входом в OC Windows	.68
7.2	Сложность паролей	.81
7.3	Контроль устройств	.83
7.4	Очистка оперативной памяти	.92



	СЕРВИС СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками	4
7.5	Гарантированное удаление файлов	94
7.6	Аудит целостности файлов	95
7.7	Аудит запуска приложений	97
7.8	Аудит печати	
7.9	Аудит доступа к медиафайлам	
7.10	Контроль целостности среды	101
7.11	Журнал аудита	103
7.12	Управление входом в ОС Linux	104
7.13	Сложность паролей в ОС Linux	111
7.14	Контроль устройств в ОС Linux	114
7.15	Контроль целостности файлов в ОС Linux	124
7.16	Очистка оперативной памяти в ОС Linux	134
7.17	Мягкий режим работы	140
8	Описание серверных политик	
8.1	Доступ к серверу	142
8.2	Пароли и сессии	146
8.3	Сбор событий по иерархии	147
9	Описание политик SafeNode System Loader	154
9.1	Настройка входа	155
9.2	Управление аутентификацией	156
9.3	Сложность пароля	165
9.4	Контроль целостности	167
9.5	Настройки подключения к домену	
9.6	Сетевой адаптер UEFI	
9.7	Мягкий режим работы СДЗ «SafeNode System Loader»	
10	Настройки сервера	189
10.1	Резервные копии	190
10.2	Автоархивация событий	200
10.3	Кеш событий	202
10.4	Построение иерархии серверов	203
10.5	Экспорт событий в SIEM	212
11	Настройки клиента	216
11.1	Дискреционный доступ	218



	СЕРВИС СЗИ ОГНОД «БЛОКХОСТ-СЕТБ 4» Руководство администратора безопасности. Ч Управление политиками	асть 1 5
11.2	Замкнутая программная среда	
11.3	Контроль печати	231
11.4	Контроль целостности файлов с восстановлением	
11.5	Мандатный доступ	
11.6	Проверка пароля в СЗИ	
11.7	Пользователи с разрешением на вход в ОС	
11.8	Пользователи СДЗ	
11.9	Сетевой адаптер UEFI	
11.10	) Проверка пароля в SafeNode	
11.11	1 Пользователи с разрешением на вход в ОС	
Переч	чень сокращений	

СЗИ от НСД «Блокхост-Сеть 4»



### Введение

СЗИ от НСД «Блокхост-Сеть 4» является программным средством защиты информации от несанкционированного доступа к информации, предназначенным для комплексной И многофункциональной защиты информационно-программных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных компьютеров (ПК) под Windows управлением (OC)Microsoft операционных систем 2008R2/7/8.1/2012/2012R2/10/11/2016/2019/2022, Astra Linux Special Edition (Смоленск), Альт 8 СП, РЕД ОС 7.3 Муром.

СЗИ от НСД «Блокхост-Сеть 4» содержит клиентскую часть, которая устанавливается на клиентские рабочие станции под управлением ОС MS Windows/Linux (РЕД ОС), клиента управления, который устанавливается на ПК под управлением сертифицированной ОС Linux (Astra Linux SE, Альт 8 СП)<sup>1</sup>, серверную часть, которая устанавливается на серверы безопасности под управлением ОС MS Windows/Linux, и консоль управления, которая устанавливается на рабочее место администратора в ОС MS Windows/Linux.

Степени важности примечаний:



#### Важная информация

Указания, требующие особого внимания.



### Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

<sup>&</sup>lt;sup>1</sup> Функциональные возможности клиента управления под управлением OC Linux (Astra Linux SE, Альт 8 СП) ограничены возможностью управления входом в ОС и двухфакторной аутентификацией пользователей при входе в ОС при помощи персональных электронных идентификаторов, в т.ч. с использованием цифровых сертификатов пользователей, хранящихся на них; возможностью контроля целостности файлов и гарантированным удалением по требованию.

### 1 Назначение, задачи и состав СЗИ от НСД «Блокхост-Сеть 4»

### 1.1 Назначение СЗИ от НСД «Блокхост-Сеть 4»

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть **4**» является программным средством защиты информации OT несанкционированного доступа к информации, предназначенным для комплексной и многофункциональной защиты информационно-программных ресурсов OT несанкционированного доступа при работе В многопользовательских автоматизированных системах на базе персональных компьютеров под управлением OC Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/11/2016/2019/2022, Astra Linux Special Edition (Смоленск), Альт 8 СП, РЕД ОС 7.3 Муром.

Реализованные в СЗИ от НСД «Блокхост-Сеть 4» механизмы защиты информации позволяют администратору безопасности решать следующие задачи:

- усиление защиты от несанкционированного доступа в систему;
- разграничение доступа пользователей к ресурсам;
- обеспечение гарантированного удаления информации;
- разграничение доступа к запуску программ;
- контроль целостности объектов файловой системы;
- очистка памяти после завершения работы приложений;
- контроль вывода информации на печать, маркировка документов;
- разграничение доступа пользователей к администрированию СЗИ;
- просмотр информационных сообщений СЗИ в ходе работы;

– контроль событий, связанных с безопасностью защищаемой информации.

Для обеспечения безопасности защищаемой информации администратор безопасности обязан:

 осуществить настройку СЗИ от НСД «Блокхост-Сеть 4» в соответствии с данным руководством (настройка заключается в формировании серверных и клиентских политик безопасности по всей иерархии подчиненных серверов, групп и рабочих станций в сети);

– выполнять аудит информационной безопасности по всей иерархии подчиненных серверов, групп и рабочих станций в сети (ведение оперативного контроля событий для выявления ошибок в настройках СЗИ и корректировки правил разграничения доступа, а также для своевременного реагирования на осуществление НСД к защищаемой информации).



### 1.2 Состав СЗИ от НСД «Блокхост-Сеть 4»

Для СЗИ в зависимости от приобретаемой лицензии возможны два варианта использования:

– вариант №1 - автономный вариант СЗИ, при котором СЗИ устанавливается на ПК под управлением ОС MS Windows и используется локально;

– вариант №2 - вариант с удаленным управлением СЗИ, при котором клиентские части СЗИ устанавливаются на ПК под управлением ОС MS Windows/Linux (РЕД ОС), клиент управления устанавливается на ПК под управлением сертифицированной ОС Linux (Astra Linux SE, Альт 8 СП) и работают под управлением серверной части СЗИ установленной на сервер безопасности под управлением ОС MS Windows/Linux. В состав установки клиента управления/клиента под управлением ОС Linux включается консоль управления клиентом.

В состав варианта №1 входят консоль управления, серверная и клиентская части СЗИ, функционирующие на одном ПК под управлением ОС MS Windows. Сетевой режим работы для данного варианта использования невозможен и ограничен автономной лицензией.

В состав варианта №2 входят:

– клиентская часть СЗИ от НСД «Блокхост-Сеть 4», которая устанавливается на клиентские рабочие станции под управлением ОС MS Windows/Linux (РЕД ОС);

– серверная часть СЗИ от НСД «Блокхост-Сеть 4», которая устанавливается на серверы безопасности под управлением ОС MS Windows/Linux,

– клиент управления, который устанавливается на рабочую станцию под управлением сертифицированной ОС Linux (Astra Linux SE, Альт 8 СП);

 консоль управления, которая устанавливается на рабочее место администратора под управлением ОС MS Windows/Linux и позволяет управлять развертыванием СЗИ на клиентах, подключением клиентских частей к серверной части и настройками сбора событий безопасности.

**Для управления клиентскими рабочими станциями** администратору безопасности доступны следующие механизмы защиты:

идентификация аутентификация администратора безопасности И И пользователей, работающих на ПК с СЗИ от НСД «Блокхост-Сеть 4», в том числе с применением персональных электронных идентификаторов (перечень поддерживаемых персональных электронных идентификаторов приведен в таблице 3.1 документа «СЗИ от НСД «Блокхост-сеть 4. Описание применения») с возможностью взаимодействия со службами каталогов (Microsoft Active Directory, Samba AD, ALD Pro и FreeIPA);

возможность двухфакторной аутентификации пользователей средствами СЗИ,
 при входе в ОС с использованием цифровых сертификатов пользователей

(сертификаты могут храниться на вышеуказанных персональных электронных идентификаторах) с возможностью взаимодействия со службами каталогов (Microsoft Active Directory и FreeIPA);

– аудит и регистрация событий безопасности при обращении к защищаемым ресурсам ПК;

– контроль устройств (съемные USB-устройства; CD/DVD-устройства; устройства, подключаемые через СОМ- и LPT-порты) на защищаемых ПК;

контроль целостности и восстановления СЗИ при сбоях;

 контроль прав доступа пользователей к защищаемым ресурсам на ПК с использованием дискреционного принципа контроля доступа;

 контроль прав доступа пользователей к защищаемым ресурсам на ПК с использованием мандатного принципа контроля доступа;

 контроль запуска установленных программ, служб/драйверов; отслеживание изменений перечня каталогов общего доступа, контроль аппаратной среды на защищаемых ПК;

– очистку остаточной информации при удалении файловых объектов на жестких дисках и в оперативной памяти на защищаемых ПК;

контроль целостности файлов на защищаемых ПК;

контроль исполняемых файлов и медиафайлов на защищаемых ПК;

 контроль печати документов, с возможностью маркировки документов при печати;

– управление и администрирование СЗИ при помощи настроек безопасности клиентской части СЗИ, хранящихся в БД настроек безопасности на ПК;

 возможность обеспечения управлением персональными электронными идентификаторами пользователя (токенами) на протяжении всего жизненного цикла;

– возможность обеспечения управлением параметрами механизмов защиты (управление входом, управление аутентификацией локальных и доменных пользователей, управление сложностью паролей, контроль целостности) средства доверенной загрузки «SafeNode System Loader» на клиентских рабочих станциях.

Настройки серверной части СЗИ позволяют выполнять следующие функции:

 централизованное удаленное управление и администрирование подчиненных серверов, групп и клиентских рабочих станций в сети;

 управление настройками безопасности и передача настроек безопасности по всей иерархии в БД настроек подчиненных серверов и клиентских рабочих станций;

– централизованный сбор событий аудита, определенных администратором безопасности, по всей иерархии подчиненных серверов, групп и клиентских рабочих



станций вплоть до головного сервера с последующей передачей в SIEM;

– управление персональными электронными идентификаторами пользователя (токенами) на протяжении всего жизненного цикла для пользователей служб каталогов Microsoft Active Directory и Samba AD DC для клиентов под управлением OC MS Windows и Microsoft Active Directory, Samba AD DC, ALD Pro и FreeIPA для клиента управления под управлением сертифицированной OC Linux (Astra Linux SE, Альт 8 СП) и клиента под управлением РЕД ОС;

 сбор данных о правах мандатного доступа пользователей, при входе пользователей на ПК;

 управление параметрами механизмов защиты (управление входом, управление аутентификацией локальных и доменных пользователей, управление сложностью паролей, контроль целостности) средства доверенной загрузки «SafeNode System Loader» на клиентских рабочих станциях;

Возможность управления клиентом управления СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС семейства Linux (Astra Linux SE, Альт 8 СП) ограничена. Для клиентов управления СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС семейства Linux доступны следующие функциональные возможности:

 идентификация и аутентификация администратора безопасности и пользователей, работающих на защищаемых ПК, в том числе с применением персональных электронных идентификаторов, с возможностью взаимодействия со службами каталогов (Microsoft Active Directory, Samba AD DC, ALD Pro и FreeIPA);

 возможность двухфакторной аутентификацией пользователей средствами СЗИ при входе в ОС, при помощи персональных электронных идентификаторов, в том числе с использованием цифровых сертификатов пользователей, расположенных на персональных электронных идентификаторах, с возможностью взаимодействия со службами каталогов (Microsoft Active Directory и FreeIPA);

 возможность обеспечения управлением персональными электронными идентификаторами пользователя (токенами) на протяжении всего жизненного цикла;

 возможность обеспечения управлением параметрами механизмов защиты (управление входом, управление аутентификацией локальных и доменных пользователей, управление сложностью паролей, контроль целостности) средства доверенной загрузки «SafeNode System Loader»;

контроль целостности файлов на защищаемых ПК;

 гарантированное удаление выбранных объектов файловой системы по требованию пользователя с носителей информации (за исключением оптических) без возможности их дальнейшего восстановления на защищаемых ПК.

Механизмы защиты информации, реализующие функциональные возможности безопасности СЗИ описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Описание применения».

#### 72410666.00063-04 95 01-01

# 2 Условия применения СЗИ от НСД «Блокхост-Сеть 4»

### 2.1 Требования к программной и аппаратной конфигурации

СЗИ от НСД «Блокхост-Сеть 4» устанавливается на ПК с процессорами, имеющими архитектуру x86 и AMD64. Поддерживаемые ОС, под управлением которых функционирует СЗИ, приведены в таблице 2.1.

Таблица 2.1 – Перечень поддерживаемых операционных систем

00
MS Windows
Windows Server 2008R2 Foundation Edition SP1 (64-разрядная)
Windows Server 2008R2 Standard Edition SP1 (64-разрядная)
Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная)
Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная)
Windows Server 2012/2012R2 Foundation (64-разрядная)
Windows Server 2012/2012R2 Essentials (64-разрядная)
Windows Server 2012/2012R2 Standard (64-разрядная)
Windows Server 2012/2012R2 Datacenter (64-разрядная)
Windows Server 2016 Standard (64-разрядная)
Windows Server 2016 Datacenter (64-разрядная)
Windows Server 2016 Essentials (64-разрядная)
Windows Server 2019 (64-разрядная)
Windows Server 2022 Standard (64-разрядная)
Windows Server 2022 Essentials (64-разрядная)
Windows Server 2022 Datacenter (64-разрядная)
Windows 7 Professional SP1 (32-разрядная/64-разрядная)
Windows 7 Enterprise SP1 (32-разрядная/64-разрядная
Windows 7 Ultimate SP1 (32-разрядная/64-разрядная)
Windows 8.1 Core (32-разрядная/64-разрядная)
Windows 8.1 Professional (32-разрядная/64-разрядная)
Windows 8.1 Enterprise (32-разрядная/64-разрядная)
Windows 10 Home (32-разрядная/64-разрядная)
Windows 10 Pro (32-разрядная/64-разрядная)
Windows 10 Enterprise (32-разрядная/64-разрядная)
Windows 11 Home (64-разрядная)
Windows 11 Professional (64-разрядная)
Linux
AstraLinux SE (Смоленск)
Альт 8СП
РЕД ОС 7.3 Муром

Программные и аппаратные требования к средствам вычислительной техники, на



которых функционирует клиентская и серверная часть СЗИ приведены в таблице 2.2.

Таблица 2.2 – Программные и аппаратные требования к средствам вычислительной техники, на которых функционирует клиентская и серверная часть СЗИ

Требования	Наименование	Примечание	
Требования к	Обусловлены требованиями		
производительности	используемых ОС	см. таолицу 2.т	
	Использование персональных иден	тификаторов	
Ашаратные треоования	USB-порт		
	Обновления		
	KB3033929, KB4474419, KB4490628	для OC Windows 7 и Windows Server 2008/2008R2	
	KB2921916	в OC Windows 7 и Windows Server 2008/2008R2 для механизма «Контроль печати»	
	Реализация аутентификации с	использованием ГОСТ	
	сертификатов – КриптоПро <sup>2</sup>		
	СКЗИ «КриптоПро CSP»	версии 3.6 и выше	
	Драйверы токенов		
	Драйверы устройств		
	производителей		
	Программная платформа		
	распространяемый пакет Microsoft		
	Visual C++ 2015-2019 Redistributable		
Дополнительное программное обеспечение	NET Framework 4.5.2	При использовании подсистемы ГУПТ	
	обновление «Remote Server Administration Tools»: • для OC Windows 7 "Remote Server Administration Tools for Windows 7" (https://www.microsoft.com/en- us/download/details.aspx?id=7887); • для OC Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (https://www.microsoft.com/en- us/download/details.aspx?id=28972); для OC Windows 10 до версии 1903 "Remote Server Administration Tools for Windows 10" (https://www.microsoft.com/en- us/download/details.aspx?id=45520).	При использовании подсистемы управления токенами на клиентских ОС	
Системы управления базами	СУБД «PostgreSQL»		
данных (СУБД)	СУБД «Jatoba»	Сертификат соответствия ФСТЭК России № 4327 от 19.11.2020	

<sup>&</sup>lt;sup>2</sup> При использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

Ограничения при эксплуатации СЗИ от НСД «Блокхост-Сеть 4» описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Описание применения».

## 2.2 Пакеты для функционирования СЗИ под управлением OC Linux

Перед установкой серверной части СЗИ от НСД «Блокхост-Сеть 4», агента развертывания, клиента Блокхост-Сеть или консоли управления, необходимо убедиться, что на рабочей станции под управлением ОС Linux установлены следующие пакеты:

	Сторонние зависимости, наличие которых	Сторонние зависимости,
Пакет СЗИ ОТ НСД	должен обеспечить администратор для	устанавливаемые вместе с
«DJIOKXOCI-CEIB 4»	полноценной работы пакета	пакетом автоматически
		libxcb-xinerama0
		libpq5
Серверная частв	-	ldap-utils
		libsasl2-modules-gssapi-mit
	libxcb-xinerama0	
Клиентская часть	Idap-utils	-
	libsasl2-modules-gssapi-mit	
	libxcb-xinerama0	
Консоль	Idap-utils	-
	libsasl2-modules-gssapi-mit	
Подсистема	libych vinerama(	
развертывания		-
Подсистема		_
аутентификации	-	-

- для OC AstraLinux SE (Смоленск):

для ОС Альт 8 СП:

	Сторонние зависимости, наличие которых	Сторонние зависимости,
Пакет Сой ОГПОД	должен обеспечить администратор для	устанавливаемые вместе с
«DIIOKXUCI-CEIB 4»	полноценной работы пакета	пакетом автоматически
		libxcbutil-image
		libxcbutil-icccm
Серверная часть	-	libxcbutil-keysyms
		libxcb-render-util
		openIdap-clients
	libxcbutil-image	
	libxcbutil-icccm	
Клиентская часть	libxcbutil-keysyms	-
	libxcb-render-util	
	openIdap-clients	
	libxcbutil-image	
	libxcbutil-icccm	
Консоль	libxcbutil-keysyms	-
	libxcb-render-util	
	openIdap-clients	
Подсистема	libxcbutil-image	
развертывания	libxcbutil-icccm	-



Пакет СЗИ от НСЛ	Сторонние зависимости, наличие которых	Сторонние зависимости,
«Блокуост-Соть Д»	должен обеспечить администратор для	устанавливаемые вместе с
«DIIOKAUCI-CEIB 4»	полноценной работы пакета	пакетом автоматически
	libxcbutil-keysyms	
	libxcb-render-util	
Подсистема		
аутентификации	-	-

### для ОС РЕД ОС 7.3 Муром:

	Сторонние зависимости, наличие которых	Сторонние зависимости,
Пакет Сэй от нод	должен обеспечить администратор для	устанавливаемые вместе с
«DJIOKXOCI-CEIB 4»	полноценной работы пакета	пакетом автоматически
		xcb-util-image
		xcb-util-wm
Серверная часть	-	xcb-util-keysyms
		xcb-util-renderutil
		openIdap-clients
	xcb-util-image	
	xcb-util-wm	
Клиентская часть	xcb-util-keysyms	-
	xcb-util-renderutil	
	openIdap-clients	
	xcb-util-image	
	xcb-util-wm	
Консоль	xcb-util-keysyms	-
	xcb-util-renderutil	
	openIdap-clients	
	xcb-util-image	
Подсистема	xcb-util-wm	
развертывания	xcb-util-keysyms	-
	xcb-util-renderutil	
Подсистема		_
аутентификации	-	-

### 2.3 Изменение уровня контроля UAC

В некоторых случаях для корректного функционирования СЗИ необходимо понизить уровень контроля учетных записей (UAC) в ОС Windows (вплоть до полного отключения) (рисунок 2.1). Для изменения параметров UAC необходимо войти в ОС под учетной записью встроенного администратора.



15



Рисунок 2.1 – Изменение уровня контроля UAC

### 2.4 Отключение запуска консоли восстановления ОС

Для группового отключения среды восстановления ОС Windows на рабочих станциях (предварительно на рабочих станциях должны быть установлены агенты развертывания) администратору необходимо выполнить следующие действия:

1) На сервере СЗИ от НСД «Блокхост-Сеть 4» с помощью текстового редактора создать bat-файл с названием *reagent.bat*, в котором необходимо указать команду отключения среды восстановления и сохранить изменения в файле:

REAGENTC.EXE /disable.

 Перейти в раздел «Развертывание» во вкладку Задачи и, нажав кнопку выбрать пункт Удаление программы (рисунок 2.2).

C	<b>i</b>  S	Базинформ Сервис	C: Py Vr	ВИ от НСД «Блокхост-С ководство администра правление политиками	Сеть 4» атора б	> безопасности.	Часть 1	16
	🗙 Бло	окхост-Сеть 4					- 0	ı ×
	\$	Развёртывание						
	кţл	Агенты Пакеты установки	Задачи					
		+ 🖉 Изменить 🗑 Удалить 🗅	Запустить 🚍 Все резул	ьтаты				C
	70	коря Установка агента развертывания		≜ Тип ОС	С Ста			
	=	🔄 Установка программы	ренной загрузки SafeNode Syst	е установка программы	3		6 C214	
		👿 Удаление программы		поиск компьютеров	0	ПОИСК КОМПЫ	отеров без СЗИ	
		Перезагрузка компьютеров				Тип залачи:	поиск компьютеров без СЗИ	
		> Выполнение скрипта		удаление программы	0	тип задачи.	поиск компьютеров оез сэм	
		😹 Взятие под управление	е по требованию 4.4.16789.2989	00 удаление программы W	ï o	OU:	1	
		🗟 Поиск компьютеров без СЗИ		установка программы W	ï o	Статус:	ожидает выполнения	
		Настройка входа по сертификатам	зания 4.4.18233.31334	установка агента раз Li.	o	Планировщик:	 Ручной	

Рисунок 2.2 – Создание задачи на удаление программы

3) В открывшемся окне мастера создания задачи на удаление программы выбрать подзадачу **Выполнение скрипта для удаления программы** (рисунок 2.3) и нажать кнопку **Далее**.

🗙 Мастер создания задачи на удаление программы	×
Выберите тип задачи	
🔿 Удаление Блокхост-Сеть Клиент	
🔘 Удаление программы из списка инсталляционных пакетов (только для msi-инсталляторов)	
🖲 Выполнение скрипта для удаления программы	
🔘 Удаление модуля аутентификации (только Linux машины)	
Далее	Отмена

Рисунок 2.3 – Выбор типа задачи

4) В открывшемся окне выбрать созданный файл *reagent.bat*, нажать *Далее* (рисунок 2.4).



17

🔀 Мастер создания задачи на удаление программы		×
Выберите файл скрипта		
Выберите файл скрипта, содержащий команды для выполнения на клиенте. Поддерживаются bat и ps1 скрипты.		
Файл скрипта:		
C:\Users\Administrator\Documents\reagent.bat		Изменить
Параметры командной строки файла скрипта (опционально):		
Отмена	Назад	Далее

Рисунок 2.4 – Выбор файла скрипта

5) В следующем окне (рисунок 2.5) выбрать из списка все рабочие станции на которых предполагается запуск скрипта для отключения среды восстановления ОС Windows и нажать **Далее**.

💢 Мастер создания задачи на удаление программы				×
Выберите компьютеры				
Q. Поиск			C	3
🖋 Выбрать всё 🔲 Снять всё				
Имя 🔺 IP-адрес Версия ОС				
🗹 🗐 10.72.18.129 Windows 7 SP1 32-bit				
Всего: 1 Отмечено: 1				
	Отмена	Назад	Далее	

Рисунок 2.5 – Выбор рабочих станций

6) На следующих шагах мастера создания задачи на удаление программы необходимо отредактировать:

 параметры планировщика запуска задачи и определить интервалы времени выполнения задачи;

– параметры перезагрузки рабочей станции.

Более подробно процесс создания задачи на удаление программы описан в пункте 6.3 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

7) После успешного редактирования всех необходимых параметров, необходимо ввести имя создаваемой задачи и нажать кнопку **Создать**.

В зависимости от установленных параметров планировщика запуск задачи на удаление программ с рабочих станций осуществляется автоматически или вручную. Для запуска созданной задачи вручную необходимо выделить созданную задачу в списке, и в открывшейся панели нажать кнопку **Запустить**.

# 2.5 Устранение проблем совместимости с антивирусным ПО

Для устранения проблем совместимости СЗИ от НСД «Блокхост-Сеть 4» с «Kaspersky Security for Windows Server» необходимо добавить в исключения папку *C:\Blockhost* в компоненте *«Проверка при старте операционной системы»*.

Для этого необходимо выполнить следующие действия:

1) Выполнить запуск консоли «Kaspersky Security for Windows Server».

2) Выбрать «Проверка по требованию» → «Проверка при старте операционной системы».

3) Перейти по ссылке «Свойства» во вкладку «Общие».

- 4) Выбрать «Применять доверенную зону».
- 5) Перейти по ссылке «доверенная зона» и нажать «Добавить».

6) Выбрать «Проверяемый объект» → «Диск, папка или сетевой объект».

7) Выбрать папку *C:\Blockhost* и установить следующие флаги: «Учитывать подпапки», «Постоянная защита файлов», «Проверка по требованию».

Для устранения проблем совместимости СЗИ от НСД «Блокхост-Сеть 4» с «DrWeb» на время установки СЗИ от НСД «Блокхост-Сеть 4» необходимо установить разрешение «Конфигурация безопасного режима» (рисунок 2.6).



WDIWEB			Ади	инистрирова	ние Ант	иварусн
нтивирусная сеть > pc9164.da.lan	> Windows	5 > Превентивная защита ☆				
<ul> <li>Выбранные объекты</li> </ul>	×					
• Общие		pc9164.da.lan. Заданы персональные настройк	н.			
• Графики		Общие				
<ul> <li>Идентификаторы безопасности</li> </ul>						•
• Компоненты защиты		иномравать на клинение неавторизованного кода	•			
• Карантин		Уровень блокировки подозрительных действий				
<ul> <li>Оборудование и программы</li> </ul>		Пользовательский			-	*
• Обнаруженные устройства						
• Сессии пользователен		Зашишаемый объект	Разрешать	Спрашиват	ь Запрец	ать
Статистика		Целостность запушенных приложений				
• Угрозы			-	-	-	
• Ошибки		Целостность файлов пользователей			~	
<ul> <li>Сводные данные</li> </ul>		Файл HOSTS	$\checkmark$			
<ul> <li>Статистика сканирования</li> </ul>		Низкоуровневый доступ к диску				
• Запуск/Завершение		Parameter and Annual		-	_	
• Статистика угроз		Загрузка драиверов				
• Состояние		Параметры запуска приложений (IFEO)	$\checkmark$			
• задания		Драйверы мультимедийных устройств				
• Заолокированные устроиства		Параметры оболочки Winlogon				
• Вирусные базы			-	-	-	
<ul> <li>Дисковое пространство</li> </ul>		Нотификаторы Winlogon				
• Модули		Автозапуск оболочки Windows			~	
<ul> <li>События Превентивной защиты</li> </ul>		Ассоциации исполняемых файлов			~	
<ul> <li>События Контроля приложений</li> </ul>		Политики опранцивния записка просонии (СОВ)		_	-	
• Инсталляции Агентов		Hommund of parameterior samyora hoo para (see)				
• Деянсталляция Агентов		Плагины Internet Explorer (ВНО)	$\checkmark$			
<ul> <li>Конфигурация</li> </ul>		Автозапуск программ				
<ul> <li>права</li> <li>Планировник за даний</li> </ul>		Автозалуск политик				
<ul> <li>Ограничения обновлений</li> </ul>			-			
<ul> <li>Устанавливаемые компоненты</li> </ul>		конфигурация везопасного режина				
<ul> <li>Параметры подключения</li> </ul>		Параметры Менеджера сессий			~	
<ul> <li>Виртуальный агент</li> </ul>		Системные службы				

Рисунок 2.6 – Настройки антивирусного ПО

### 2.6 Постановка на КЦ программных модулей СЗИ в ОС Linux

Для обеспечения безопасности защищаемой информации и контроля целостности модулей СЗИ на клиентских рабочих станциях под управлением ОС Linux администратору безопасности необходимо с помощью механизмов контроля целостности ОС выполнить постановку на контроль следующих программных модулей:

auth_app	Приложение выполняющее проверку аутентификационных данных			
gis_client_auditsystem	Служба отвечающая за сбор и хранение сообщений аудита (на клиенте)			
gis_client_db	Менеджер работы с БД Политик и настроек клиента			
gis_client_deploymentsystem	Агент развертывания			
gis_client_info	Менеджер определения информации о ресурсах ПК			
gis_client_networkclient	Модуль клиента сетевого взаимодействия			
gis_client_settings_dispatcher	Диспетчер событий аудита клиента			



gis_client_tokensystem	Служба управления токенами на клиенте (Клиентская служба удалённого выпуска токенов для аутентификации) (на клиенте)				
libauditwidget.so	Формирование оповещений сигнализации (на клиенте)				
libbh_local_auth_alt.so	Библиотека для взаимодействия с графической подсистемой Linux				
	для аутентификации локальных пользователей				
libbh_post_auth_alt.so libbh_post_auth_astra.so	Библиотека для взаимодействия с графической подсистемой Linux для аутентификации доменных пользователей				
libbh_pre_auth_alt.so	Библиотека для взаимодействия с графической подсистемой Linux				
libbh_pre_auth_astra.so	для подготовки к аутентификации				
libDebugLoggerA.so	Библиотека для записи отладочных логов работы службы аудита в файл.				
libDebugLoggerDS.so	Библиотека для записи отладочных логов работы службы аудита в файл.				
libDebugLoggerTs.so	Библиотека для записи отладочных логов				
libTCPProtocol.so	Библиотека сетевого протокола TCP/IP				
libTokenLib.so	Библиотека для записи сертификатов на персональные электронные идентификаторы (токены) (для аутентификации в домене) (на сервере и на клиенте управления)				
pinapp	Клиентское приложения для ввода пользователем PIN-кода для удалённо выдаваемого пользовательского токена администратором (на клиенте)				

### 3 Основные элементы интерфейса

Основная работа администратора безопасности по управлению политиками ведется во вкладке **Менеджер иерархии**, содержащей дерево иерархии и рабочую область (рисунок 3.1).

Менеджер иерархий					
C: 8   4   4   4   4	2, С Па зб9dc В 1 ₽ 2 Онлайн ●	Статистика События	Deconstrates		c
<ul> <li>вая вознас</li> <li>все компьютеры</li> </ul>	<ul> <li>Создать С. Отвязать &amp; Измение</li> </ul>	ть 🖾 Удалить	and the second		Экспорт
• 🗅 fpynna 1	Наиментование	Группа	Cranyc	Создано	stame-e-p
<ul> <li>Tpynna 2</li> </ul>	<ul> <li>Клиентские политики - 3</li> </ul>				
• 📑 PC2	Клиентская политика 1	🗅 fpynna1	Активна	21.09.2021 12:38	21.09.2021 12
◆ □ Tpynna s ♀ s09dc	Клиентская политика 2	🗀 fpynna 2	Активна	21.09.2021 12:38	21.09.2021 12
🗀 līpynna 4	Политика клиента по умолчанию	🗀 Все компьютеры	Активна	09.09.2021 13:00	21.09.2021 12
	<ul> <li>Политика SafeNode System Loader - 3</li> </ul>				
	Политика SafeNode System Loader no у	Все компьютеры	Активна	09.09.2021 13:00	17.09.2021 15
	Политика SNSL 1	C [pynnal	Активна	21.09.2021 12:42	21.09.2021 12
	Политика SNSL 2	🗀 fpynna 2	Активна	21.09.2021 12:42	21.09.2021 12
	<ul> <li>Серверные политики - 3</li> </ul>				
	Политика сервера по умолчанию	🗀 Все компьютеры	Активна	09.09.2021 13:00	09.09.2021 13
	Серверная политика 1	C Fpynne 1	Активна	21.09.2021 12:38	21.09.2021 12:
	Серверная политика 2	C l'pynna 2	Активна	21.09.2021 12:38	21.09.2021 12:
	Клиентские: 3 Серверные: 3 SafeNode: 3	n in the second s			

Рисунок 3.1 – Вкладка управления политиками

Область **дерева иерархии** предназначена для отображения сформированной сетевой структуры: основной и подчиненные серверы, клиентские рабочие станции и группы, включающие подчиненные серверы и клиентские рабочие станции.

Рабочая область изменяет вид в зависимости от элемента, выбранного в иерархии.

В верхней части рабочей области отображается информация о выбранном в иерархии элементе (рисунок 3.1). Например, для выбранного в иерархии сервера отображается следующая информация:

- наименование выбранного сервера;
- количество подчиненных серверов и клиентских рабочих станций;
- состояние сервера (онлайн/офлайн).

При выборе в иерархии основного или головного сервера, информация в рабочей области будет разделена на вкладки:

### 72410666.00063-04 95 01-01



Общее – предназначена для отображения общей информации по выбранному в иерархии серверу, серверной политике, применяемой к серверу, количестве серверов и клиентов, подчиненных выбранному серверу, и информации по последнему циклу опроса подчиненных серверов и клиентов.

– **Политики** – предназначена для создания и просмотра клиентских, серверных политик, политик SafeNode System Loader, назначения политик группам, внесения изменений в разделы политик.

 Настройки – предназначена для управления настройками сервера (управление автоархивацией событий, настройка размера кеша событий, построение иерархии серверов).

 Статистика – предназначена для отображения сводной статистики по текущему серверу или с учетом всех подчиненных серверов, находящимся в прямом или косвенном подчинении выбранному серверу;

– **События** – предназначена для поиска событий в хранилище сервера, собранных с подчиненных ему серверов и клиентских рабочих станций.

*Лицензии* – предназначена для активации продукта и просмотра всех лицензий, имеющихся на сервере.

При выборе в иерархии **группы** серверов или рабочих станций, информация в рабочей области будет разделена на вкладки:

 Общее – предназначена для отображения общей информации по выбранной в иерархии группе, клиентской и серверной политике, применяемых к группе, количестве серверов и клиентов в группе.

– *Компьютеры* – предназначена для отображения серверов и клиентских рабочих станций, входящих в группу.

– **Политики** – предназначена для просмотра клиентских, серверных политик, политик SafeNode System Loader, назначенных группе, внесения изменений в разделы политик и удаления политик.

При выборе в иерархии клиентской рабочей станции, информация в рабочей области будет разделена на вкладки:

 Общее – предназначена для отображения общей информации о клиенте и о разделах клиентской политики, возможных к назначению на клиентской рабочей станции.

- **Токены** – предназначена для управления токенами, подключенными к рабочей станции (назначение, изъятие, приостановка, синхронизация токена).

 Пользователь – предназначена для просмотра активных учетных записей пользователей клиентской рабочей станции и управлением устройствами, назначенными пользователям.



Настройки – предназначена для управления настройками клиента Блокхост-Сеть (дискреционный механизм разграничения доступа, замкнутая среда функционирования, контроль печати, контроль целостности и восстановление файлов, мандатный доступ, проверка пароля в СЗИ, пользователи с разрешением на вход в ОС) и настройками клиента со взятым под управление SafeNode (пользователи СДЗ, сетевой адаптер UEFI, проверка пароля в SafeNode, пользователи с разрешением на вход в ОС).

– **События** – предназначена для поиска и отображения всех событий, зарегистрированных на клиентской рабочей станции.



### 4 Общие принципы работы

### 4.1 Управление иерархией

Общий принцип построения иерархии, содержащей головной и подчиненные серверы, а также клиентские рабочие станции изображен на рисунке 4.1.



Рисунок 4.1 – Иерархия серверов Блокхост-Сеть

В консоли управления иерархия СЗИ отображается в левой части вкладки **Менеджер** *иерархии* содержит основной и подчиненные серверы, клиентские рабочие станции и группы, включающие подчиненные серверы и клиентские рабочие станции (рисунок 4.2).

СЗИ от НСД «Блокхост-Сеть 4» СЕРВИС Руководство администратора безопасности. Часть 1 Управление политиками Х Блокхост-Сеть 4 × Менеджер иерархий 2 C: 8 4 4 Q C 🖬 s09dc Онлайн 🔹 C d. Общее Токены Пользователь Настройки События - 🖬 s09dc Все компьютеры О компьютере Ipynna1 Клиентская политика Политика клиента по умолчанию 😅 冏 😼 astra 18:54 21:09.2021 Время применения Группа 2 . B PC2 Windows Server 2012 R2 Datacenter (64 Girta) Burryck OC C) Epynna 3 Пакет обновления Отсутствует 🖬 s09dc C Fpynna 4 127.0.0.1 IP appec DNS WAR 109.dc Модули 5/15 0 128 0 網 B R Сложность Контроль Очистка Управлен входом в ОС паролей целостности файлов оперативной памяти 6 0 8 R a Аудит запуска Гарантир Аудит доступа к медиафайлам Контроля даление файлов целостности среды 63 P 6 âc Мандати Дискрез Замкнутая Конт устройств доступ программи доступ (a) Контро Ē Довере аутентификаци загрузка 

25

Рисунок 4.2 – Отображение иерархии

В верхней части иерархии расположены следующие элементы управления:

 кнопка <sup>Ш</sup> позволяет удалить созданные группы или добавленные в иерархию клиентские рабочие станции и подчиненные серверы;

 кнопка позволяет отображать иерархию более детально на уровне клиентских рабочих станций и подчиненных серверов, включенных во все имеющиеся в иерархии группы (рисунок 4.2);

- кнопка 🛱 позволяет отображать иерархию только на уровне групп.

– кнопка <sup>С</sup> позволяет обновить иерархию и увидеть текущее состояние клиентских рабочих станций и подчиненных серверов;

 кнопка , открывающая строку поиска, предназначенную для отбора клиентских рабочих станций, подчиненных серверов или групп в иерархии в соответствии со значением, введенным в строку поиска.

газинформ

### GIS ГАЗИНФОРМ СЕРВИС

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками



Фильтрация по вводимому в строку значению осуществляется в списке иерархии автоматически, после введения трех и более символов (рисунок 4.3), при этом регистр вводимых символов не учитывается.

🗙 Бло	кхост-Сеть 4	
&	Менеджер иерархий	
кĴя		Q C
0	w1	×
ŕÐ	Введите более 3 символов	

Рисунок 4.3 – Поиск в иерархии

В зависимости от статуса сервера или клиентской рабочей станции, пиктограмма отображения сервера/клиента в иерархии различается:

Габлица 4.1 -	- Статусы клиентс	ких рабочих станций	
Пиктограмма	Статус клиента	Возможные ситуации установки статуса	Решение
OC Windows	Штатный режим функционирования (online/offline)	<ul> <li>Версия СЗИ, установленная на клиенте, совместима с версией сервера.</li> <li>Клиент занимает слот лицензии.</li> <li>Клиент работает в режиме</li> </ul>	
		полной функциональности (не в мягком режиме). • Последняя синхронизация клиентской политики на клиенте завершилась без ошибок.	
£	Выполняется синхронизация политики	<ul> <li>Внесение изменений в клиентскую политику.</li> <li>Синхронизация клиентской политики</li> </ul>	
OC Windows	Клиент БХ-Сеть несовместим с версией сервера	• Версия СЗИ, установленная на клиенте, несовместима с версией	Необходимо обновить версию на актуальную. (если версия клиента и

Т

И



Пиктограмма	Статус клиента	Возможные ситуации установки статуса	Решение
GC Linux		сервера.	сервера несовместимы, клиент отвязывается от лицензии (перестает занимать слот лицензии).
	Лицензия отсутствует. Включен режим ограниченной функциональности (мягкий режим)	<ul> <li>Максимальное количество клиентов, обслуживаемых сервером, превышено.</li> </ul>	Необходимо проверить наличие свободных слотов в активированных на сервере лицензиях, до привязки к лицензии клиент будет работать в мягком режиме.
	Включен мягкий режим. Клиент БХ- Сеть работает в режиме ограниченной функциональности	• Включен мягкий режим.	Информация о мягком режиме берется из клиентской политики. В мягком режиме клиент не обеспечивает заявленных функций безопасности. Измените режим работы клиента в разделе политики <b>«Другие параметры»</b> .
	Ошибка применения политики.	<ul> <li>Ошибка в механизмах. Не удалось получить доступ к некоторым файлам.</li> </ul>	Возможно, файлы заняты другими процессами.
	Ошибка в работе клиента БХ-Сеть	<ul> <li>Клиент не ответил на запрос своевременно.</li> <li>Не удалось подтвердить валидность лицензии на клиенте.</li> </ul>	Ошибка при применении политики. Выполните синхронизацию политики для повторного применения к клиенту.
			Ошибка при проверке лицензии на клиенте. Проверьте, что на клиенте установлено правильное время.
SC Windows CC Windows CC Linux	Формирование замкнутой программной среды	• Выполняется формирование перечня программ для замкнутой программной среды (запущен режим автоформирования). Механизм работает в режиме ограниченной функциональности (не препятствует запуску каких-	
		либо программ). Остальные механизмы работают в	



Пиктограмма	Статус клиента	Возможные ситуации установки статуса	Решение
		обычном режиме, без каких- либо ограничений.	
GC Windows	Установлен СДЗ «SafeNode System Loader»	• На клиенте установлен СДЗ «SafeNode System Loader», но не взят под управление	
SC Linux			

Пиктограмма	Статус сервера	Возможные ситуации установки статуса	Решение
C Windows	Штатный режим функционирования	<ul> <li>Версия дочернего сервера СЗИ совместима с версией головного сервера.</li> <li>Дочерний сервер занимает слот лицензии.</li> <li>Последняя синхронизация политики с дочерним сервером завершилась без ошибок.</li> </ul>	
	Выполняется синхронизация политики	<ul> <li>Внесение изменений в серверную политику.</li> <li>Синхронизация серверной политики.</li> </ul>	
C Windows	Сервер БХ-Сеть несовместим с версией головного сервера	• Версия СЗИ, установленная на сервере, несовместима с версией головного сервера.	Возможность изменения параметров работы и сбор данных для сервера недоступны. Необходимо обновить версию на актуальную (если версия родительского и подчиненного серверов несовместимы, дочерний сервер отвязывается от лицензии (перестает занимать слот лицензии).
	Отсутствует лицензия.	• Нет свободных слотов в активированных на головном сервере лицензиях.	Проверьте наличие свободных слотов в активированных на головном сервере лицензиях.
	Ошибка применения политики.	<ul> <li>Сервер не ответил на запрос своевременно</li> </ul>	Выполните синхронизацию политики для повторного применения к серверу.



Группа «Все компьютеры» является родительской по отношению к остальным группам. Она создается по умолчанию при установке СЗИ и не может быть удалена или перемещена по иерархии.

Любая из созданных в иерархии групп не может быть удалена, если в ней, или в одной из ее дочерних групп есть хотя бы один сервер или клиентская рабочая станция (рисунок 4.4).



Рисунок 4.4 – Удаление группы в иерархии

Созданные в иерархии группы могут быть перемещены по иерархии с помощью удержания и перетаскивания элемента левой кнопкой мыши или с помощью контекстного меню группы **Вырезать/Вставить**. При этом действуют следующие правила при выделении групп, серверов и клиентских рабочих станций в иерархии:

 можно выделить для перемещения только одну группу (если группа уже выделена, при выделении другой группы выделение с предыдущей группы снимается);

 одновременно выделить серверы/клиентские рабочие станции и группы невозможно (при добавлении группы к уже выделенным серверам или клиентским рабочим станциям выделение с них снимается);

 выделение нескольких серверов или клиентских рабочих станций возможно только если они являются подчиненными одному и тому же серверу (при добавлении к уже выделенным серверам или клиентским рабочим станциям сервера или клиента, подчиненных другому серверу, выделение с них снимается);

 при выделении корневого сервера невозможно выделить другие серверы или клиентские рабочие станции (выделяется отдельно от всех остальных);

 перемещение групп, клиентских рабочих станций и серверов, возможно только внутри сервера, к которому эти клиенты/серверы относятся (попытка переместить такие машины в группы другого сервера не увенчается успехом).



### 4.2 Общее описание политик

Политика – это определенный набор настроек механизмов безопасности и параметров работы СЗИ.

В СЗИ существует три типа политик (рисунок 4.5):

серверная политика (определяет параметры работы серверов);

клиентская политика (определяет параметры работы клиентских рабочих станций);

политика SafeNode System Loader (позволяет установить дополнительный этап прохождения аутентификации пользователей до загрузки ОС с помощью средства доверенной загрузки «SafeNode System Loader» и определяет параметры аутентификации пользователей до загрузки ОС).

Х Блон	киост-Сеть 4					– 🗆 ×
8	Менеджер иерархий					
÷	다 (1) 10 10 10 10 10 10 10 10 10 10 10 10 10	Гад 1094с ⊟1 ⊊2 Оклайн Ф Общее Политики Настройки Статистики	а События Лицено	пи		c
10 10	<ul> <li>Все компьютеры</li> <li>Группа 1</li> <li>astra</li> </ul>	Осоздать «С Отвязать «Изменить В У     Наменить В У     Намените наме	Далить Группа	Cranys	🛓 Из Создано	ипорт 👌 Экспорт Изменно
	C Tpynna 2     F PC2     D Tpynna 3     G dddo	<ul> <li>Клиентские политика - 3</li> <li>Клиентская политика 1</li> <li>Клиентская политика 2</li> </ul>	C Fpynna 1	Активна Активна	21.09.2021 12:38 21.09.2021 12:38	21.09.2021 12:38 21.09.2021 12:38
	C) Fpynna 4	Политика клиента по умолчанию	🗅 Все компьютеры	Активна	09.09.2021 13:00	21.09.2021 18:44
		<ul> <li>политика SafeNode System Loader то умолчанию</li> </ul>	🗅 Все компьютеры	Активна	09.09.2021 13:00	17.09.2021 15:24
		Политика SNSL 1 Политика SNSL 2	C Fpynna 1	Активна Активна	21.09.2021 12:42 21.09.2021 12:42	21.09.2021 12:42 21.09.2021 12:42
		<ul> <li>Серверные политики - 3</li> <li>Политика сервера по умолчанию</li> </ul>	Все компьютеры	Активна	09.09.2021 13:00	09.09.2021 13:00
		Серверная политика 1	C Fpynnel	Активна	21.09.2021 12:38	21.09.2021 12:38
m		Серверная политика 2	🗅 Группа 2	Активна	21.09.2021 12:38	21.09.2021 12:38
0		Клиентские: 3 Серверные: 3 SafeNode: 3				-

Рисунок 4.5 – Отображение политик в интерфейсе

Привязать политику можно только к группе в иерархии. При этом количество создаваемых администратором безопасности групп неограниченно.

Политики верхнего уровня (политики корневой группы «Все компьютеры») являются родительскими по отношению ко всем нижестоящим группам.

Настройки и параметры политик корневой группы «Все компьютеры» оказывают влияние на все группы в иерархии при условии установки принудительного

### 72410666.00063-04 95 01-01



наследования политик (см. раздел *«Принудительное наследование»*) или при условии отсутствия в этих группах собственных политик, если принудительное наследование не установлено.

Политики корневой группы «Все компьютеры»:

не могут быть отвязаны от данной группы;

- не могут быть удалены из базы данных СЗИ;
- не могут быть замещены другими политиками.

Любая политика может находится в статусах:

 не активна – созданная политика содержится в базе данных СЗИ, ее настройки и параметры не влияют на работу серверов или клиентских рабочих станций;

 активна – политика является действующей, привязана к группе в иерархии, параметры политики влияют на работу серверов и клиентских рабочих станций.

У каждой созданной группы должна быть действующая серверная и клиентская политики (группы, не имеющей действующих клиентской и серверной политик не может существовать), причем возможна привязка только <u>одной</u> серверной и клиентской политик к группе.

Группа может существовать, не имея привязанных политик, также можно отвязать политики от группы без одновременной привязки замещающих политик. В этом случае действующими политиками для группы становятся наследуемые действующие серверная и клиентская политики родительской группы.

### 4.3 Принудительное наследование

В СЗИ существует возможность принудительно наследовать отдельные параметры или разделы политик родительских групп политиками нижестоящих групп.

Индикация принудительного наследования какого-либо параметра или раздела политики в интерфейсе представлена в виде замка « ) / » (рисунок 4.6).



32

🗙 Изменение клиентской политики: Политика клиента по умолчанию			
Общее	Контроль целостности среды 🗅		
Windows	Отмеченные события будут записываться в систему аудита		
Управление входом в ОС	Контроль		
Сложность паролей	🗌 Аппаратной среды 🛈 🔓		
Контроль устройств	🗌 Изменения перечня каталогов общего доступа  🔒		
Очистка оперативной памяти	🗹 Установки/удаления драйверов d		
Гарантированное	🗌 Установки/удаления служб 🔓		
удаление файлов	🗹 Установки/удаления программ 🔒		
Аудит целостности файлов			
Аудит запуска приложений			
Аудит печати			
Аудит доступа к медиафайлам			
Контроль целостности среды			
Журнал аудита			
Linux			
Мягкий режим			
	Ок Отмена Применит	ъ	

Рисунок 4.6 – Принудительное наследование параметров типа флаг

Открытый замок « <sup>С</sup> » на каком-либо параметре или разделе политики означает возможность изменения такого параметра или раздела администраторами нижестоящих уровней иерархии.

Закрытый замок « > на каком-либо параметре или разделе политики влечет за собой невозможность перезаписи такого параметра или раздела на всех нижестоящих уровнях иерархии. Значение раздела или параметра становится полностью идентичным значению, заданному на верхнем уровне без возможности его восстановления ранее заданным значением. Администраторы нижестоящих уровней иерархии не имеют технической возможности изменить параметр или раздел политики с установленным замком; или снять режим принудительного наследования политики.

Наследуемые параметры политик подразделяются на следующие категории:

параметры типа флаг, принимающие значения «включено»/«выключено»
 (например: ограничения сложности пароля пользователя, собираемые события аудита);

– параметры типа *список*, включающие в себя множество элементов, каждый из которых может иметь свои настройки (например: список файлов для контроля



целостности, список доменных или локальных пользователей или групп пользователей с различными настройками аутентификации для каждого пользователя/группы пользователей).

### 4.3.1 Принудительное наследование параметров политик типа флаг

Рассмотрим принудительное наследование параметров политик типа *флаг* на примере механизма **«Контроль целостности среды»** (рисунок 4.6).

Имеется иерархия групп следующей структуры (рисунок 4.7):

верхний уровень – группа «Все компьютеры», с действующей политикой «Политика клиента по умолчанию»;

подчиненная группа – «Группа 1», с действующей политикой «Клиентская политика 1».

🗙 Бло	кхост-Сеть 4			_	×
ጽ	Менеджер иерархий				
к∱л		🗀 Все компьютеры			C
÷ ۳	<ul> <li>т ш w09w13</li> <li>т Все компьютеры</li> <li>т Группа 1</li> <li>щ localhost</li> <li>т Группа 2</li> <li>щ PC1</li> <li>т Группа 3</li> <li>т Группа 4</li> </ul>	Общее Компьютеры О группе Клиентская политика Серверная политика Политика SafeNode	Политики Политика клиента по умолчанию Политика сервера по умолчанию Политика SafeNode System Loader по умолчанию Всего		
		Серверов	0		
X Бло	кхост-Сеть 4 Менеджер иерархий	a	)	-	×
~\$* 10	С: Ш Д В Q С • Щ w09w13 • С Все компьютеры • Группа 1 — Iocalhost • С Группа 2 — PC1 • С Группа 3 С Группа 4	□ Группа 1 ■ 0 ₽ Общее Компьютеры О группе Клиентская политика Серверная политика Политика SafeNode Серверов Компьютеров	1 Политики Клиентская политика 1 Серверная политика 1 Политика SafeNode System Loader по умолчанию Всего 0 1		C

б)

Рисунок 4.7 – Пример иерархии



### Пример 1:

В политике «Политика клиента по умолчанию» в механизме **«Контроль целостности среды»** администратор верхнего уровня включил контроль установки/удаления программ и установил на него замок – принудительное наследование (рисунок 4.8 а).

В политике «Клиентская политика 1» значение параметра «под замком» наследуемое с верхнего уровня станет идентичным значению, заданному на верхнем уровне. При этом изменение данного параметра недоступно администратору нижнего уровня (рисунок 4.8 б).

X Изменение клиентской политики: Политика клиента по умолчанию X			
Общее	Контроль целостности среды 🗅		
Windows	Отмеченные события будут записываться в систему аудита		
Управление входом в ОС	Контроль		
Сложность паролей	🗌 Аппаратной среды 🛈 🕒		
Контроль устройств	Изменения перечня каталогов общего доступа		
Очистка оперативной памяти	Установки/удаления драйверов		
Гарантированное	Установки/удаления служб □ <sup>∩</sup>		
удаление файлов	🗹 Установки/удаления программ  🔒		
	a)		
🔀 Изменение клиентской полити	ики: Клиентская политика 1	×	
Общее	Контроль целостности среды 🗅		
Windows	Отмеченные события будут записываться в систему аудита		
Управление входом в ОС	Контроль		
Сложность паролей	🗌 Аппаратной среды 🛈 🗗		
Контроль устройств	□ Изменения перечня каталогов общего доступа □		
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🔓		
Гарантированное удаление файлов	🗌 Установки/удаления служб 🔓		
	📴 Установки/удаления программ 🔒		
б)			

Рисунок 4.8 – Принудительное наследование установленного параметра

Администратор верхнего уровня выключает контроль установки/удаления программ в политике «Политика клиента по умолчанию» (рисунок 4.9 а).

Так как для этого параметра установлено принудительное наследование, значение параметра в политике «Клиентская политика 1» станет идентичным значению, заданному на верхнем уровне. При этом изменение данного параметра недоступно администратору нижнего уровня (рисунок 4.9 б).



35

🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию	×
Общее	Контроль целостности среды 🗅	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗌 Аппаратной среды 🛈 🕒	
Контроль устройств	Изменения перечня каталогов общего доступа	
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🕒	
Гарантированное	🗌 Установки/удаления служб 🔓	
удаление файлов	🗌 Установки/удаления программ  🔒	
	3)	
	α)	
🗙 Изменение клиентской полити	ики: Клиентская политика 1	×
Общее	Контроль целостности среды 🗅	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗌 Аппаратной среды 🛈 🗗	
Контроль устройств	□ Изменения перечня каталогов общего доступа □	
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🕒	
Гарантированное	🗌 Установки/удаления служб 🔓	
удаление файлов	Установки/удаления программ 🔒	

б)

Рисунок 4.9 – Принудительное наследование после выключения параметра

### Пример 2:

В политике «Политика клиента по умолчанию» установлен контроль установки/удаления программ, принудительное наследование параметра установлено (рисунок 4.8 а).

В политике «Клиентская политика 1» значение параметра «под замком» наследуемое с верхнего уровня идентично значению, заданному на верхнем уровне. При этом изменение данного параметра недоступно администратору нижнего уровня (рисунок 4.8 б).

Администратор верхнего уровня выключает контроль установки/удаления программ и снимает замок в политике «Политика клиента по умолчанию» (рисунок 4.10 а).

Так как принудительное наследование не осуществляется, изменение параметра в политике «Политика клиента по умолчанию» не влияет на параметр в политике «Клиентская политика 1» — значение параметра не изменяется. При этом администратору нижнего уровня становится доступно изменение данного параметра (рисунок 4.10 б).



🗙 Изменение клиентской политики: Политика клиента по умолчанию		
Общее	Контроль целостности среды	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗌 Алпаратной среды 🛈 🗗	
Контроль устройств	🗌 Изменения перечня каталогов общего доступа 🖉	
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🔓	
Гарантированное	🗌 Установки/удаления служб 🕒	
удаление файлов	Установки/удаления программ	
	a)	
Х Изменение клиентской полити	іки: Клиентская политика 1	×
Общее	Контроль целостности среды	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗌 Аппаратной среды 🛈 🗗	
Контроль устройств	🗌 Изменения перечня каталогов общего доступа 🕒	
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🔤	
Гарантированное	🗌 Установки/удаления служб 🗗	
удаление файлов	🗹 Установки/удаления программ  🔒	

б)

Рисунок 4.10 – Принудительное наследование после снятия замка с параметра

### Пример 3:

В политике «Политика клиента по умолчанию» выключен контроль установки/удаления программ, принудительное наследование не установлено (рисунок 4.10 а).

В политике «Клиентская политика 1» значение параметра не наследуется, администратором нижнего уровня установлены следующие настройки параметра: контроль установки/удаления программ выключен, установлен замок (рисунок 4.11).

🗙 Изменение клиентской политики: Клиентская политика 1		×
Общее	Контроль целостности среды	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗌 Аппаратной среды 🛈 🗗	
Контроль устройств	🗌 Изменения перечня каталогов общего доступа 🖉	
Очистка оперативной памяти	🗌 Установки/удаления драйверов 🔤	
Гарантированное удаление файлов	Установки/удаления служб	
	🗌 Установки/удаления программ  🔒	

Рисунок 4.11 – Настройка параметра администратором нижнего уровня

36
Администратор верхнего уровня включает параметр и устанавливает замок в политике «Политика клиента по умолчанию» (рисунок 4.8 а).

Так как установлено принудительное наследование, значение параметра в политике «Клиентская политика 1» станет идентичным значению, заданному на верхнем уровне. При этом изменение данного параметра становится недоступно администратору нижнего уровня (рисунок 4.8 б).

## 4.3.2 Принудительное наследование параметров типа список

Рассмотрим принудительное наследование параметров политик типа *список* на примере механизма **«Управление входом в ОС»** (рисунок 4.12).

🗙 Изменение клиентской полити	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	и в ОС 🗅			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	Q Поиск пользователей				
Сложность паролей	+ 🔟 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows	<b>~</b>	
Гарантированное	pki.local\user02	Active Directory	По токену		
удаление файлов	о́∩о́в Все пользователи		Тип входа		
Аудит целостности файлов			-		
Аудит запуска приложений			ил	Разрешить	запретить
Аудит печати			интерактивный вход		
			Сегевой вход		
Аудит доступа к медиафайлам					
Контроль целостности среды					
Журнал аудита					
Linux					
Мягкий режим	Пользователей: 2 Групп: 1				
		Οĸ	Отмена	Прим	іенить

Рисунок 4.12 – Принудительное наследование параметров типа список

В механизме **«Управление входом в ОС»** содержится список параметров следующей структуры:





<ПользовательN> 🔒 / 🗗

Имеется иерархия групп следующей структуры (рисунок 4.7):

верхний уровень – группа «Все компьютеры», с действующей политикой «Политика клиента по умолчанию»;

подчиненная группа – «Группа 1», с действующей политикой «Клиентская политика 1».

В политике «Политика клиента по умолчанию» администратор верхнего уровня установил замок на весь список пользователей и на один из элементов списка *«user02»* (рисунок 4.13 а).

В политике «Клиентская политика 1» список пользователей и элемент списка «под замком» наследуемые с верхнего уровня станут идентичными значениям, заданным на верхнем уровне (рисунок 4.13 б).

Администратор нижнего уровня не может изменить список элементов, добавить или удалить какой-либо элемент списка.

🗙 Изменение клиентской полити	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	и в ОС 🗗			
Windows	Список пользователей 🔒	Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	pki.local\user02	Active Directory	По токену		
удаление файлов	ല്റ്റ് Все пользователи		Тип входа		
Аудит целостности файлов			Tura	Daspanuum	2300001474
Аудит запуска приложений			Интерактивный вусл		
Аудит печати			Сетевой вход		

a)

GIS газинформ сервис		СЗИ от НСД «Блокхост- Руководство администр Управление политиками	Сеть 4» атора безопасности. Часть 1	1	3
🗙 Изменение клиентской полит	ики: Клиентская политика 1				×
Общее	Управление входом в	<b>oc</b>			
Windows	Список пользователей 🔒 До	полнительные настройки			
Управление входом в ОС	Q Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Wind	lows 🔽	
Гарантированное	🔒 🙁 pki.local\user02	Active Directory	По токену		
удаление файлов	°∩° Все пользователи		Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
		ര്			

Рисунок 4.13 – Принудительное наследование, установленное в списке

Если в политике «Клиентская политика 1» присутствовали какие-либо пользователи в списке до принудительного наследования настроек политики «Политика клиента по умолчанию», например, как на рисунке 4.14, они будут заменены значениями элементов списка политики «Политика клиента по умолчанию» (рисунок 4.13 б).

🗙 Изменение клиентской полит	ики: Клиентская политика 1				×
Общее	Управление входом	и в ОС 🗗			
Windows	Список пользователей 🔒	Дополнительные настройки			
Управление входом в ОС	Q Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	.▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	🔒 🙁 pki.local\pkiuser	Active Directory	Аутентификация Windows		
Гарантированное	aos Все пользователи		По токену		
удаление файлов			Тип входа		
Аудит целостности файлов			T	D	7
Аудит запуска приложений			и	Разрешить	запретить
Аудит печати			Сетевой вход		

Рисунок 4.14 – Настройка параметра администратором нижнего уровня

Администратор верхнего уровня снимает замок со списка пользователей в политике «Политика клиента по умолчанию» (рисунок 4.15 а).

Так как принудительное наследование не осуществляется, содержание списка пользователей в дочерней политике «Клиентская политика 1» не изменится. Пользователь «*user02*» остающийся под замком в политике «Политика клиента по умолчанию» транслируется в политику «Клиентская политика 1» и недоступен для



изменения (рисунок 4.15 б).

Администратор нижнего уровня может изменять пользователей списка: добавлять, удалять (кроме пользователя *«user02»* на котором установлен замок в родительской политике), а также снимать/устанавливать замок на всем списке пользователей.

🗙 Изменение клиентской полити	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	и в ОС 🗅			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	Q Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	≜ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows	<b>~</b>	
Гарантированное	🔒 💽 pki.local\user02	Active Directory	По токену		
удаление файлов	å <sup>O</sup> å Все пользователи		Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
		2)			
		aj			
🗙 Изменение клиентской полити	ики: Клиентская политика 1				×
Общее	Управление входом	и в ОС 🗗			
Windows	Список пользователей 🔒	Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows	<b>~</b>	
Гарантированное	🔒 🙁 pki.local\user02	Active Directory	По токену		
удаление файлов	°О° Все пользователи		Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход	<b>~</b>	

б)

Рисунок 4.15 – Принудительное наследование после снятия замка на списке

#### Пример 2:

В политике «Политика клиента по умолчанию» в механизме **«Управление входом в ОС»** список пользователей включает одного пользователя «*user01*», принудительное наследование не установлено ни на списке, ни на элементе списка (рисунок 4.16 а).

В политику «Клиентская политика 1» список пользователей из родительской политики не наследуется, администратору нижнего уровня доступны любые действия со



списком. В политике «Клиентская политика 1» задан аналогичный список пользователей, включающий пользователя «*user01*», и установлено принудительное наследование на пользователе (рисунок 4.16 б).

Х Изменение клиентской полити	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	л в ОС 🗗			
Windows	Список пользователей 占	Дополнительные настройки			
Управление входом в ОС	🔍 Поиск пользователей				
Сложность паролей	+ 🗊 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	°∩° Все пользователи		По токену		
удаление файлов			Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
		a)			
Х Изменение клиентской полити	ики: Клиентская политика 1				×
Общее	Управление входом	и в ОС 🗗			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	🔒 💽 pki.local\user01	Active Directory	Аутентификация Windows	<b>~</b>	
Гарантированное	°0° Все пользователи		По токену		
удаление файлов			Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
5			интеристионый вход		
Аудит печати			Сетевой вход		

б)

Рисунок 4.16 – Принудительное наследование в списках не установлено

В политике «Политика клиента по умолчанию» администратор верхнего уровня добавляет в список пользователя «*user02*» и устанавливает замок на него (рисунок 4.17 а).

В политику «Клиентская политика 1» пользователь «под замком» наследуется с верхнего уровня. При этом «*user02*» недоступен для изменения администратором нижнего уровня (рисунок 4.17 б).



СЗИ от НСД «Блокхост-Сеть 4»
Руководство администратора безопасности. Часть 1
Управление политиками

42

🗙 Изменение клиентской полити	ки: Политика клиента по умолчанию				×
Общее	Управление входом в С	<b>с</b> 🗗			
Windows	Список пользователей 占 Допо	лнительные настройки			
Управление входом в ОС	Q. Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	pki.local\user02	Active Directory	По токену		
удаление файлов	്റ്റ് Все пользователи		Тип входа		
Аудит целостности файлов			Tue	Datasuur	222222
Аудит запуска приложений			Интерактивный вход	Разрешить	запретить
Аудит печати			Сетевой вход		
		,	Сстевой вход		
		2)			
		aj			
🗙 Изменение клиентской полити	ки: Клиентская политика 1	a)			×
X Изменение клиентской полити Общее	ки: Клиентская политика 1 Управление входом в О	a) DC 🗗			×
X Изменение клиентской полити Общее Windows	ки: Клиентская политика 1 Управление входом в С Список пользователей 🗗 Допо	а) ОС 🗗			×
X Изменение клиентской полити Общее Windows Управление входом в ОС	ки: Клиентская политика 1 Управление входом в С Список пользователей ப Допо	а) ОС ப			×
X Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей	ки: Клиентская политика 1 Управление входом в О Список пользователей ப Допо Списк пользователей Ф Удалить	а) ОС ப	Аутентификация		Скрыть
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств	ки: Клиентская политика 1 Управление входом в С Список пользователей பி Допо Список пользователей • Ø Удалить Пользователь/Группа	а) ОС С	<b>Аутентификация</b> Тип	Разрешить	<b>Х</b> Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти	ки: Клиентская политика 1 Управление входом в С Список пользователей பி Допо Список пользователей Ф Поиск пользователей Ф Далить Пользователь/Группа рki.local\user01	а) DC С илнительные настройки * Тип Active Directory	Аутентификация Тип Аутентификация Windows	Разрешить	Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное	ки: Клиентская политика 1 Управление входом в О Список пользователей பிДопо Список пользователей Список пользователей Удалить Пользователь/Группа рki.local\user01 рki.local\user02	СС линительные настройки Колнительные настройки Асtive Directory Аctive Directory	Аутентификация Тип Аутентификация Windows По токену	Разрешить	Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов	ки: Клиентская политика 1 Управление входом в С Список пользователей பி Допо Списск пользователей Поиск пользователей Тудалить Пользователь/Группа рki.local\user01 рki.local\user02 ஃஃ Все пользователи	а ) DC С ллнительные настройки Асtive Directory Active Directory	Аутентификация Тип Аутентификация Windows По токену Тип входа	Разрешить	К Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов Аудит целостности файлов	ки: Клиентская политика 1 Управление входом в С Список пользователей С Допо Список пользователей Допо Список пользователей Удалить Пользователь/Группа Ф Ркі.local\user01 Ркі.local\user02 аёва Все пользователи	ССС илнительные настройки * Тип Аctive Directory Active Directory	Аутентификация Тип Аутентификация Windows По токену Тип входа	Разрешить	Скрыть Запретить П
<ul> <li>У Изменение клиентской полити</li> <li>Общее</li> <li>Windows</li> <li>Управление входом в ОС</li> <li>Сложность паролей</li> <li>Контроль устройств</li> <li>Очистка оперативной памяти</li> <li>Гарантированное удаление файлов</li> <li>Аудит целостности файлов</li> <li>Аудит запуска приложений</li> </ul>	ки: Клиентская политика 1 Управление входом в С Список пользователей பி Допо Списск пользователей Списск пользователей Удалить Пользователь/Группа ркi.local\user01 рki.local\user02 аபа Все пользователи	СС ллнительные настройки Тип Active Directory Active Directory	Аутентификация Тип Аутентификация Windows По токену Тип входа Тип	Разрешить	Скрыть Запретить Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов Аудит целостности файлов Аудит запуска приложений Аудит печати	ки: Клиентская политика 1 Управление входом в С Список пользователей	С С лнительные настройки ▲ Тип Active Directory Active Directory	Аутентификация Тип Аутентификация Windows По токену Тип входа Тип Интерактивный вход	Разрешить С Разрешить Разрешить С С С С С С С С С С С С С С С С С С С	Скрыть Запретить Запретить

б)

Рисунок 4.17 – Принудительное наследование после добавления элемента с замком

#### Пример 3:

В политике «Политика клиента по умолчанию» в механизме **«Управление входом в ОС»** список пользователей включает одного пользователя «*user01*», принудительное наследование не установлено ни на списке, ни на элементе списка (рисунок 4.16 а).

В политику «Клиентская политика 1» список пользователей из родительской политики не наследуется, администратору нижнего уровня доступны любые действия со списком. В политике «Клиентская политика 1» задан аналогичный список пользователей, включающий пользователя «*user01*», и установлено принудительное наследование установлено на пользователе (рисунок 4.16 б).

В политике «Политика клиента по умолчанию» администратор верхнего уровня



добавляет в список пользователя «*user02*», принудительное наследование не установлено (рисунок 4.18 а).

В политику «Клиентская политика 1» пользователь «*user02*» не наследуется (рисунок 4.18 б).

🗙 Изменение клиентской полити	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	и в ОС 🗗			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	Q Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	≜ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	pki.local\user02	Active Directory	По токену		
удаление фаилов	ំ)ំំ Все пользователи		Тип входа		
Аудит целостности фаилов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
		a)			
Х Изменение клиентской полити	іки: Клиентская политика 1				×
X Изменение клиентской полити Общее	ки: Клиентская политика 1 Управление входом	<b>в ОС</b> பி			×
X Изменение клиентской полити Общее Windows	ики: Клиентская политика 1 Управление входом Список пользователей ப	<b>в ОС 🗅</b> Дополнительные настройки			×
X Изменение клиентской полити Общее Windows Управление входом в ОС	іки: Клиентская политика 1 Управление входом Список пользователей С	<b>в ОС</b> 🗗 Дополнительные настройки			×
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей	<ul> <li>ки: Клиентская политика 1</li> <li>Управление входом</li> <li>Список пользователей С</li> <li>Поиск пользователей</li> <li>Э Удалить</li> </ul>	<b>в ОС</b> Дополнительные настройки	Аутентификация		Скрыть
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств	<ul> <li>ки: Клиентская политика 1</li> <li>Управление входом</li> <li>Список пользователей С</li> <li>Поиск пользователей</li> <li>Поиск пользователей</li> <li>Тудалить</li> <li>Пользователь/Группа</li> </ul>	в ОС С Дополнительные настройки * Тип	<b>Аутентификация</b> Тип	Разрешить	Х Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти	<ul> <li>ки: Клиентская политика 1</li> <li>Управление входом</li> <li>Список пользователей С</li> <li>Поиск пользователей</li> <li>Поиск пользователей</li> <li>Тользователь/Группа</li> <li>pki.local/user01</li> </ul>	в ОС С Дополнительные настройки Тип Аctive Directory	<b>Аутентификация</b> <sup>Тип</sup> Аутентификация Windows	Разрешить	Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное	ки: Клиентская политика 1 Управление входом Список пользователей С Поиск пользователей Список пользователей Список пользователей Список пользователей Список пользователей С ри.local\user01 с в в Все пользователи	в ОС С Дополнительные настройки Тип Аctive Directory	Аутентификация <sup>Тип</sup> Аутентификация Windows По токену	Разрешить	Скрыть Запретить
Х Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов	ки: Клиентская политика 1 Управление входом Список пользователей Поиск пользователей	в ОС Дополнительные настройки ▲ Тип Аctive Directory	Аутентификация Тип Аутентификация Windows По токену Тип входа	Разрешить	Скрыть Запретить
У Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов Аудит целостности файлов	кки: Клиентская политика 1 Управление входом Список пользователей Список пользователей ↓ ☑ Удалить Пользователь/Группа ↓ ☑ рki.local\user01 பீப் Все пользователи	в ОС С Дополнительные настройки * Тип Active Directory	Аутентификация <sup>Тип</sup> Аутентификация Windows По токену <b>Тип входа</b> Тип	Разрешить	Скрыть Запретить Запретить Запретить
У Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов Аудит целостности файлов Аудит запуска приложений	ки: Клиентская политика 1 Управление входом Список пользователей С Поиск пользователей Список пользователей Опьзователь/Группа С ркі.local\user01 а°а Все пользователи	в ОС Дополнительные настройки ▲ Тип Аctive Directory	Аутентификация <sup>Тип</sup> Аутентификация Windows По токену <b>Тип входа</b> Тип	Разрешить С Разрешить Разрешить	Скрыть Запретить Запретить
У Изменение клиентской полити Общее Windows Управление входом в ОС Сложность паролей Контроль устройств Очистка оперативной памяти Гарантированное удаление файлов Аудит целостности файлов Аудит запуска приложений Аудит печати	ки: Клиентская политика 1 Управление входом Список пользователей С Список пользователей	в ОС Дополнительные настройки ▲ Тип Аctive Directory	Аутентификация <sup>Тип</sup> Аутентификация Windows По токену <b>Тип входа</b> Тип Интерактивный вход Сетевой вход	Разрешить С Разрешить С С С	Скрыть Запретить Запретить Запретить

Рисунок 4.18 – Принудительное наследование после добавления элемента без замка

# 4.4 Пересечение прав

Во всех разделах политик каждому пользователю или группе пользователей из списка сопоставляется матрица доступа – настройка, определяющая права доступа пользователя или группы пользователей к какому-либо ресурсу.

Типовая матрица доступа для пользователя или группы пользователей может быть



представлена в следующем виде:

Тип доступа	Разрешение	Запрет
Чтение (R)	Да/Нет	Да/Нет
Запись (W)	Да/Нет	Да/Нет

При этом в разделе политики возможны пересечения, так как конечный пользователь может входить в несколько групп, присутствующих в списке.

Для вычисления результирующих настроек конечного пользователя с учетом настроек групп, куда входит данный пользователь, вводятся правила пересечения прав:

– <u>разрешения</u> для пользователя из всех групп (в том числе если этого пользователя добавить в список напрямую) <u>суммируются;</u>

 если в одной группе стоит разрешение на чтение, а в другой такое разрешение снято, то в итоговой настройке доступ на чтение пользователю будет разрешен;

 все пользователи и группы обладают одинаковым приоритетом при вычислении результирующих настроек;

 <u>запрет всегда приоритетнее разрешения</u> (если в одной группе пользователю разрешен доступ на чтение, а в другой - запрещен, то результирующей настройкой будет запрет).

Рассмотрим вычисление результирующих настроек пользователей на примерах.

#### Пример 1:

Настройка для группы Group:

	Разрешено	Запрещено
R	V	
W	V	

Настройка для пользователя User (входит в группу Group):

	Разрешено	Запрещено
R	V	
W		V

#### Результат:

Все пользователи (кроме *User*), входящие в группу *Group*, будут иметь разрешение на чтение (R) и запись (W).

Пользователь User будет иметь разрешение на чтение, запрет на запись.



> (входит в группу *Group*): Разрешено Зап

> > V

V

Настройка для пользователя User

Запрещено

# Пример 2:

Настройка для группы *Group*:

	Разрешено	Запрещено
R	V	
W		V

# Результат:

Все пользователи (кроме *User*), входящие в группу *Group*, будут иметь разрешение на чтение (R), запрет на запись (W).

R

W

Пользователь User будет иметь разрешение на чтение, запрет на запись.

# Пример 3:

Настройка для группы *Group*:

	Разрешено	Запрещено
R	V	
W		

Настройка для пользователя *User* (входит в группу *Group*):

	Разрешено	Запрещено
R	V	
W	V	

#### Результат:

Все пользователи (кроме *User*), входящие в группу *Group*, будут иметь разрешение на чтение (R), запрет на запись (W).

Пользователь *User* будет иметь разрешение на чтение и запись.

#### Пример 4:

Настройка для группы *Group*:

	Разрешено	Запрещено
R	V	
W		

Настройка для пользователя User (входит в группу Group):

	Разрешено	Запрещено
R	V	
W		V

#### Результат:

Все пользователи (кроме *User*), входящие в группу *Group*, будут иметь разрешение на чтение (R), запрет на запись (W).

Пользователь *User* будет иметь разрешение на чтение, запрет на запись.



## Пример 5:

Настройка для группы *Group1*:

Настройка для группы *Group2*:

Настройка для пользователя User (входит в группы Group1 и Group2):

	Разрешено	Запрещено		Разрешено	Запрещено		Разрешено	Запрещено
R	V		R	V		R	V	
W	V		W		V	W	V	

#### Результат:

Все пользователи (кроме *User*), входящие в группу *Group1*, будут иметь разрешение на чтение и запись.

Все пользователи (кроме *User*), входящие в группу *Group2*, будут иметь разрешение на чтение, запрет на запись.

Пользователь User будет иметь разрешение на чтение, запрет на запись.

46

# 5 Вкладка «Общее»

Вкладка **Общее** предназначена для отображения общей информации в зависимости от выбранного в иерархии элемента (сервера, группы или клиентской рабочей станции).

При выборе в иерархии сервера во вкладке отображается информация (рисунок 5.1):

– Статус сервера (сервер является головным или подчиненным в иерархии).

– Наименование серверной политики, назначенной серверу, и время ее применения.

– Служебная информация (информация об установленной ОС, IP адрес сервера, DNS имя сервера, часовой пояс выбранного сервера, порты для подключения клиентов и серверов).

 Количество серверов и клиентских рабочих станций, подчиненных выбранному серверу («Этот сервер») и общее количество серверов и клиентов во всей иерархии («Всего»).

Информация о последнем цикле опроса подчиненных серверов/клиентских компьютеров:

- **Статус** статус последнего цикла опроса подчиненных серверов/клиентских компьютеров (завершен, выполняется, не выполнялся);
- **Время начала** дата и время начала последнего цикла опроса подчиненных серверов/клиентских компьютеров;
- Время завершения дата и время завершения последнего цикла опроса подчиненных серверов/клиентских компьютеров;
- **Длительность** продолжительность последнего цикла опроса подчиненных серверов/клиентских компьютеров.



ХБло	жхост-Сеть 4			-	×
ጽ	Менеджер иерархий				
$\Phi$	C: 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	🛱 w09w13 🗐 0 🖵 3	Онлайн 🖲		с
冏	<ul> <li>ию9w13</li> <li>Все компьютеры</li> </ul>	Общее Политики Н	астройки <mark>Статистика</mark> События Лицензии		
	<ul> <li>C Fpynna 1</li> <li>Iocalhost</li> </ul>	Статус сервера	Мастер-сервер 🛈		
	<ul> <li>C Fpynna 2</li> <li>PC1</li> </ul>	Серверная политика Время применения	Политика сервера по умолчанию 13:23 22.07.2022		
	<ul> <li>C Fpynna 3</li> <li>C Fpynna 4</li> </ul>	Выпуск ОС	Windows 10 Pro for Workstations (64 Gera)		
		Версия ОС DNS имя	1809 SERVI.pki.local		
		IP адрес	10.72.9.65		
		Порт для подключения клиентов	999 🗇		
		Порт для построения иерархии серверов 🔞	59731		
		Часовой пояс	(UTC+03:00) Москва, Санкт-Петербург, Волгоград		
			Этот сервер/Всего 🔘		
		Серверов	1/1		
		Компьютеров	1/3		
		Последний цикл опрос	а аудита Подчиненные серверы 👻		
۲		Статус	завершен		

Рисунок 5.1 – Вкладка *Общее* при выборе в иерархии сервера

При выборе в иерархии группы во вкладке отображается информация (рисунок 5.2):

– Наименование серверной, клиентской политик и политики SafeNode System Loader, назначенных группе.

– Количество серверов и клиентских рабочих станций, входящих в выбранную группу.

🗙 Бло	кхост-Сеть 4				_	×
ஃ	Менеджер иерархий					
кÔя		QC	🗀 Все компьютеры			C
四	▼ ₩ w09w13		Общее Компьютерь	і Политики		
٢U	🔹 🗀 Все компьютеры		О группе			
	• 🗀 Группа 1					
	localhost		Клиентская политика	Политика клиента по умолчанию		
	🔹 🗀 Группа 2		Серверная политика	Политика сервера по умолчанию		
	PC1		Политика SafeNode	Политика SafeNode System Loader по умолизиию		
	• 🗀 Группа З		HOMMINKA SAFENOUE	Hommina Salehoue System Loader no ymonaanno		
	🗀 Группа 4			Bcero		
			Серверов	0		
			Компьютеров	0		

Рисунок 5.2 – Вкладка Общее при выборе в иерархии группы

При выборе в иерархии клиентской рабочей станции во вкладке отображается информация (рисунок 5.3):

– Режим функционирования рабочей станции и имеющиеся ограничения.

– Наименование клиентской политики, назначенной клиенту, и время ее применения.

– Служебная информация (информация об установленной ОС, IP адрес и DNS имя клиента).

– Модули – перечень разделов клиентской политики, возможных к назначению/не доступных для назначения на клиентской рабочей станции.

🗙 Бло	кхост-Сеть 4				_		×
ጽ	Менеджер иерархий						
кĴл		🙀 w09w13 Онлайн 🏾					С
ror fü	<ul> <li> <ul> <li>W09w13             <ul> <li>Все компьютеры</li> <li>Группа 1</li> <li>Calhost</li> <li>Группа 2</li> <li>PC1</li> <li>Группа 3</li> <li>Группа 4</li> </ul> </li> </ul> </li> </ul>	Общее Токены По Включен мягкий реж Клиентская политика Время применения Выпуск ОС Версия ОС IP адрес DNS имя	настро ким. Клиент БХ-Сеть ра Клиентская политика 1 18:36 22:03:2022 Windows 10 Pro (64 бита 1803 127.0.0.1 w09w13	йки События ботает в режиме огранич	енной функциональности	•	
		Модули 5/15					ł
		Управление входом в ОС	○     □     □	Контроль целостности файлов	Очистка оперативной памяти		I
		Сонтроль целостности среды	(i) Аудит доступа к медиафайлам	() Аудит запуска приложений	(i) Гарантированное удаление файлов		l
		і) Дискреционный доступ	і) Замкнутая программная среда	(і) Мандатный доступ	(i) Контроль устройств		I
		і) Контроль печати	(i) Расширенная аутентификация	(i) Доверенная загрузка			
ැ							

Рисунок 5.3 – Вкладка Общее при выборе в иерархии клиентской рабочей станции

# 6 Управление политиками

Политика – набор настроек механизмов безопасности и параметров работы СЗИ. Серверная политика определяет параметры работы серверов, клиентская политика определяет параметры работы клиентских рабочих станций.

Управление политиками осуществляется во вкладке *Политики* (рисунок 6.1) при выборе в иерархии основного или подчиненного серверов.

Принципы управления клиентской, серверной политиками и политикой SafeNode System Loader (создание, назначение, изменение, удаление) аналогичны.

🔀 Бло	жхост-Сеть 4							- 0	×	
윦	Менеджер иерархий									
к∱я		C	🎬 w09w13 🗮 0 🖵 3 Онлайн •						С	
6	▼ ∰ w09w13		Общее Политики Настройки (	Статис	тика События	Лицензии				
-	<ul> <li>все компьютеры</li> <li>Группа 1</li> </ul>		④ Создать С' Отвязать Изменить	ت ت	/далить		⊻ Имі	порт 之 З	)кспорт	
	localhost		• Клиентские политики - 3	ipyn	na	статус	Создано	Изменено		
	PC1		Клиентская политика 1		Группа 1	Активна	22.03.2022 17:59	22.03.202	2 18:37	
	• 🗀 Группа З		Клиентская политика 2		Группа 2	Активна	22.03.2022 18:45	22.03.202	2 18:45	
	🗀 Группа 4		Политика клиента по умолчанию		Все компьютеры	Активна	22.03.2022 16:57	22.03.202	2 18:32	
			▼ Политика SafeNode System Loader - 3							
			Политика SafeNode System Loader по у		Все компьютеры	Активна	22.03.2022 16:57	22.03.202	2 16:57	
			Политика SNSL 1		Группа 1	Активна	22.03.2022 18:46	22.03.202	2 18:46	
			Политика SNSL 2		Группа 2	Активна	22.03.2022 18:47	22.03.202	2 18:47	
			<ul> <li>Серверные политики - 3</li> </ul>							
			Политика сервера по умолчанию		Все компьютеры	Активна	22.03.2022 16:57	22.03.202	2 16:57	
			Серверная политика 1		Группа 1	Активна	22.03.2022 17:59	22.03.202	2 17:59	
			Серверная политика 2		Группа 2	Активна	22.03.2022 18:45	22.03.202	2 18:45	
								_		
şĝş			Клиентские: 3 Серверные: 3 SafeNode: 3							

Рисунок 6.1 – Управление политиками

# 6.1 Создание политик

Создание клиентской или серверной политики доступно во вкладке **Политики**, по кнопке <sup>(+)</sup> Создать</sup> (рисунок 6.1) или выбором пункта **Создать политику** в контекстном меню.

В появившемся окне (рисунок 6.2) выберите тип политики, которую хотите создать.



При необходимости скопируйте параметры любой другой созданной ранее политики того же типа, установив переключатель *Скопировать параметры другой политики выбранного типа* и выбрав нужную политику из списка имеющихся.

🔀 Создание политики							;
Выберите тип политик	си						
en nosemec							
🖵 Клиентская политика							
🗄 Серверная политика							
B Политика SafeNode System Lo	ader						
Скопировать параметры ,	другой политики выбра	нного типа					
Отобразить все 👻 🔍 Поиск кл	иентских политик						
Hammingaarane	fpynna	Cranyc	Создано	Изменено	Коллівнтарий		
Слиентская политика 1	🗀 Fpynna 1	Активна	21.09.2021 12:38	21.09.2021 12:38			
Слиентская политика 2	C Fpynna 2	Активна	21.09.2021 12:38	21.09.2021 12:38			
Толитика клиента по умолчанию	🗅 Все компьютеры	Активна	09.09.2021 13:00	21.09.2021 18:44			
cero: 3							
						Далее	Отмена

Рисунок 6.2 – Создание политики

Во вкладке *Общее* (рисунок 6.3) задайте наименование политики и выберите группу, которой будет назначена создаваемая политика.



🗙 Создание клиентской политик	и на основе: Клиентская п	олитика 1				×
Общее	Имя и группа п	олитики				
Windows Linux	Наименование* Группа ①	Клиентская политика Выбрать	5			
Мягкий режим	Комментарий					
				Назад	Создать	Отмена

Рисунок 6.3 – Добавление политики

Eсли группа не задается сразу при создании политики, политика остается не привязанной к группе и находится в состоянии *Не активна*.

В дальнейшем, созданную политику можно привязать к любой группе.

Остальные вкладки окна позволяют задать определенный набор настроек механизмов безопасности и параметров работы СЗИ, применяемых к группе, для которой создавалась политика. Описание настроек приведено в разделах **«Описание клиентских политик» и «Описание серверных политик»**.

После настройки всех необходимых параметров создаваемой политики нажмите кнопку *Создать*. Новая политика добавится в список политик (рисунок 6.2).

В списке политик можно просмотреть наименование политики, группу, к которой политика привязана, статус, в котором находится политика, дату создания политики и дату внесения в нее изменений.

# 6.2 Назначение политик группе

Для назначения политики группе, во вкладке *Политики* перейдите на строку с политикой, которую требуется привязать к группе, и нажмите кнопку <sup>СО Привязать</sup>

72410666.00063-04 95 01-01



(рисунок 6.1).

В появившемся окне (рисунок 6.4) выберите группу, к которой привязывается выбранная политика и нажмите **Привязать**.

🗙 Выбор группы для применения политики							
+ Q							
▼ ₩ w09w13							
🝷 🗋 Все компьютеры							
🗅 Группа 1							
🗅 Группа 2							
🗀 Группа З							
🗅 Группа 4							
	Отмена						

Рисунок 6.4 – Выбор группы для привязки политики

В случае, если у привязываемой группы уже имеется действующая политика (рисунок 6.5), при нажатии кнопки **Продолжить**, политика, привязанная ранее к группе, будет отвязана от группы и перейдет в статус **Не активна**, действующей политикой для группы станет новая политика.





Рисунок 6.5 – Назначение новой политики группе

В случае, если привязываемая к группе политика, уже была привязана к другой группе (рисунок 6.6), при нажатии кнопки **Продолжить**, политика будет отвязана от предыдущей группы и станет действующей политикой для новой группы. В группе, от которой политика была отвязана, станет действующей политика родительской группы.



Рисунок 6.6 – Открепление политики от предыдущей группы

Политики корневой группы «Все компьютеры», созданные в системе по умолчанию, не могут быть привязаны к другой группе или откреплены от корневой группы «Все компьютеры» (рисунок 6.7).





Рисунок 6.7 – Действия со стандартными политиками

Для открепления политики от группы к которой она привязана, во вкладке **Политики** перейдите на строку с политикой, которую требуется открепить, и нажмите кнопку С Отвязать (рисунок 6.1).

В появившемся окне (рисунок 6.8) подтвердите действие, нажав кнопку Отвязать.



Рисунок 6.8 – Открепление политики от группы

Открепить возможно только политику, привязанную к группе, т.е. находящуюся в состоянии *Активна*.

После открепления от группы, политика перестанет быть действующей и изменит статус на *Не активна*. В дальнейшем, политику можно привязать к любой группе.

# 6.3 Изменение политик

Для изменения политики, во вкладке *Политики* перейдите на строку с политикой, в которую необходимо внести изменения, и нажмите кнопку *Изменить* (рисунок 6.1).

В появившемся окне (рисунок 6.9) возможно внести необходимые изменения в

настройки механизмов безопасности для данной политики, изменить наименование политики и изменить группу, к которой привязана политика.

X Изменение клиентской политики: Клиентская политика 1						
Общее	Имя и группа г	толитики				
Windows	Наименование*	Клиентская политика 1				
Linux	Группа 🛈	ြ Группа 1 ၎င်				
Мягкий режим						
	Комментарий					
	L					
			Ок	Отмена		

Рисунок 6.9 – Внесение изменений в политику

После внесения изменений нажмите кнопку *Ок* для применения всех изменений и закрытия окна редактирования политики.

# 6.4 Удаление политик

Для удаления политики, во вкладке *Политики* перейдите на строку с политикой, в которую необходимо удалить, и нажмите кнопку <sup>Удалить</sup> (рисунок 6.1).

В случае удаления действующей политики, привязанной к группе (рисунок 6.10), при нажатии кнопки **Да**, политика удалится, при этом для группы, к которой была привязана удаляемая политика станет действующей политика родительской группы.



🔀 Блокхост-Сеть 4	×
Внимание	
Политика привязана к группе «Группа 1». Настройки механизмов безопасности компьютеров, находящихся в группе и подгруппах, будут изменены. Вы также потеряете все настройки политики.	
Удалить Отмена	

Рисунок 6.10 – Удаление действующей политики

# 6.5 Экспорт/импорт политик

Для экспорта политики, во вкладке **Политики** перейдите на строку с политикой, которую необходимо экспортировать на внешнее хранилище данных, и в правом верхнем углу вкладки нажмите на кнопку *Зкспорт* (рисунок 6.11).

🗙 Бло	кхост-Сеть 4					- 🗆 ×
ጽ	Менеджер иерархий					
кţл		🛱 w09w13 🗮 0 🖵 3 Онлайн 🖲				С
cд	▼ ∰ w09w13	Общее Политики Настройки	Статистика События	Лицензии		
٢U	<ul> <li>Все компьютеры</li> </ul>	④ Создать С Отвязать Изменита	ы 🔟 Удалить		± Им	порт 👌 Экспорт
0	• 🗅 Группа 1					
	localhost	Наименование	Группа	Статус	Создано	Изменено
	🔻 🗀 Группа 2	<ul> <li>Клиентские политики - 4</li> </ul>				
	PC1	Клиентская политика 1	🗀 Группа 1	Активна	22.03.2022 17:59	22.03.2022 18:37
	Группа 3	Клиентская политика 2	🗀 Группа 2	Активна	22.03.2022 18:45	22.03.2022 18:45
	🗀 Группа 4	Клиентская политика 5		Не активна	22.03.2022 18:49	22.03.2022 18:49

Рисунок 6.11 – Экспорт/импорт политик

В следующем окне укажите нужную директорию или выберите внешний носитель информации куда необходимо сохранить экспортируемый файл, задайте имя файла и нажмите **Сохранить**. Экспортируемая политика сохранится в заданном месте (рисунок 6.12).



🗙 Блокхост-Сеть 4	×
Политика "Клиентская политика 1" успешно экспортирована.	
04	
OK	

Рисунок 6.12 – Успешное завершение экспорта политики

Для импорта политики, во вкладке *Политики* в правом верхнем углу вкладки нажмите

на кнопку 🖄 Импорт (рисунок 6.11).

В следующем окне укажите нужную директорию или выберите внешний носитель информации откуда необходимо импортировать файл, содержащий политику, и нажмите **Открыть**.

В окне импорта политики (рисунок 6.13) можно изменить название импортируемой политики, задать или просмотреть набор настроек механизмов безопасности и параметров работы СЗИ, настроенных в политике, и назначить импортируемую политику группе. Для продолжения импорта нажмите кнопку *Импортировать*.



🗙 Импорт клиентской политики	и из файла: clientpolicy.bhpol	×
Общее	Имя и группа политики	
Windows	Наименование* Клиентская политика 1 - 2	
Мягкий режим	Труппа 🛈 Выбрать	
	Комментарий	
	Импортировать Отмена	

Рисунок 6.13 – Импорт политики

После успешного выполнения импорта политика отобразится в списке политик (рисунок 6.14).

🗙 Бло	жхост-Сеть 4						- 🗆	×
ጽ	Менеджер иерархий							
к <sup>ф</sup> я	C. @ <b>3</b> 5	Q C	🏭 w09w13 🗮 0 🖵 3 Онлайн •					С
四	▼ III w09w13		Общее Политики Настройки С	татистика События	Лицензии			
rω	• 🗀 Все компьютеры		🕀 Создать 🗢 Привязать 🖉 Изменить	🔟 Удалить		⊥ Им	порт 👌 Эксп	юрт
8	▼ ☐ Группа1		Наименование	Группа	Статус	Создано	Изменено	
	ter localhost		<ul> <li>Клиентские политики - 5</li> </ul>					
	PC1		Клиентская политика 1	🗀 Группа 1	Активна	22.03.2022 17:59	22.03.2022 18	3:37
	Группа 3		Клиентская политика 1 - 2		Не активна	22.03.2022 19:06	22.03.2022 19	):06
	🗀 Группа 4		Клиентская политика 2	🗀 Группа 2	Активна	22.03.2022 18:45	22.03.2022 18	3:45
			Клиентская политика 5		Не активна	22.03.2022 18:49	22.03.2022 18	3:49
			Политика клиента по умолчанию	🗀 Все компьютеры	Активна	22.03.2022 16:57	22.03.2022 18	3:32
			▼ Политика SafeNode System Loader - 3					
			Политика SafeNode System Loader по у	🗀 Все компьютеры	Активна	22.03.2022 16:57	22.03.2022 16	i:57
			Политика SNSL 1	🗅 Группа 1	Активна	22.03.2022 18:46	22.03.2022 18	3: <b>46</b>

Рисунок 6.14 – Успешное завершение импорта политики

# 6.6 Примеры наследования политик

## Пример 1:

Рассмотрим иерархию групп следующей структуры (рисунок 6.15):

– верхний уровень – группа «Все компьютеры», с политиками «Политика клиента по умолчанию» и «Политика сервера по умолчанию»,

- подчиненные группы:
  - «Группа 1», с действующими политиками «Клиентская политика 1» и «Серверная политика 1»;
  - «Группа 2», не имеющая собственных действующих политик, действующими политиками для группы являются наследуемые политики «Политика клиента по умолчанию» и «Политика сервера по умолчанию» родительской группы «Все компьютеры».



Рисунок 6.15 – Иерархия групп и наследование политик до внесения изменений

При удалении действующей клиентской политики группы «Группа 1», политика «Клиентская политика 1» отвязывается от группы «Группа 1» и удаляется. Действующей политикой для группы «Группа 1» становится наследуемая политика «Политика клиента по умолчанию», являющаяся действующей в родительской группе «Все компьютеры» (рисунок 6.16).

X Бло	кхост-Сеть 4					-		×
Å	Менеджер иерархий							
к <sup>†</sup> л		С	🗀 Группа 1 🗮 0 🖵 1					С
络	▼ E w09w13		Общее Компьютеры Политики					
٢u	🝷 🗋 Все компьютеры		Э Создать и привязать • • Просмотреть		⊻	Импорт	رگ Эксі	порт
۲	• С Группа 1		Наименование	Наследование	Создано	Изменено		
	» 🗀 Группа 2		<ul> <li>Клиентская политика</li> </ul>					
			🦌 Политика клиента по умолчанию	Все компьютеры	22.03.2022 16:57	22.03.202	2 18:32	
			<ul> <li>Серверная политика</li> </ul>					
			Серверная политика 1		22.03.2022 17:59	22.03.202	2 17:59	
			▼ Политика SafeNode System Loader					
			Политика SNSL 1		22.03.2022 18:46	22.03.202	2 18:46	

Рисунок 6.16 – Наследование политик после удаления политики «Клиентская политика 1»

# **Пример 2**:

Рассмотрим иерархию групп следующей структуры (рисунок 6.17):

– верхний уровень – группа «Все компьютеры», с действующими политиками «Политика клиента по умолчанию» и «Политика сервера по умолчанию»,

- подчиненные группы:
  - «Группа 1», не имеющая собственных действующих политик, действующими политиками для группы являются наследуемые политики «Политика клиента по умолчанию» и «Политика сервера по умолчанию» родительской группы «Все компьютеры»;
  - «Группа 2», с действующими политиками «Клиентская политика 2» и «Серверная политика 2»;
  - «Группа 3», с действующими политиками «Клиентская политика 3» и «Серверная политика 3».

🗙 Бло	жхост-Сеть 4					-		×
윦	Менеджер иерархий							
кÔл	C, ŵ \$	QC	🗅 Группа 1 🗮 0 🖵 1					С
<u>s</u> ع	▼ ₩ w09w13		Общее Компьютеры Политики					
٢U	• 🗅 Все компьютеры		🕀 Создать и привязать 🔹 👁 Просмотреть		4	Импорт 👌	; Экспо	рт
8	Группа 1		Наименование	Наследование	Создано	Изменено		
	Группа 2		<ul> <li>Клиентская политика</li> </ul>					
	🗅 Группа 3		Политика клиента по умолчанию	Все компьютеры	22.03.2022 16:57	22.03.2022 1	18:32	
			<ul> <li>Серверная политика</li> </ul>					
			Политика сервера по умолчанию	Все компьютеры	22.03.2022 16:57	22.03.2022 1	L6:57	
			* Политика SafeNode System Loader					
			🖣 Политика SafeNode System Loader по умолчанию	Все компьютеры	22.03.2022 16:57	22.03.2022 1	16:57	

a)



🗙 Бло	жхост-Сеть 4					- 0	×
윦	Менеджер иерархий						
кĴя		Q C	🗀 Группа З				С
70	<ul> <li>₩09w13</li> <li>Все компьютеры</li> </ul>		Общее Компьютеры Политики	с'с Отвязать 🗑 Удалить	¥	Импорт 👌 Эксі	порт
۲	<ul> <li>Группа 1</li> <li>Группа 2</li> </ul>		Наименование	Наследование	Создано	Изменено	
	🗀 Группа 3		<ul> <li>Клиентская политика</li> <li>Клиентская политика 3</li> </ul>		23.03.2022 08:50	23.03.2022 08:50	
			<ul> <li>Серверная политика</li> </ul>				
			Серверная политика 3		23.03.2022 08:51	23.03.2022 08:51	R
			<ul> <li>Политика SafeNode System Loader</li> <li>Политика SNSL 3</li> </ul>		23.03.2022 08:51	23.03.2022 08:51	

в)

Рисунок 6.17 – Иерархия групп и наследование политик до внесения изменений

При перемещении групп «Группа 1» и «Группа 2» в группу «Группа 3», «Группа 3» становится родительской для групп «Группа 1» и «Группа 2». Для группы «Группа 1» действующими политиками становятся политики «Клиентская политика 3» и «Серверная политика 3» новой родительской группы «Группа 3», так как эта группа не имеет собственных действующих политик. Политики «Клиентская политика 2» и «Серверная политика 2», привязанные к группе «Группа 2» после перемещения группы «Группа 2» остаются привязаны к данной группе (рисунок 6.18).

🗙 Бло	жхост-Сеть 4					-		Х
윦	Менеджер иерархий							
÷.	С; Ш ☐ С • Щ w09w13 • ☐ Все компьютеры • ☐ Группа 3 • ☐ Группа 1 • ☐ Группа 2	Q C	<ul> <li>□ Группа 1 □ □ □ □ □ 1</li> <li>Общее Компьютеры</li> <li>④ Создать и привязать ▼</li> <li>Наименование</li> <li>• Клиентская политика 3</li> <li>• Серверная политика 3</li> <li>• Серверная политика 3</li> <li>• Политика ShSL 3</li> </ul>	Политики ● Просмотреть Насле Групп Loader Групп	дование Создано па 3 23.03.2022 0 па 3 23.03.2022 0	<ul> <li>⊻ Импор Измен</li> <li>8:50 23.03.2</li> <li>8:51 23.03.2</li> </ul>	от È Эксг ено 2022 08:50 2022 08:51 2022 08:51	С
			a)					
			1					
🗙 Бло	жхост-Сеть 4		,			-		×
X Бло	жост-Сеть 4 Менеджер иерархий		,			-		×
Х Бло	жост-Сеть 4 Менеджер иерархий Стай фаба	QC	С Группа 2 📑 0 🖵 2			-		c
Х Бло С	жхост-Сеть 4 Менеджер иерархий Ста ба ба • Щ мо9м13	QC	, С Группа 2 🗟 0 🖵 2 Общее Компьютеры	Политики		_		c
Х Бло В П П	жхост-Сеть 4 Менеджер иерархий Ст 🖻 🗐 🛱 * 📾 v09w13 * 🖸 Все компьютеры	Q C	<ul> <li>Группа 2 ☐ 0 ♀ 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать ▼</li> </ul>	Политики «Изменить Ссотвязать П	🗑 Удалить		D T 👌 Экст	С
<mark>х</mark> Бло 66 Ф 10 П	ахост-Сеть 4 Менеджер иерархий С	Q C	<ul> <li>Группа 2 目 0 早 2</li> <li>Общее Компьютеры</li> <li>Ф Создать и привязать ▼</li> <li>Наименование</li> </ul>	Политики «Изменить Ссотвязать П Насле	🐨 Удалить дование Создано	<u>↓</u> Импор Изменч	от <u>д</u> Эксп	С
<mark>х</mark> Бло & Ф П	жхост-Сеть 4 Менеджер иерархий Ст 🖻 🗐 🗐 * 🖼 w09w13 * 🖻 Все компьютеры - Ст Группа 3 - Ст Группа 1	QC	<ul> <li>Группа 2 目 0 ♀ 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать ▼</li> <li>Наименование</li> <li>Клиентская политика</li> </ul>	Политики «Изменить Ссотвязать { Насле	छ Удалить дование Создано		от 👌 Экст	С
Х Бло	ахост-Сеть 4 Менеджер иерархий С	Q C	<ul> <li>Группа 2 目 0 早 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать ▼</li> <li>Наименование</li> <li>Клиентская политика</li> <li>Клиентская политика 2</li> </ul>	Политики «Изменить Су Отвязать П Насле	교 Удалить дование Создано 22.03.2022 1	Импор Изменя 8:45 22.03.2	от & Экст ено 2022 18:45	С
<mark>х</mark> Бло & Ф П	жхост-Сеть 4 Менеджер иерархий Ф 👜 🗐 🛱 • 📾 v09w13 • 🖻 Все компьютеры • 🗅 Группа 3 • С Группа 1 • С Группа 2	QC	<ul> <li>Группа 2 ☐ 0 ♀ 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать ▼</li> <li>Наименование</li> <li>Клиентская политика</li> <li>Клиентская политика 2</li> <li>Серверная политика</li> </ul>	Политики & Изменить Сс Отвязать П Насле	교 Удалить дование Создано 22.03.2022 1		от с Экст ено 2022 18:45	С
<mark>}</mark> Бло ♣ ₽ П	жхост-Сеть 4 Менеджер иерархий □ @ @ @ • @ w09w13 • □ Все компьютеры • □ Группа 3 • □ Группа 1 • □ Группа 2	Q C	<ul> <li>Группа 2 目 0 早 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать ▼</li> <li>Наименование</li> <li>Клиентская политика</li> <li>Клиентская политика 2</li> <li>Серверная политика 2</li> </ul>	Политики « Изменить «Сотвязать ( Насле	III Удалить дование Создано 22.03.2022 1 22.03.2022 1	<ul> <li></li></ul>	от & Экст ено 2022 18:45	С
<mark>х</mark> Бло & Ф П	жхост-Сеть 4 Менеджер иерархий Ф 👜 🗐 🛱 • 📾 v09w13 • 🖻 Все компьютеры • 🗅 Группа 3 • С Группа 1 • С Группа 2	QC	<ul> <li>С Группа 2 В 0 ⊋ 2</li> <li>Общее Компьютеры</li> <li>Создать и привязать *</li> <li>Наименование</li> <li>Клиентская политика</li> <li>Клиентская политика 2</li> <li>Серверная политика 2</li> <li>Политика SafeNode System</li> </ul>	Политики	<ul> <li>Удалить</li> <li>дование</li> <li>Создано</li> <li>22.03.2022 1</li> <li>22.03.2022 1</li> </ul>	<ul> <li></li> <li></li> <li></li> <li>Импор</li> <li>Измене</li> <li>8:45</li> <li>22.03.2</li> <li>8:45</li> <li>22.03.2</li> </ul>	от ѐ Эксг ено 2022 18:45 2022 18:45	С
<mark>) Х</mark> Бло	жхост-Сеть 4 Менеджер иерархий С	Q C	<ul> <li>С Группа 2 В 0 ₽ 2</li> <li>Общее Компьютеры</li> <li>Осоздать и привязать *</li> <li>Наименование</li> <li>Клиентская политика</li> <li>Клиентская политика 2</li> <li>Серверная политика 2</li> <li>Политика SafeNode System Политика SNSL 2</li> </ul>	Политики Изменить СС Отвязать Насле Loader	II Удалить дование Создано 22.03.2022 1 22.03.2022 1	<ul> <li> </li> <li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	от & Экст ено 2022 18:45 2022 18:45	С

Рисунок 6.18 – Иерархия групп и наследование политик после перемещения групп

# 6.7 Синхронизация политик

В ряде случаев при назначении политики группе или внесении изменений в настройки механизмов политики может потребоваться синхронизация заданных в политике настроек по всей иерархии дочерних групп и клиентских рабочих станций, на которые оказывает влияние политика родительской группы.

72410666.00063-04 95 01-01

# 6.7.1 Синхронизация политики с пересчетом КС файлов

Выполнять синхронизацию политики с пересчетом контрольных сумм (КС) файлов целесообразно при выявлении нарушений целостности файлов, поставленных на контроль в механизме **Аудит целостности файлов**. Целостность поставленных на контроль файлов обеспечивается путем проверки КС, вычисленных при постановке файлов на контроль, и при каждой проверке целостности таких файлов формируются события аудита об обнаруженных нарушениях в КС файлов.

Синхронизация политики с пересчетом КС файлов доступна в дереве иерархии при выборе в контекстном меню группы или клиентской рабочей станции пункта *Синхронизировать политику* — *С пересчетом контрольных сумм файлов* (рисунок 6.19).

🗙 Бло	окхост-Сеть 4		-	×
ጽ	Менеджер иерархий			
к <u></u> †я	C. m g g g	🖬 w09w13 Онлайн •		С
冏	▼ ∰ w09w13	Общее Токены Пользователь Настройки События		
10	• 🗋 Все компьютеры	О компьютере		
=	▼ ☐ Группа 1			
	localhost	Клиентская политика Политика клиента по умолчанию		
	<ul> <li>Группа 2</li> <li>Удалить</li> </ul>	именения 08:56 23.03.2022		
	🗅 Группа З 🎖 Вырезать	C Min Jawa 10 Per (64 Sume)		
	🛱 Синхронизирова	ъ политику 🕨 💽 С пересчетом контрольных сумм файлов		
	О компьютере	🐼 Без пересчета контрольных сумм файлов		

Рисунок 6.19 – Синхронизация политик с пересчетом КС файлов

После синхронизации политики выполняется пересчет КС файлов, в которых были выявлены нарушения, и при последующей проверке целостности КС файлов соответствуют эталонным значениям, фиксация событий в журнале аудита не производится.

# 6.7.2 Синхронизация политики без пересчета КС файлов

Синхронизация политики без пересчета КС файлов позволяет выполнить повторное принудительное назначение политики родительской группы клиентским рабочим станциям, на которые оказывает влияние политика, в случае, если при назначении или изменении политики возникли ошибки.

Синхронизация политики без пересчета КС файлов доступна в дереве иерархии при выборе в контекстном меню группы или клиентской рабочей станции пункта *Синхронизировать политику* — *Без пересчета контрольных сумм файлов* (рисунок 6.19).

# 7 Описание клиентских политик

Клиентские политики определяют параметры работы клиентских рабочих станций. Для настройки в клиентских политиках доступны следующие механизмы:

1) Для клиентских рабочих станций под управлением OC Windows:

– **Управление входом в ОС** (управление параметрами аутентификации пользователей при входе на клиентские рабочие станции под управлением ОС семейства Windows).

- **Сложность паролей** (управление ограничениями при задании пароля и PINкода токена пользователя, настройка количества неправильных попыток входа).

- *Контроль устройств* (разграничение доступа к отчуждаемым носителям информации).

– **Очистка оперативной памяти** (управление очисткой всей свободной физической памяти поставленных на контроль приложений после их завершения).

 Гарантированное удаление файлов (настройка гарантированного удаления объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления).

– **Аудит целостности файлов** (отслеживание изменений в контрольных суммах заданных файлов).

– **Аудит запуска приложений** (регистрация событий аудита запуска и прекращения работы исполняемых файлов).

– **Аудит печати** (регистрация событий аудита при печати документов для всех приложений).

 Аудит доступа к медиафайлам (регистрация событий аудита при попытках доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям).

– **Контроль целостности среды** (отслеживание изменений в списке установленных программ, служб, драйверов, каталогах общего доступа, контроль аппаратной среды).

- *Журнал аудита* (управление настройками журнала аудита).

2) Для клиентских рабочих станций под управлением OC Linux:

 Управление входом в ОС (управление параметрами аутентификации пользователей при входе на клиентские рабочие станции под управлением ОС семейства Linux);

- **Сложность паролей** (управление ограничениями при задании пароля и PIN-кода токена пользователя, настройка количества неправильных попыток входа);

- *Контроль устройств* (разграничение доступа к отчуждаемым носителям информации).



 $(\mathbf{i})$ 

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

- *Контроль целостности файлов* (отслеживание изменений в контрольных суммах заданных файлов);

– **Очистка оперативной памяти** (управление очисткой всей свободной физической памяти поставленных на контроль приложений после их завершения)<sup>3</sup>.

3) Для всех клиентских рабочих станций:

Мягкий режим (настройка возможности работы в мягком режиме).

Для всех клиентских политик запрещено добавление в политику следующих доменных групп:

- для клиентов под управлением ОС Linux (рисунок 7.1):
  - BUILTIN;
  - Destributed.
- для клиентов под управлением OC Windows:
  - Destributed.

Х Добавление пользователей							
	<u>Домены</u> Компьютеры Псевдонимы	Пользователи и группы	Будут добавлены				
- \$ I	oki.local (AD)	Q. Введите запрос и нажмите Enter					
C	D Builtin	0N# * 0N0					
C	Computers	ရိပ္မီနဲ Access Control ရိပ္မီနဲ Accean Встроенные группы недоступн	ы для выбора				
C	Domain Controllers	්රී Administrators					
C	ForeignSecurityPrincipals	åons Backup Operat					
C	Managed Service Accounts	åons Certificate Servi					
C	Users	aိ Cryptographic	Выбранные пользователи				
		aိြီရီ Distributed CO	отсутствуют				
		aັດດີຣ Event Log Read					
		ီမြီး Guests					
		aິດ໊ຣ Hyper-V Admin					
<table-cell-rows> Доба</table-cell-rows>	авить домен	Bcero: 27					
			Добавить Отмена				

Рисунок 7.1 – Запрет добавления доменных групп

Принудительное наследование в разделах политики может быть установлено целиком на всем разделе, на списке элементов, и на отдельных элементах или группах.

Установка принудительного наследования на всем разделе запрещает изменение всех элементов раздела на нижестоящих уровнях иерархии. Вышестоящая политика

<sup>&</sup>lt;sup>3</sup> Механизм очистки оперативной памяти доступен только для клиентских рабочих станций под управлением РЕД ОС.

наследуется в неизменном виде. Администраторам нижестоящих уровней иерархии не доступно изменение, удаление или добавление элементов (подробнее в разделе *«Принудительное наследование»*).

# 7.1 Управление входом в OC Windows

В разделе **«Управление входом в ОС»** клиентской политики администратор может управлять параметрами аутентификации пользователей или группы пользователей клиентских рабочих станций под управлением OC Windows, к которым применяется данная политика.

Настройки входа в ОС представляют собой список пользователей и групп с сопоставленными им настройками аутентификации. Для всех пользователей, которые не обозначены в данном списке (напрямую или через группы) вход на клиентские рабочие станции будет запрещен.

# 7.1.1 Общий принцип аутентификации пользователя в СЗИ от НСД «Блокхост-Сеть 4»

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»;
  - 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);
  - сверка введенного пароля с копией в локальной базе данных клиента

# 72410666.00063-04 95 01-01

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 в документе «СЗИ от НСД «Блокхост-Сеть 4». Описание применения».

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

Предусмотрены следующие возможные виды входа пользователя в систему, описанные в таблице 7.1.

Аутентификация	Описание	Возможные виды	Комментарий		
		входа			
По токену:	Аутентификация	• вход по	При входе пользователя СЗИ		
- с записанным	возможна только с	сертификату на	выполняет проверку		
паролем или	использованием	токене;	принадлежности токена		
безопасный вход по	токена, назначенного	• вход по паролю	пользователю		
паролю (БВПП);	пользователю с	на токене.			
- с сертификатом.	помощью				
	подсистемы				
	управления токенами				
	СЗИ				
По паролю	Аутентификация с	• вход по паролю,	При входе пользователя СЗИ		
	помощью пароля,	вводимому	выполняет проверку		
	вводимого	вручную.	введенного пароля с паролем		
	пользователем		пользователя, хранящимся в		
	вручную		БД <sup>4</sup>		
Аутентификация	Аутентификация	любой возможный	При входе пользователя		
Windows/Linux	пользователя,	вид входа,	идентификационные данные		
	предполагающая	поддерживаемый	пользователя проверяются		
	полное доверие	средствами ОС	средствами операционной		
	проверкам входа,		системы, СЗИ только		
	выполняемым		осуществляет проверку в		
	средствами ОС		своей базе наличия учетной		
			записи пользователя,		
			выполняющего вход в ОС		

Таблица 7.1 – Возможные виды входа пользователя в систему

#### 7.1.2 Аутентификация по паролю на токене

Аутентификация пользователя с использованием безопасного входа по паролю на токене предоставляет возможность защищенного входа пользователя в ОС, при этом

<sup>&</sup>lt;sup>4</sup> Настройка входа пользователя по паролю осуществляется в настройках клиентской рабочей станции, если вышестоящим сервером установлено разрешение на данную настройку. Подробное описание настройки приведено в разделе *«Проверка пароля в СЗИ»*.

пользователю не требуется запоминать пароль и вводить его при каждом входе в систему, сгенерированный пароль хранится на токене и пользователю для входа необходимо предъявить только PIN-код к ключевому носителю, используемому для входа.

Аутентификация с использованием БВПП возможна:

1) По PIN-коду со сменой пароля.

Для перехода на аутентификацию с использованием токена с БВПП со сменой пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

2) По PIN-коду без смены пароля.

Для перехода на аутентификацию с использованием токена с БВПП без смены пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

3) По паролю без PIN-кода.

Вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом пароля пользователя. PIN-код токена вводить не требуется.

Назначение токена пользователю с использованием БВПП описано в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора Блокхост-Сеть 4. Часть 5. Управление токенами».

# 7.1.3 Аутентификация по цифровому сертификату на токене

Аутентификация по цифровому сертификату на токене предоставляет возможность защищенного входа в ОС по сертификату для входа, выданному пользователю.

Для аутентификации пользователя по цифровому сертификату необходимо настроить возможность входа пользователей по сертификатам и выдать токен с сертификатом пользователю с помощью подсистемы управления токенами (подробное описание приведено в документах «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора Блокхост-Сеть 4. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA», «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора Блокхост-Сеть 4. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag»).

72410666.00063-04 95 01-01

При этом сертификат для входа может быть выпущен:

- средствами подсистемы управления токенами (должен быть развернут удостоверяющий центр (УЦ) с возможностью выдачи пользователю сертификатов необходимого типа);

сторонними средствами.

## 7.1.4 Добавление пользователей или групп пользователей

Для добавления пользователей или группы пользователей, которым требуется установить настройки входа, перейдите в раздел политики **«Управление входом в ОС»** в режиме изменения клиентской политики на сервере или в группе рабочих

🗙 Изменение клиентской полит	ики: Политика клиента по умолчанию	)			×
Общее	Управление входом в				
Windows	Список пользователей 🗗 Дог	полнительные настройки			
Управление входом в ОС					
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	pki.local\user02	Active Directory	По токену		
удаление файлов	°∩° Все пользователи		Тип входа		
Аудит целостности файлов			Tun	Daapauura	Zanoatuti
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
Аудит доступа к медиафайлам					
Контроль целостности среды					
Журнал аудита					
Linux					
Мягкий режим	Пользователей: 2 Групп: 1				
			Ок Отмена		

Рисунок 7.2 – Управление входом в ОС

В появившемся окне (рисунок 7.4) добавьте учетную запись пользователя или выберите группу пользователей, которым необходимо установить настройку входа.

Для добавления доступны:

– доменные пользователи (во вкладке **Домены**). Для добавления доменного пользователя во вкладке **Домены** выберите нужный домен или, при отсутствии



необходимого домена в списке, добавьте его по ссылке • Добавить домен (рисунок 7.4 а).

– локальные пользователи рабочей станции (во вкладке Компьютеры). Для добавления локального пользователя перейдите во вкладку Компьютеры и выберите рабочую станцию, локального пользователя которой требуется добавить (рисунок 7.4 б). Возможна фильтрация выбираемых рабочих станций для поиска машин только в состоянии Онлайн, или ввод имени рабочей станции для поиска по иерархии.

 группы пользователей Все пользователи и Локальные пользователи (во вкладке Псевдонимы). Псевдоним Все пользователи подразумевает всех доменных и локальных пользователей, псевдоним Локальные пользователи локальных пользователей клиентской рабочей станции (рисунок 7.4 в).

Домены во вкладке Домены подразделяются на:

- системные домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения. Системный домен невозможно удалить из списка.

пользовательские домены, которые добавляются по кнопке • Добавить домен. При подключении к пользовательскому домену всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется). Пользовательский домен возможно удалить из списка.

**(;**)

Администратор имеет возможность выполнить подключение/переподключение к домену под нужной ему учетной записью (ввести логин/пароль).

Если при подключении к домену возникает ошибка вида (рисунок 7.3), необходимо настроить подключение к домену по протоколу ldaps с установкой ssl-сертификатов (подробное описание приведено в документе «СЗИ от НСД «Блокхост-Сеть». Руководство администратора безопасности. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA»).




Рисунок 7.3 – Ошибка при подключении к домену

При выборе домена или компьютера, в средней части окна отобразятся учетные записи, доступные для добавления в список пользователей. Выбранные пользователи дублируются в правой части окна.

🗙 Добавление пользователей для группы "Все компьютеры"		×
<mark>Домены</mark> Компьютеры Псевдонимы	Пользователи и группы	Будут добавлены - 2
▼ 🖑 pki.local (AD)	Введите запрос и нажмите Enter  Имя     ФИО	e user01 pkilocal user02
🗅 Builtin	Did User Rena	pkilocal
C Computers	Depi.local\Petrov-р Петров Петр	
Domain Controllers	pki.local\pkiuser pkiuser	
ForeignSecurityPrincipals	pki.local\sky Anakin Skywal	
Managed Service Accounts	🗹 🙁 pki.local\user01 user01	
▶ 🗀 testOU	pki.local\user02 user02	
🗅 Users	່ a_o Protected Users and IAS Serv	
<ul> <li>O 10.72.9.11 (FreeIPA)</li> </ul>	່ ວິດໍ Read-only Domai	
	ြံ ခိြိုင် Schema Admins	
Добавить домен	Bcero: 31	
		Добавить Отмена

a)



🗙 Доба	вление пользователей для	группы "Все компьютерь	n I			Х
	Домены <mark>Компьютеры</mark>	Псевдонимы С	Пользователи		Будут добавлены - 1	
Bce 🔻	Q. Поиск		Q Поиск		localUser w09w13	
yw 🚽	)9w13		Имя	<ul> <li>Полное имя</li> </ul>		
₽ PC	1		Останит         Останит           8°№         IIS_JUSRS           IIS_IUSRS         IIS_IUSRS           IIS_IUSRS         IIS_IUSRS           IIS_IUSRS         IIS_IUSRS           IIS_IUSRS         IIS_IUSRS           IIS_IUSRS         IIS_IUSRS           IIS_IUSRS         IIS_IUSRS           IIS_INTRACT         IIS_INTRACT           8°№         Администра           8°№         Гости           IIS_INTRACT         IIS_INTRACT	unt Some local user er Some other local u Account торы торы		
Bcero:	2		Bcero: 24			
					Добавить	Отмена

б)

🗙 Добавление пользователей для группы "Все компьютеры"		×
Домены Компьютеры <mark>Псевдонимы</mark>	Пользователи	Будут добавлены - 1
Все псевдонимы	MMR	оо Локальные пользователи а́⊖¤
	🗹 ီြိb Локальные пользователи	
	а́а́ Все пользователи	
		Добавить Отмена

в)

Рисунок 7.4 – Добавление пользователей или группы пользователей

После нажатия кнопки **Добавить**, добавленный пользователь или группа отобразятся в списке пользователей окна **Управление входом в ОС** (рисунок 7.5).

74

🗙 Изменение клиентской полит	К Изменение клиентской политики: Политика клиента по умолчанию					
Общее	Управление входом в	oc 🗗				
Windows	Список пользователей 🗗 Доп	юлнительные настройки				
Управление входом в ОС	🔍 Поиск пользователей					
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть	
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить	
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows			
Гарантированное	pki.local\user02	Active Directory	По токену			
удаление файлов	w09w13\localUser	Локальный пользователь	Тип входа			
Аудит целостности файлов	്റ്റ് Все пользователи					
Аудит запуска приложений	°0°в Локальные пользователи		Тип	Разрешить	Запретить	
			Интерактивный вход			
Аудит печати			Сетевой вход	<b>~</b>		

Рисунок 7.5 – Отображение добавленного пользователя

Для принудительного наследования списка пользователей/групп пользователей всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке элемента списка, на всем списке или на всем разделе настроек входа.

## 7.1.5 Управление настройками входа

Для каждого пользователя/группы пользователей возможно установить тип аутентификации пользователя при входе в ОС (аутентификация Windows и/или аутентификация с использованием токена) и тип входа (интерактивный вход и/или сетевой).

Тип аутентификации Аутентификация Windows предполагает проверку идентификационных данных пользователя средствами операционной системы, СЗИ при этом не осуществляет никаких проверок, кроме проверки наличия учетной записи пользователя, выполняющего вход в ОС, в своей базе данных. При установке данного типа аутентификации, для пользователя возможен любой вид входа, предусмотренный средствами ОС (вход по паролю, по сертификату на токене или по паролю на токене).

Тип аутентификации **По токену** предполагает аутентификацию пользователя с использованием токена, при этом СЗИ осуществляет проверку принадлежности токена пользователю. В зависимости от информации, хранящейся на токене, аутентификация пользователя будет осуществляться по паролю (БВПП) или по цифровому сертификату для входа на токене.



Для аутентификации **По токену** необходимо чтобы токен, с помощью которого будет осуществляться аутентификация, был <u>назначен пользователю</u> <u>подсистемой управления токенами СЗИ:</u>

 для аутентификации пользователя с использованием пароля, записанного на токен (в случае входа по паролю на токене);

– для аутентификации с использованием цифрового сертификата, записанного на токен (в случае входа по сертификату на токене). При этом сертификат для входа может быть выпущен как средствами подсистемы управления токенами, так и сторонними средствами.

Дополнительно администратор может установить разрешение/запрет на интерактивный вход пользователя (локальный вход на клиентскую рабочую станцию) или сетевой вход. При запрете обоих видов входа, пользователь не сможет осуществить вход на клиентскую рабочую станцию.

Во вкладке **Дополнительные настройки** (рисунок 7.6) администратор при необходимости может установить дополнительные настройки для пользователей, добавленных в список механизма управления входом в ОС, установив соответствующие флаги:

- **Блокировать служебные учетные записи** – возможность установить запрет для учетных записей, которые явно не внесены в базу СЗИ, но осуществляют попытки доступа к информации (от своего имени или от имени служб) на уровне запуска приложений;

Блокировать сетевой доступ пользователям, не добавленным в список
 возможность установить запрет на сетевой вход для пользователей, не добавленных в список;

Включить механизм «Проверка пароля в СЗИ» на клиентских компьютерах – возможность настраивать вход пользователя по паролю в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Проверка пароля в СЗИ»);

– Включить механизм «Пользователи с разрешением на вход в ОС» на клиентских компьютерах – возможность разрешать вход на клиентскую рабочую станцию только пользователям из списка, заданного в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Пользователи с разрешением на вход в ОС»).



🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию	Х
Общее	Управление входом в ОС 🗅	
Windows	Список пользователей 🗗 Дополнительные настройки	
Управление входом в ОС	🗌 Блокировать служебные учетные записи 🗗	
Сложность паролей	🗌 Блокировать сетевой доступ пользователям, не добавленным в список 🗗	
Контроль устройств	Включить механизм "Проверка пароля в СЗИ" на клиентских компьютерах 🗗	
Очистка оперативной памяти	Включить механизм "Пользователи с разрешением на вход в ОС" на клиентских компьютерах ☐'	
Гарантированное удаление файлов		
Аудит целостности файлов		
Аудит запуска приложений		
Аудит печати		
Аудит доступа к медиафайлам		
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим		
	Ок Отмена Применить	

Рисунок 7.6 – Дополнительные настройки для пользователей

## 7.1.6 Удаление пользователей или групп пользователей

Для удаления единичного пользователя или группы пользователей из списка настроек входа в клиентской политике, в режиме изменения клиентской политики, в разделе политики **«Управление входом в ОС»** выберите в списке пользователя/группу пользователей, которого необходимо удалить и нажмите кнопку , расположенную в конце строки, или воспользуйтесь контекстным меню.

Для удаления нескольких пользователей/групп пользователей выделите необходимые позиции списка, удерживая клавишу *<Ctrl>* (для удаления выборочных пользователей) или удерживая клавишу *<Shift>* (для удаления пользователей в выбранном диапазоне) и воспользуйтесь кнопкой <sup>Удалить</sup> (рисунок 7.5).

При удалении элементов списка возможны два варианта удаления (рисунок 7.7):

– удаление элементов списка только в текущей политике – для этого в окне удаления пользователей/групп необходимо выбрать **Удалить для текущей**.

удаление элементов списка и в текущей политике и во всех дочерних политиках
 для этого в окне удаления пользователей/групп необходимо выбрать Удалить для



всех.

🗙 Удаление пользователей/групп				
Удалить (2) пользователей/групп также для всех дочерних политик?				
Вы также можете удалить пользователей/группы для текущей политики				
Отмена Удалить для текущей Удалить для всех				

Рисунок 7.7 – Удаление пользователей/групп пользователей

## 7.1.6.1 Удаление элементов в текущей политике

Удаление элемента списка только в текущей политике не затронет дочерние политики. При этом, если на удаляемом элементе списка установлено принудительное наследование («замок»), удаление элемента в текущей политике приведет к тому, что дочерней политике появится возможность изменять настройки данного элемента.

## Пример:

В политике «Политика клиента по умолчанию» в механизме **«Управление входом в ОС»** список пользователей включает пользователей «*user01*» и «*user02*», принудительное наследование установлено на пользователе «*user02*» (рисунок 4.14 а).

В политике «Клиентская политика 1» список пользователей также включает пользователя «*user01*», пользователь «*user02*» наследуется с вышестоящей политики, при этом администратору нижнего уровня доступны любые действия со списком пользователей, кроме наследуемого элемента (рисунок 4.14 б).

В политике «Политика клиента по умолчанию» администратор верхнего уровня удаляет из списка пользователя «*user02*» только для текущей политики (рисунок 7.8 а).

Удаление элемента на верхнем уровне приводит к тому, что у администратора нижнего уровня появляется возможность изменять данного пользователя (рисунок 7.8 б).



Х Изменение клиентской полит	ики: Политика клиента по умолч	анию			×
Общее	Управление входом	и в ОС 🗅			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	°о° Все пользователи		По токену		
удаление файлов			Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		
		a)			
Х Изменение клиентской полити	ики: Клиентская политика 1				×
Общее	Управление входом	л в ОС 🗅			
Windows	Список пользователей 🗗	Дополнительные настройки			
Управление входом в ОС	О Поиск пользователей				
Сложность паролей	+ 🗑 Удалить		Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа	▲ Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	pki.local\user01	Active Directory	Аутентификация Windows		
Гарантированное	🔒 💽 pki.local\user02	Active Directory	По токену		
удаление файлов	å∩ீв̀ Все пользователи		Тип входа		
Аудит целостности файлов			Тип	Разрешить	Запретить
Аудит запуска приложений			Интерактивный вход		
Аудит печати			Сетевой вход		

Рисунок 7.8 – Принудительное наследование после удаления элемента списка для текущей политики

## 7.1.6.2 Удаление элементов для всех политик

Удаление элемента списка и в текущей политике и в дочерних политиках приведет к тому, что элементы списка будут удалены не только в текущей политике, но и во всех политиках, которые являются дочерними по отношению к текущей.

При этом, установлено принудительное наследование на удаляемом элементе списка или нет не имеет значения.

## Пример:

В политике «Политика клиента по умолчанию» в механизме «Управление входом по паролю» список пользователей включает пользователей «user01» и «user02»,

## 72410666.00063-04 95 01-01

79

принудительное наследование установлено на пользователе «*user02*» (рисунок 4.14 а).

В политике «Клиентская политика 1» список пользователей также включает пользователя «*user01*», пользователь «*user02*» наследуется с вышестоящей политики, при этом администратору нижнего уровня доступны любые действия со списком пользователей, кроме наследуемого элемента (рисунок 4.14 б).

В политике «Политика клиента по умолчанию» администратор верхнего уровня удаляет из списка пользователей «*user01*» и «*user02*» для всех политик (рисунок 7.9 а).

Удаление элементов на верхнем уровне приводит к тому, что данные элементы удаляются во всех дочерних политиках (рисунок 7.9 б).

Х Изменение клиентской полити	ки: Политика клиента по умолчанию			×
Общее	Управление входом в ОС 🗅			
Windows	Список пользователей 🗗 Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей			
Сложность паролей	+ 🗑 Удалить	Аутентификация		Скрыть
Контроль устройств	Пользователь/Труппа 🔺 Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	aိြရိ Все пользователи	Аутентификация Windows	<b>~</b>	
Гарантированное		По токену		
удаление файлов		Тип входа		
Аудит целостности файлов		Тип	Разрешить	Запретить
Аудит запуска приложений		Интерактивный вход		
Аудит печати		Сетевой вход		
	a)			
Х Изменение клиентской полити	ики: Клиентская политика 1			×
Общее	Управление входом в ОС 🗗			
Windows	Список пользователей 🗗 Дополнительные настройки			
Управление входом в ОС	Q. Поиск пользователей			
Сложность паролей	+ 🗑 Удалить	Аутентификация		Скрыть
Контроль устройств	Пользователь/Группа 🔺 Тип	Тип	Разрешить	Запретить
Очистка оперативной памяти	ដိ <mark>ု</mark> ိ Все пользователи	Аутентификация Windows		
Гарантированное		По токену		
удаление файлов		Тип входа		
Аудит целостности файлов		Тип	Разрешить	Запретить
Аудит запуска приложений		Интерактивный вход		
Аудит печати		Сетевой вход		

б)

Рисунок 7.9 – Удаление элемента списка для всех политик

# 7.2 Сложность паролей

Механизм настройки сложности паролей 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.

Настройка параметров политики аутентификации пользователей заключается в установке требований к паролю пользователя, PIN-коду доступа к токену и блокировке пользователя при неудачных попытках авторизации в ОС. Описание настраиваемых параметров политики приведено в таблице 7.2.

Наименование параметра	Описание	Возможные значения	По умолчанию
Пароль пользователя			
Минимальное количество символов	Требования к минимальной длине пароля	от 6 до 14 символов	6 символов
Срок действия пароля (дней)	Требования к максимальному времени действия пароля пользователя	от 1 до 999 дней	42 дня
Количество новых символов при смене пароля	Требования к изменению состава при создании нового пароля пользователя	от 1 до 24	1 символ
Запретить использование последних паролей	Запрет на использование предыдущих паролей пользователя	от 1 до 6 паролей	1 символ
Проверять пароль на соответствие требованиям сложности	Требования к сложности пароля. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Блокировать использование популярных паролей	Запрет на использование популярных и общеизвестных паролей		
РІN-код токена			
Минимальное количество символов	Требования к минимальной длине PIN-кода доступа к аппаратному идентификатору	от 6 до 20 символов.	6 символов
Срок действия PIN-кода (дней)	Требования к максимальному времени действия PIN-кода пользователя	от 1 до 365 дней	45 дня

Таблица 7.2 – Параметры политики аутентификации пользователей

Наименование параметра	Описание	Возможные значения	По умолчанию
Количество новых символов при смене PIN- кода	Требования к изменению состава при создании нового PIN-кода пользователя	от 1 до 15	3 символа
Запретить использование последних PIN-кода	Запрет на использование предыдущих PIN- кодов пользователя		3 PIN-кода
Проверять PIN-код на соответствие требованиям сложности	Требования к сложности PIN-кода. PIN-код должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Блокировать использование популярных PIN-кодов	Запрет на использование популярных и общеизвестных PIN-кодов		
Аутентификация			
Количество попыток входа	Значение максимального количества неудачных попыток входа пользователя в ОС до его автоматической блокировки	от 3 до 999 попыток	3 попытки
Блокировать пользователя при неправильном вводе паролей на (минут)	Время (в минутах) блокировки возможности входа пользователя в ОС рабочей станции после превышения им максимального количества неудачных попыток входа в ОС	от 1 до 480 минут	5 минут

Если при установленной политике срока действия PIN-кода C3И не находит информации о времени последней смены PIN-кода, хранящейся на токене (например, при форматировании носителя эта информация была удалена), то после выдачи токена, пользователю при входе будет выведено требование о смене PIN-кода, даже при условии, что при назначении токена пользователю принудительная смена PIN-кода пользователя при первом входе не была установлена.

Для настройки параметров политики аутентификации учетных записей пользователей перейдите в раздел политики **«Сложность паролей»** в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите требующиеся параметры и их значения (рисунок 7.10).

Для принудительного наследования установленных параметров аутентификации всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе аутентификации.



🗙 Изменение клиентской полити	ки: Клиентская политика 1					×
Общее	Сложность паролей 🗗					
Windows	Пароль пользователя					
Управление входом в ОС	Минимальное количество символов	6	6			
Сложность паролей	Срок действия пароля (дней)	42	<b></b>			
Контроль устройств	<ul> <li>Количество новых символов при смене пароля <sup>(1)</sup></li> <li>Запретить использование последних паролей <sup>(1)</sup></li> </ul>	1	≜ ſ			
Очистка оперативной памяти	Проверять пароль на соответствие требованиям сложности 🕄		6			
Гарантированное удаление файлов	🗌 Блокировать использование популярных паролей 🛈		9,			
Аудит целостности файлов	PIN-код токена					
	Минимальное количество символов	6				
Аудит запуска приложений	Срок действия PIN-кода (дней)	45	6			
Аудит печати	🗌 Количество новых символов при смене PIN-кода 🛈	3	ď			
Аулит доступа к мелиафайдам	☐ Запретить использование последних PIN-кодов ☺	3	6			
Аудит доступа к медиафаилам	Проверять PIN-код на соответствие требованиям сложности 🙂		9,			
Контроль целостности среды	Блокировать использование популярных PIN-кодов 🙂		С.			
Журнал аудита	Аутентификация					
Linux	🗸 Количество попыток входа 🛈	3	6			
Мягкий режим	Блокировать пользователя при неправильном вводе паролей на (минут)	5	ර			
		Ок	D1	мена	Примен	ить

Рисунок 7.10 – Настройка параметров аутентификации

# 7.3 Контроль устройств

Контроль устройств предназначен для разграничения доступа к отчуждаемым носителям информации. Он позволяет администратору безопасности возможность санкционировать доступ к USB-устройствам, CD/DVD-устройствам, устройствам, подключаемым через СОМ- и LPT-порты, а также сформировать список разрешенных устройств<sup>5</sup>, доступных для чтения/записи пользователю или группе пользователей.

## 7.3.1 Разграничение доступа к USB-устройствам

Для настройки разграничения доступа к USB-устройствам перейдите в раздел политики **«Контроль устройств»** в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку **USB-устройства** (рисунок 7.11).

<sup>&</sup>lt;sup>5</sup> Формирование списка разрешенных устройств возможно только для классов USB-устройств: устройства хранения данных, переносные устройства.



Х Изменение клиентской политики: Политика клиента по умолчанию Х						
Общее	Контроль устройств					
Windows	USB устройства 🗂 Другие устройства	а 🗗 Доверенный список 🗗				
Управление входом в ОС	📀 📋 Устройства хранения данных	Правила доступа Аудит				
Сложность паролей	🥏 🏢 Переносные устройства					
Контроль устройств	🥏 奈 🛛 Wi-Fi и Bluetooth адаптеры	🗹 Доступ разрешен 📋				
Очистка оперативной памяти	🥏 🔟 Смарт-карты и считыватели	+ 🔟 Удалить				
-	🥏 🕦 Устройства ввода	Имя	▲ Тип	Вид	Разрешить	Запретить
Гарантированное удаление файлов	📀 🖳 Прочие USB устройства	ိြိုရိ Все пользователи		Чтение	<b>~</b>	
Аудит целостности файлов				Запись		
Аудит запуска приложений						
Аудит печати						
Аудит доступа к медиафайлам						
Контроль целостности среды						
Журнал аудита						
Linux						
Мягкий режим		Всего: Все пользователи				
		Ok	Отме	ена		енить

Рисунок 7.11 – Настройка разграничения доступа к USB-устройствам

USB-устройства во вкладке структурированы по следующим классам USB-устройств:

устройства хранения данных (съемные USB-носители);

– переносные устройства (WPD-устройства: телефоны, фотокамеры, музыкальные проигрыватели);

Wi-Fi и Bluetooth адаптеры;

смарт-карты и считыватели;

устройства ввода (клавиатура, мышь, планшет);

– прочие USB устройства (устройства, не структурированные ни в один из вышеперечисленных классов).

# 7.3.1.1 Настройка разграничения доступа к устройствам хранения данных и переносным устройствам

Доступ к USB-устройствам классов *Устройства хранения данных* и *Переносные устройства* разграничивается на уровне пользователей, и представляет собой список пользователей с установленными настройками доступа к таким устройствам:

## 72410666.00063-04 95 01-01

84

- **Чтение** (возможность чтения пользователем информации с устройства);
- Запись (возможность внесения изменений в информацию на устройстве).

Для настройки правил доступа пользователя к устройствам хранения данных и переносным устройствам выберите в списке нужный класс устройств (рисунок 7.11) и

во вкладке **Правила доступа** по кнопке <sup>+</sup> сформируйте список пользователей в окне **Добавление пользователей** (см. раздел **«Добавление пользователей или** *групп пользователей»*), которым необходимо разграничить доступ к выбранному классу устройств и нажмите **Добавить**.

Установите требующиеся ограничения на доступ к выбранному классу устройств для каждого из добавленных пользователей (рисунок 7.12) и нажмите **Применить**.

🗙 Изменение клиентской полит	ики: Политика клиента по умолчанию		×
Общее	Контроль устройств		
Windows	USB устройства 🗗 Другие устройств	а 🗗 Доверенный список 🗗	
Управление входом в ОС	📀 📋 Устройства хранения данных	Правила доступа Аудит	
Сложность паролей	📀 🏢 Переносные устройства		
Контроль устройств	🥏 🛜 Wi-Fi и Bluetooth адаптеры	✓ Доступ разрешен — О.	
Очистка оперативной памяти	📀 🔟 Смарт-карты и считыватели	+ 🔟 Удалить	
	🥑 🕦 Устройства ввода	Имя 🔺 Тип	Вид Разрешить Запретить
Гарантированное удаление файлов	🥏 星 Прочие USB устройства	≗∩ீ Все пользователи	Чтение 🔽 🗌
Аудит целостности файлов		pki.local\user01 Active Directory	Запись
		pki.local\user02 Active Directory	

Рисунок 7.12 – Разграничение доступа выбранного пользователя

По умолчанию в списке пользователей добавлен псевдоним *Все пользователи,* который подразумевает, что все доменные и локальные пользователи клиентской рабочей станции имеют доступ на чтение и запись в устройство выбранного класса.

При необходимости возможно установить общий запрет или разрешение на доступ к выбранному классу устройств для всего сформированного списка пользователей, установив или сняв флаг **Доступ разрешен** (рисунок 7.12). При установке запрета использование любых подключенных к рабочей станции устройств из выбранного класса будет запрещено.

Во вкладке **Аудит** задается перечень событий аудита, которые необходимо фиксировать в журнале аудита (рисунок 7.13). Возможно фиксировать события включения/выключения устройства, успешный доступ к устройству, отказ на доступ к устройству.



86

🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию	Х
Общее	Контроль устройств	
Windows	USB устройства 🗗 Другие устройства 🗗 Доверенный список 🗗	
Управление входом в ОС	Устройства хранения данных         Правила доступа         Аудит	
Сложность паролей	📀 🏢 Переносные устройства	
Контроль устройств	✓ Э Wi-Fi и Bluetooth адаптеры	
Очистка оперативной памяти	Смарт-карты и считыватели Выполнять аудит успешных операций доступа к устройствам	
	✓ ① Устройства ввода ✓ Выполнять аудит отказов на доступ к устройствам	
гарантированное удаление файлов	📀 💂 Прочие USB устройства	

Рисунок 7.13 – Выбор событий, регистрируемых в журнале аудита

Принудительное наследование параметров (установка «замка») всеми политиками, являющимися дочерними по отношению к текущей, доступно:

- для всего раздела USB-устройств,
- для общего запрета/разрешения на доступ к выбранному классу устройств,
- для пользователя в сформированном списке,
- для регистрируемых событий аудита.

## 7.3.1.2 Настройка разграничения доступа к остальным классам USBустройств

Для USB-устройств классов *Wi-Fi и Bluetooth адаптеры*, *Смарт-карты и считыватели*, *Устройства ввода* и *Прочие USB устройства* предоставление или запрет доступа настраивается на уровне клиентской рабочей станции (рисунок 7.14).



Рисунок 7.14 – Настройка правил доступа для остальных классов USB-устройств

Установить запрет или предоставить разрешение на доступ к выбранному классу устройств на клиентской рабочей станции возможно установив или сняв флаг **Доступ разрешен** в области **Правила доступа** (рисунок 7.14). При установке запрета

использование любых подключенных к рабочей станции устройств из выбранного класса будет запрещено.

При необходимости фиксировать в журнале аудита события включения/выключения выбранного класса устройств установите флаг **Выполнять аудит** *включения/выключения устройств* в области **Аудит**.

# 7.3.2 Разграничение доступа к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты

Для настройки разграничения доступа к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты, перейдите в раздел политики **«Контроль устройств»** в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку *Другие устройства* (рисунок 7.15).

Предоставление или запрет доступа для CD/DVD-приводов и устройств, подключаемым через COM- и LPT-порты, настраивается на уровне клиентской рабочей станции.

🗙 Изменение клиентской полити	🗙 Изменение клиентской политики: Политика клиента по умолчанию	
Общее	Контроль устройств	
Windows	USB устройства 🗗 Другие устройства 🗗	Доверенный список 🕒
Управление входом в ОС	📀 ᇢ CD/DVD-приводы	Правила доступа
Сложность паролей	🥏 📼 сом	✓ Доступ разрешен
Контроль устройств	📀 🔠 LPT	
Очистка оперативной памяти		

Рисунок 7.15 – Настройка правил доступа для CD/DVD-устройств

Установить запрет или предоставить разрешение на доступ к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты, на клиентской рабочей станции возможно установив или сняв флаг **Доступ разрешен** в области **Правила доступа** (рисунок 7.15), в результате чего использование любых подключенных к рабочей станции устройств будет запрещено.

При использовании на клиентской рабочей станции программ по работе с CDи DVD-дисками (для чтения, создания, эмуляции и т.д., например, UltraISO), установленные настройки разграничения доступа к CD-/DVD-приводам будут применены только после перезагрузки рабочей станции.

## 7.3.3 Формирование доверенного списка устройств

Доступ для классов USB-устройств: *Устройства хранения данных* и *Переносные устройства* может настраиваться индивидуально для каждого устройства путем формирования доверенного списка для выбранного пользователя или группы пользователей на клиентской рабочей станции.

87



После формирования доверенного списка устройств у пользователя или группы пользователей будет доступ к устройству из списка, независимо от ограничений, заданных для классов USB-устройств во вкладке **USB-устройства**. При обращении к устройству из доверенного списка формируется событие аудита на успешный доступ/отказ доступа к устройству.

Общая схема запрета/разрешения доступа пользователя к устройству при сформированном доверенном списке устройств по примеру доступа к USB-устройству приведена на рисунке 7.16.



Рисунок 7.16 – Схема запрета/разрешения доступа пользователя к устройству

Для добавления в список доверенных устройств доступны все устройства, которые подключены ко всем клиентским рабочим станциям сервера в настоящий момент или были подключены ранее.

Для формирования доверенного списка устройств перейдите в раздел политики **«Контроль устройств»** в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку **Доверенный список** (рисунок 7.17).

Во вкладке **Доверенный список** возможно сформировать список устройств, доступных для выбранного пользователя или группы пользователей на клиентской рабочей станции. При этом формирование списка разрешенных устройств возможно



только для классов USB-устройств: **Устройства хранения данных** и **Переносные** устройства.

🗙 Изменение клиентской полити	Изменение клиентской политики: Политика клиента по умолчанию	
Общее	Контроль устройств	
Windows	USB устройства 🗗 Другие устройства 🗗 <mark>Доверенный список</mark> 🖒	
Управление входом в ОС	Q. Поиск	
Сложность паролей	<b>+</b>	🛃 Импорт 👌 Экспорт
Контроль устройств		
Очистка оперативной памяти		
Гарантированное удаление файлов		
Аудит целостности файлов		
Аудит запуска приложений	FE	
Аудит печати		
Аудит доступа к медиафайлам	Устройства отсутствуют	
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим		
	Ок Отмена	Применить

Рисунок 7.17 – Формирование доверенного списка устройств

По кнопке откроется окно **Добавление в список разрешенных устройств** (рисунок 7.18), содержащее список устройств со всех клиентских рабочих станций сервера. Устройства могут быть подключены к рабочей станции в настоящий момент (на значке устройства индикация зеленым цветом) или были подключены к рабочей станции ранее (история подключений из реестра).

🔀 Добавление в список разрешенных устройств		Х			
9	Выберите устройство и нажмите на кнопку "Далее				
w09w13	Все устройства 🔹 🔍				C
	Имя	≜ Вид	Идентификатор	Серийный номер	
	<ul> <li>Устройства хранения данных</li> </ul>				
	🝷 📋 🛛 JetFlash Transcend 32GB USB Device - 1	Модель	VID_8564 PID_1000		
	📙 JetFlash Transcend 32GB USB Device	Экземпляр	VID_8564 PID_1000	4012611103	

Рисунок 7.18 – Добавление устройств в доверенный список



Устройства в списке структурированы по классу, к которому они относятся (*Устройства хранения данных* и *Переносные устройства*) и по модели устройства.

Идентификатор модели устройства формируется из комбинации идентификатора производителя (*VID*) и продукта (*PID*).

Каждый экземпляр устройства идентифицируется по модели и уникальному серийному номеру устройства.

Выберите нужный экземпляр или модель устройства в окне **Добавление в список** *разрешенных устройств* и нажмите **Далее** (рисунок 7.18).

Для формирования списка пользователей, которым разрешен доступ к выбранному

экземпляру/модели по кнопке (рисунок 7.19) перейдите в окно **Добавление** пользователей (см. раздел **«Добавление пользователей или групп** пользователей»), выберите пользователей или группу пользователей и нажмите **Добавить**.

🗙 Добавление в список разрешенных устройств			×
Устройство JetFlash Transcend 32GB USB Device (Экземпляр)			
Имя устройства			
JetFlash Transcend 32GB USB Device			
Пользователи			
+ Ш Удалить			Q
Имя 🔺 Тип	Вид	Разрешить	Запретить
pki.local\user01 Active Directory	Чтение	<b>~</b>	
eki.local\user02 Active Directory	Запись		

Рисунок 7.19 – Формирование списка пользователей, которым разрешен доступ к устройству

Установите требующиеся ограничения на доступ к выбранному устройству или модели для добавленных пользователей:

- **Чтение** (возможность чтения пользователем информации с устройства);
- Запись (возможность внесения изменений в информацию на устройстве).

По окончанию формирования списка пользователей, которым разрешен доступ к выбранному устройству/модели нажмите **Добавить**. Во вкладке **Доверенный** *список* отобразится сформированный список устройств, доступных для выбранных пользователей (рисунок 7.20).



91

🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию	×
Общее	Контроль устройств	
Windows	USB устройства С Другие устройства С Доверенный список С	
Управление входом в ОС	Q. Поиск	
Сложность паролей	+ 🔟 Удалить 🖉 Изменить 🛓 Импорт 👌 Экспор	r
Контроль устройств	Имя 🔺 Тип устройства Пользов. Идентификатор Серийный номер Вид	
Очистка оперативной памяти	📋 JetFlash Transcend 3 Устройства хранения да 🖄 2 VID_8564 PID_1000 Модель	

Рисунок 7.20 – Сформированный доверенный список устройств

Принудительное наследование параметров (установка «замка») всеми политиками, являющимися дочерними по отношению к текущей, доступно для всего списка доверенных устройств или для каждого из добавленных устройств отдельно.

По кнопкам 🖄 Импорт / 🖄 Экспорт доступен импорт/экспорт сформированного доверенного списка устройств. При импорте доверенного списка возможно:

– дополнить уже существующий список доверенных устройств объединением имеющегося и импортируемого списков по кнопке **Дополнить** (рисунок 7.21);

 заменить уже существующий список доверенных устройств по кнопке Замена<sup>6</sup>:
 при выполнении замены, существующий список доверенных устройств будет полностью заменен устройствами из импортированного файла.



Рисунок 7.21 – Выполнение импорта списка доверенных устройств

<sup>&</sup>lt;sup>6</sup> Операция замены списка доверенных устройств может использоваться при импорте списка устройств из программно-аппаратного комплекса автоматизированного учета защищаемых носителей информации (ПАК «САУЗНИ»).

 $(\mathbf{i})$ 

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

Необходимо учитывать, что при выполнении операции импорта перезапись и дополнение списка доверенных устройств будет недоступна для устройств с установленным «замком» (установка принудительного наследования параметров). Если в импортируемом списке будет обнаружено устройство идентичное устройству уже имеющемуся в списке доверенных устройств, при установлен этом на устройстве В списке «замок», изменения ИЗ импортируемого списка внесены не будут (рисунок 7.22).

Х	Импорт							×
$\otimes$	Ошиб	ка						
Дл	я следующ	их у	стройств невозмож	но внести и	зменения	(закрыты замко	M)	
Имя	i	⊾ Ти	ип устройства	Идентификат	ор	Серийный номер	Вид	
	JetFlash Tr	. Ус	стройства хранени	VID_8564 PI	D_1000		Модель	
					Сохран	ить в файл	Ок	

Рисунок 7.22 – Ошибка при импорте списка доверенных устройств

## 7.4 Очистка оперативной памяти

Очистка памяти выполняется с целью удаления остаточной информации после завершения поставленных на контроль процессов.

Процесс перезаписи оперативной памяти происходит по следующей схеме: по окончании работы контролируемого процесса механизм очистки памяти производит захват всей свободной оперативной памяти, включая и область, освобожденную контролируемым процессом. Захваченные области оперативной памяти перезаписываются маскирующими данными. По мере перезаписи механизм очистки высвобождает перезаписанную область.

Для настройки параметров механизма очистки оперативной памяти перейдите в раздел политики **«Очистка оперативной памяти»** в режиме изменения клиентской политики на сервере или в группе рабочих станций (рисунок 7.23).



🔀 Изменение клиентской полити	ики: Политика клиента по умолчанию Х
Общее	Очистка оперативной памяти 🗅
Windows	Механизм включен —
Управление входом в ОС	🗹 Формировать события аудита 🗗
Сложность паролей	Приложения для очистки памяти 🗗
Контроль устройств	+ 🖉 Изменить 👿 Удалить 🖄 Импорт 👌 Экспорт
Очистка оперативной памяти	Файл приложения
Гарантированное удаление файлов	a winlogon.exe
Аудит целостности файлов	services.exe
Аудит запуска приложений	
Аудит печати	
Аудит доступа к медиафайлам	
Контроль целостности среды	
Журнал аудита	
Linux	
Мягкий режим	Bcero: 2
	Ок Отмена Применить

Рисунок 7.23 – Механизм очистки оперативной памяти

По кнопке сформируйте список приложений для постановки на контроль и включите механизм очистки оперативной памяти, установив переключатель в положение С Механизм включен (рисунок 7.24).

По кнопкам 🖄 Импорт / 🖄 Экспорт доступен импорт/экспорт списка приложений для очистки памяти.



🔀 Изменение клиентской полити	ики: Политика клиента по умолчанию		×
Общее	Очистка оперативной памяти 🗅		
Windows	Механизм включен —		
Управление входом в ОС	🗹 Формировать события аудита 占		
Сложность паролей	Приложения для очистки памяти 占		
Контроль устройств	+ Изменить 🗊 Удалить	🛃 Импорт	之 Экспорт
Очистка оперативной памяти	Файл приложения		
Гарантированное удаление файлов	Введите имя файла приложения и его расширение (.exe) без указания пути		
Аудит целостности файлов	winlogon.exe		
	services.exe		

Рисунок 7.24 – Добавление приложений для очистки памяти

При необходимости фиксировать в журнале аудита факт совершения очистки оперативной памяти выбранных приложений, установите параметр **Формировать** события аудита.

Для принудительного наследования установленных параметров механизма очистки оперативной памяти всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на выбранном параметре, в строке необходимого приложения, на всем списке приложений или на всем разделе «Очистка оперативной памяти».

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте **«Удаление пользователей или** *групп пользователей»*.

# 7.5 Гарантированное удаление файлов

файлов Гарантированное удаление предназначено для осуществления гарантированного удаления объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления. Удаление файлов происходит троекратным затиранием содержимого кластеров дисков специальному алгоритму, исключающему считывание остаточной информации на диске после их удаления.

Для настройки гарантированного удаления файлов перейдите в раздел политики «Гарантированное удаление файлов» в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите гарантированное удаление файлов на системных и/или не системных дисках (рисунок 7.25).

При необходимости фиксировать в журнале аудита факт гарантированного удаления файлов, установите параметр **Вести аудит гарантированного удаления.** 

Для принудительного наследования установленного гарантированного удаления файлов всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе гарантированного удаления файлов.

🔀 Изменение клиентской полити	ики: Политика клиента по умолчанию Х
Общее	Гарантированное удаление файлов
Windows	🗹 Системный диск 🕒
Управление входом в ОС	🗌 Не системные диски 🔒
Сложность паролей	🗌 Вести аудит гарантированного удаления 🖒
Контроль устройств	
Очистка оперативной памяти	
Гарантированное удаление файлов	
Аудит целостности файлов	
Аудит запуска приложений	
Аудит печати	
Аудит доступа к медиафайлам	
Контроль целостности среды	
Журнал аудита	
Linux	
Мягкий режим	
	Ок Отмена Применить

Рисунок 7.25 – Настройка гарантированного удаления файлов

# 7.6 Аудит целостности файлов

Аудит целостности файлов предназначен для слежения за неизменностью контролируемых файлов. Он позволяет своевременно обнаруживать несанкционированное изменение контролируемых объектов файловой системы.

Неизменность контролируемых файлов проверяется каждый раз при запуске СЗИ. Целостность поставленных на контроль файлов обеспечивается путем проверки контрольных сумм, вычисленных при постановке файлов на контроль. Период проверки контрольных сумм задается администратором безопасности на основе требований политики безопасности. При несоответствии полученных контрольных сумм файлов эталонным значениям происходит фиксация указанного события в журнале аудита.

Не рекомендуется ставить на контроль файлы большого объема (>500 Mb). Так как при периодической проверке вычисленных контрольных сумм файлов, в зависимости от используемого аппаратного обеспечения, возможно снижение производительности системы вплоть до некоторого «зависания» компьютера.



Файлы нулевой длины (имеющие размер 0 байт) невозможно поставить на контроль целостности!

Для настройки параметров контроля изменения файлов перейдите в раздел политики **«Аудит целостности файлов»** в режиме изменения клиентской политики на сервере или в группе рабочих станций (рисунок 7.26).

🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию Х	
Общее	Аудит целостности файлов 🗅	
Windows	Механизм выключен	
Управление входом в ОС	Проверять каждые (чч:мм) 02:00	
Сложность паролей	🗹 Формировать события аудита при нарушении целостности файлов 🕒	
Контроль устройств	Контролируемые файлы 🗗	
Очистка оперативной памяти	+ 🖉 Изменить 🐨 Удалить 😒 Импорт 👌 Экспорт	
Гарантированное удаление файлов	Путь к файлу	
Аудит целостности файлов	C:\Windows\WinSxS\amd64_windows-secdriver_31bf3856ad364e35_10.0.19041.1023_none_3303e7d7bd38a744\mssecfit.sys	
Аудит запуска приложений		
Аудит печати		
Аудит доступа к медиафайлам		
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим	Bcero: 2	
	Ок Отмена Применить	

Рисунок 7.26 – Контроль изменения файлов

По кнопке сформируйте список файлов для постановки на контроль и включите механизм контроля изменения файлов, установив переключатель в положение Механизм включен (рисунок 7.27).

Задайте периодичность проверки целостности файлов, установив время в параметре **Проверять каждые (чч:мм**). По умолчанию проверка целостности осуществляется каждые 2 часа.

По кнопкам 🖄 Импорт / 🖄 Экспорт доступен импорт/экспорт списка файлов для контроля за изменением.

🔀 Изменение клиентской политики: Политика клиента по умолчанию 🛛 🗡 🔀		
Общее	Аудит целостности файлов 🗅	
Windows	Механизм выключен — П	
Управление входом в ОС	Проверять каждые (чч:мм) 02:00	
Сложность паролей	🗹 Формировать события аудита при нарушении целостности файлов 占	
Контроль устройств	Контролируемые файлы 🗅	
Очистка оперативной памяти	+ 🖉 Изменить 🐨 Удалить 🛃 Импорт 🖉 З	Экспорт
Гарантированное удаление файлов	Путь к файлу	
A	Введите полный путь к файлу и его расширение	
Ayan Lenocin gannos		
Аудит запуска приложений	C:\Windows\System32\Aktiv Co\rtUSB\rtUSB.sys	

Рисунок 7.27 – Добавление файлов на контроль целостности

При необходимости фиксировать в журнале аудита выявленные изменения в контролируемых файлах, установите параметр **Формировать события аудита при нарушении целостности файлов.** 

Для принудительного наследования установленных параметров механизма контроля целостности файлов всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на выбранном параметре, в строке необходимого файла, на всем списке файлов или на всем разделе **«Аудит целостности файлов»**.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте **«Удаление пользователей или** групп пользователей».

# 7.7 Аудит запуска приложений

Аудит запуска приложений предназначен для контроля отслеживания запуска и прекращения работы исполняемых файлов. Сбор информации и регистрация событий аудита при попытке запуска и закрытия ехе-приложений осуществляется путем установки маски имени исполняемого файла.

Для настройки аудита исполняемых файлов перейдите в раздел политики **«Аудит запуска приложений»** в режиме изменения клиентской политики на сервере или в группе рабочих станций (рисунок 7.28).



🔀 Изменение клиентской полити	ики: Политика клиента по умолчанию	<
Общее	Аудит запуска приложений 🗅	
Windows	+	
Управление входом в ОС		
Сложность паролей		
Контроль устройств		
Очистка оперативной памяти		
Гарантированное удаление файлов		
Аудит целостности файлов		
Аудит запуска приложений		
Аудит печати	Приложения отсутствуют	
Аудит доступа к медиафайлам	Добавить	
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим		
	Ок Отмена Применить	]

Рисунок 7.28 – Настройка аудита исполняемых файлов

По кнопке сформируйте список исполняемых файлов для регистрации событий аудита добавив маску или имя исполняемого файла (без расширения) в появившемся окне (рисунок 7.29).



Имя исполняемого файла должно содержать минимум два символа.

Символ «\*» заменяет любое количество символов.

98



💢 Маска/имя файла		
Задайте маску или имя исполняемого файла (без расширения) и опишите его функции.		
Маска/имя файла* word* Описание		
<b>Отмена</b> Добавить		

Рисунок 7.29 – Ввод маски или имени исполняемого файла

После нажатия кнопки **Добавить** заданная маска появится в области аудита исполняемых файлов. При этом регистрация события аудита выбранного типа файла будет осуществляться только с учетом введенной маски.

Для принудительного наследования аудита исполняемых файлов всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе аудита исполняемых файлов.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте **«Удаление пользователей или** групп пользователей».

## 7.8 Аудит печати

В разделе политики **«Аудит печати»** настраивается базовый аудит печати, предназначенный для контроля печати документов. Регистрация событий аудита печати осуществляется при печати любого документа для всех приложений. В созданном событии содержится следующая информация: наименование документа, имя пользователя, который вывел документ на печать, количество распечатанных страниц.

**i** 

Аудит событий печати на принтерах общего доступа (локальных принтерах рабочих станций, доступ к которым предоставлен пользователям сети) не ведется.

Для настройки базового аудита печати перейдите в раздел политики «Аудит печати»

в режиме изменения клиентской политики на сервере или в группе рабочих станций и включите базовый аудит печати (рисунок 7.30).

Для принудительного наследования установленных параметров всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе аудита печати.

🗙 Изменение клиентской полити	іки: Политика клиента по умолчанию X
Общее	Аудит печати 🗅
Windows	☑ Включить базовый аудит печати ①
Управление входом в ОС	
Сложность паролей	
Контроль устройств	
Очистка оперативной памяти	
Гарантированное удаление файлов	
Аудит целостности файлов	
Аудит запуска приложений	
Аудит печати	
Аудит доступа к медиафайлам	
Контроль целостности среды	
Журнал аудита	
Linux	
Мягкий режим	
	Ок Отмена Применить

Рисунок 7.30 – Установка базового аудита печати

# 7.9 Аудит доступа к медиафайлам

Аудит медиафайлов предназначен для контроля доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям, путем регистрации событий аудита.

За каждым типом файла, доступным в интерфейсе программы, стоит определенный набор расширений, каждый из которых будет контролироваться путем создания события аудита о открытии и закрытии файла выбранного типа.

Для настройки аудита медиафайлов перейдите в раздел политики **«Аудит доступа к медиафайлам»** в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите регистрацию событий аудита требующихся медиафайлов (рисунок 7.31).

Для принудительного наследования установленных параметров всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе аудита медиафайлов.

Х Изменение клиентской политики: Политика клиента по умолчанию Х		
Общее	Аудит доступа к медиафайлам 🕒	
Windows	Тип файлов	
Управление входом в ОС	🗹 🎧 Аудиофайлы 🛈	
Сложность паролей	<ul> <li>Видеофайлы ()</li> <li>Клображения ()</li> </ul>	
Контроль устройств		
Очистка оперативной памяти		
Гарантированное удаление файлов		
Аудит целостности файлов		
Аудит запуска приложений		
Аудит печати		
Аудит доступа к медиафайлам		
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим		
	Ок Отмена Применить	

Рисунок 7.31 – Настройка аудита медиафайлов

# 7.10 Контроль целостности среды

Контроль целостности среды предназначен для слежения за неизменностью контролируемых объектов с целью обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

В разделе **«Контроль целостности среды»** клиентской политики администратор может задать контроль целостности следующих компонентов операционной системы контролируемой рабочей станции:

- отслеживание изменений списка установленных программ;
- отслеживание изменений списка установленных служб/драйверов;
- отслеживание изменений перечня каталогов общего доступа;

– контроль аппаратной среды (отслеживает изменения конфигурации следующих устройств компьютера: процессор, жесткий диск, CDROM, сетевой адаптер,

материнская плата, видеокарта).

Отслеживание целостности компонентов ОС осуществляется в момент запуска соответствующих служб путем взятия контрольных сумм соответствующих разделов реестра ОС клиентской рабочей станции. Если контрольные суммы в БД СЗИ не совпадут с контрольными суммами соответствующих разделов реестра рабочей станции, будет создано событие аудита о нарушении целостности программноаппаратной среды с указанием эталонного и текущего состояния раздела конфигурации, в котором выявлено нарушение.

Для настройки механизма контроля целостности среды перейдите в раздел политики **«Контроль целостности среды»** в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите требующиеся параметры и их значения (рисунок 7.32).

При нарушении целостности компонентов ОС, установленных на контроль, в журнале аудита фиксируется событие о выявленном нарушении.

Для принудительного наследования установленных параметров всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе контроля целостности среды.

X Изменение клиентской политики: Политика клиента по умолчанию X		
Общее	Контроль целостности среды	
Windows	Отмеченные события будут записываться в систему аудита	
Управление входом в ОС	Контроль	
Сложность паролей	🗹 Аппаратной среды 🛈 🔒	
Контроль устройств	🗌 Изменения перечня каталогов общего доступа 🔤	
Очистка оперативной памяти	🗹 Установки/удаления драйверов 🗋	
Гарантированное	🗌 Установки/удаления служб 🗗	
удаление файлов	🗌 Установки/удаления программ 🔒	
Аудит целостности файлов		
Аудит запуска приложений		
Аудит печати		
Аудит доступа к медиафайлам		
Контроль целостности среды		
Журнал аудита		
Linux		
Мягкий режим		
	Ок Отмена При	менить

Рисунок 7.32 – Настройка контроля целостности среды

# 7.11 Журнал аудита

Настройка размера журнала аудита предназначена для установки максимального размера журнала, использующегося для хранения событий на клиентских рабочих станциях.

Для установки максимального размера журнала аудита на клиентской рабочей станции перейдите в раздел политики **«Журнал аудита»** в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите требуемое значение в параметре *Максимальный размер журнала аудита, Мб* (рисунок 7.33).

Максимально допустимый размер журнала аудита – 50Мб, минимальный размер – 10Мб, значение журнала аудита, заданное по умолчанию – 10Мб.

Для принудительного наследования заданного размера журнала аудита всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе **«Журнал аудита»**.

🗙 Изменение клиентской полити	ки: Политика клиента по умолчанию		×
Общее	Журнал аудита 🔒		
Windows	Максимальный размер журнала аудита, Мб 🛛 10 🖕		
Управление входом в ОС			
Сложность паролей			
Контроль устройств			
Очистка оперативной памяти			
Гарантированное удаление файлов			
Аудит целостности файлов			
Аудит запуска приложений			
Аудит печати			
Аудит доступа к медиафайлам			
Контроль целостности среды			
Журнал аудита			
Linux			
Мягкий режим			
	Ок	Отмена	Применить

Рисунок 7.33 – Настройка журнала аудита

# 7.12 Управление входом в OC Linux

В разделе клиентской политики **«Управление входом в ОС»** для клиентских рабочих станций под управлением ОС семейства Linux администратор может управлять параметрами аутентификации пользователей или группы пользователей клиентских рабочих станций ОС Linux, к которым применяется данная политика.

Настройки входа в OC Linux представляют собой список пользователей и групп с сопоставленными им настройками аутентификации. Для всех пользователей, которые не обозначены в данном списке (напрямую или через группы) вход на клиентские рабочие станции будет запрещен.



Для корректной работы политики **«Управление входом в ОС»** на клиентских рабочих станциях под управлением ОС Linux необходима установка модуля аутентификации. При отсутствии модуля аутентификации на клиентской рабочей станции, все установленные запреты политики будут отклонены, и пользователь сможет осуществить вход на рабочую станцию.

# 7.12.1 Общий принцип аутентификации пользователя в СЗИ от НСД «Блокхост-Сеть 4» в ОС Linux

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

проверка не является ли пользователь суперпользователем root;

 проверка режима функционирования рабочей станции (включен/отключен «мягкий» режим работы) и проверка наличия лицензии у клиентской рабочей станции;

 проверка наличия учетной записи пользователя в списке клиентской политики в разделе «Управление входом в ОС» для клиентских рабочих станций под управлением ОС семейства Linux;

 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 «Аутентификация ОС»;
  - сверка введенного пароля с копией в локальной базе данных клиента СЗИ (в случае разрешенной аутентификации пользователя по паролю).

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

Возможные виды входа пользователя в систему, описаны в таблице 7.1.

## 7.12.2 Аутентификация по паролю на токене

Аутентификация пользователя с использованием безопасного входа по паролю на токене предоставляет возможность защищенного входа пользователя в ОС, при этом пользователю не требуется запоминать пароль и вводить его при каждом входе в систему, сгенерированный пароль хранится на токене и пользователю для входа необходимо предъявить только PIN-код к ключевому носителю, используемому для входа.

Аутентификация с использованием БВПП возможна:

1) По PIN-коду со сменой пароля.

Для перехода на аутентификацию с использованием токена с БВПП со сменой пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

2) По PIN-коду без смены пароля.

Для перехода на аутентификацию с использованием токена с БВПП без смены пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

3) По паролю без PIN-кода.

Вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом пароля пользователя. PIN-код токена вводить не требуется.

Назначение токена пользователю с использованием БВПП описано в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора Блокхост-Сеть 4. Часть 5. Управление токенами».

## 7.12.3 Аутентификация по цифровому сертификату на токене

Аутентификация по цифровому сертификату на токене предоставляет возможность защищенного входа в ОС по сертификату для входа, выданному пользователю.

Для аутентификации пользователя по цифровому сертификату необходимо настроить возможность входа пользователей по сертификатам и выдать токен с сертификатом пользователю с помощью подсистемы управления токенами (подробное описание приведено в документах «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA», «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag»).

При этом сертификат для входа может быть выпущен:

 средствами подсистемы управления токенами (должен быть развернут удостоверяющий центр (УЦ) с возможностью выдачи пользователю сертификатов необходимого типа);

сторонними средствами.

## 7.12.4 Добавление пользователей или групп пользователей

Для добавления пользователей или группы пользователей, которым требуется установить настройки входа, перейдите в раздел политики **«Управление входом в ОС»** для ОС Linux в режиме изменения клиентской политики на сервере или в группе

Х Изменение клиентской полити	ики: Политика клиента по умолчанию		×
Общее	Управление входом в ОС 🗅		
Windows	Список пользователей 🛆 Дополнительные настройки		
Linux	+ Q. Поиск		
Управление входом в ОС	👿 Удалить	Тип входа в ОС	Скрыть
Сложность паролей	Пользователь/Группа 🔺 Тип	Тип	Разрешить Запретить
Контроль устройств	Я Все пользователи	Аутентификация ОС	
		По токену (Блокхост-Сеть)	
Контроль целостности файлов			
Очистка оперативной памяти			
Мягкий режим			
	Пользователей: 0 Групп: 1		
	Οκ	Отмена	Применить

рабочих станций и нажмите кнопку 📩 (рисунок 7.34).

Рисунок 7.34 – Управление входом в ОС Linux

В появившемся окне (рисунок 7.35) добавьте учетную запись пользователя или выберите группу пользователей, которым необходимо установить настройку входа.

Для добавления доступны:

 доменные пользователи (во вкладке **Домены**). Для добавления доменного пользователя во вкладке **Домены** выберите нужный домен или, при отсутствии необходимого домена в списке, добавьте его по ссылке <sup>О Добавить домен</sup> (рисунок 7.35 а).

– локальные пользователи рабочей станции (во вкладке Компьютеры). Для добавления локального пользователя перейдите во вкладку Компьютеры и выберите рабочую станцию, локального пользователя которой требуется добавить (рисунок 7.35 б). Возможна фильтрация выбираемых рабочих станций для поиска машин только в состоянии Онлайн, или ввод имени рабочей станции для поиска по иерархии.

– группы пользователей Все пользователи и Локальные пользователи (во вкладке Псевдонимы). Псевдоним Все пользователи подразумевает всех доменных и локальных пользователей, псевдоним Локальные пользователи локальных пользователей клиентской рабочей станции (рисунок 7.35 в).

🗙 Добавление пользователей		×
<mark>Домены</mark> Компьютеры Псевдонимы	Пользователи и группы	Будут добавлены - 1
▼	Q. Введите запрос и нажмите Enter	ivanov-a pkilocal
D Builtin	MMR A ФИО	
Computers	a <sup>0</sup> b Group Policy Cre	
Domain Controllers	pki.local\adminis admin adminoff	
ForeignSecurityPrincipals	pki.local\Guest (o	
Managed Service Accounts	Devilocal\ipaadmin Ipa Admin	
► 🗀 testOU	🗹 🙁 pki.local\ivanov-а Иванов Алекс	
🗅 Users	pki.local\noname NoName User	
• 🔅 10.72.9.11 (FreeIPA)	Pki.local\noUpnU NoUpn User     Pki.local\nv.avdeev Авдеев Никит	
	pki.local\oldUser Old User Rena	
Добавить домен	Bcero: <b>31</b>	
		Добавить Отмена

a)



🗙 Добавление пользователей		X
Домены <mark>Компьютеры</mark> Псевдонимы С	Пользователи	Будут добавлены - 1
Все 🝷 🔍 Поиск	Q. Поиск	user
💂 testastra.freeipa.local	Имя • Полное имя	testastra.meeipa.iocai
	_ å⊖å tape	
	o contraction and a the second secon	
	ີ ວິ∩ືລ user	
	🗹 🙁 user	
	☐ å <sup>O</sup> <sup>A</sup> users	
	🗌 ä̃ြိå utmp	
	🗆 🙁 ииср	
	ြ aိြိရံ uucp	
	ã di video	
	ã∆å voice	
Bcero: 1	Bcero: 101	
		Добавить Отмена
	б)	
🗙 Добавление пользователей		×
Домены Компьютеры <mark>Псевдонимы</mark>	Пользователи	Будут добавлены - 1
Все псевдонимы	Имя	о Локальные пользователи ₫Дв
	🗹 🖧 ឹលំ Локальные пользователи	
	а <sup>0</sup> Все пользователи	
		Добавить Отмена

в)

Рисунок 7.35 – Добавление пользователей или группы пользователей

После нажатия кнопки **Добавить**, добавленный пользователь или группа отобразятся в списке пользователей окна **Управление входом в ОС** (рисунок 7.36).


🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию			×
Общее	Управление входом в ОС 🗅			
Windows	Список пользователей 🗗 Дополнительные настройки			
Linux	+ Q. Поиск			
Управление входом в ОС	🔟 Удалить	Тип входа в ОС		Скрыть
Сложность паролей	Пользователь/Группа 🔺 Тип	Тип	Разрешить	Запретить
Контроль устройств	pki.local\ivanov-i	Аутентификация ОС		
Контроль целостности файлов Очистка оперативной памяти	<ul><li>祭 Все пользователи</li><li>祭 Локальные пользователи</li></ul>	По токену (Блокхост-Сеть)		
Мягкий режим	Пользователей: 1 Групп: 2			
	Ок	Отмена	Примен	ить

Рисунок 7.36 – Отображение добавленного пользователя

Для принудительного наследования списка пользователей/групп пользователей всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке элемента списка, на всем списке или на всем разделе настроек входа.

### 7.12.5 Управление настройками входа

Для каждого пользователя/группы пользователей возможно установить тип аутентификации пользователя при входе в ОС Linux (аутентификация ОС и/или аутентификация с использованием токена).

Тип аутентификации **Аутентификация ОС** предполагает проверку идентификационных данных пользователя средствами операционной системы, СЗИ при этом не осуществляет никаких проверок, кроме проверки наличия учетной записи пользователя, выполняющего вход в ОС Linux, в своей базе данных. При установке данного типа аутентификации, для пользователя возможен любой вид входа, предусмотренный средствами ОС.

Тип аутентификации *По токену (Блокхост-Сеть)* предполагает аутентификацию пользователя с использованием токена, при этом СЗИ осуществляет проверку

### 72410666.00063-04 95 01-01

принадлежности токена пользователю. В зависимости от информации, хранящейся на токене, аутентификация пользователя будет осуществляться по паролю (БВПП) или по цифровому сертификату для входа на токене.

Для аутентификации По токену (Блокхост-Сеть) необходимо чтобы токен, с помощью которого будет осуществляться аутентификация, был назначен пользователю подсистемой управления токенами СЗИ:

 для аутентификации пользователя с использованием пароля, записанного на токен (в случае входа по паролю на токене);

 для аутентификации с использованием цифрового сертификата, записанного на токен (в случае входа по сертификату на токене). При этом сертификат для входа может быть выпущен как средствами подсистемы управления токенами, так и сторонними средствами.

Во вкладке **Дополнительные настройки** (рисунок 7.37) администратор при необходимости может установить дополнительные настройки для пользователей, добавленных в список механизма управления входом в ОС, установив соответствующие флаги:

 Блокировать сессию пользователя при извлечении смарт-карты – возможность настраивать блокирование сессии пользователя при входе через графический интерфейс при извлечении токена (при входе пользователя с использованием токена через графический интерфейс (по сертификату на токене или по БВПП) при извлечении токена, сессии с графическим интерфейсом блокируются);

Завершать сессии без графического интерфейса при извлечении смарт-карты – возможность настраивать завершение сессии пользователя при входе без графического интерфейса (например, через терминал) при извлечении токена (при входе пользователя с использованием токена без графического интерфейса (по сертификату на токене или по БВПП) при извлечении токена, сессии без графического интерфейса блокируются);

 $\bigcirc$ 

Необходимо учитывать следующее: сессии без графического интерфейса, созданные внутри сессии с графическим интерфейсом, завершаться не будут.

**i** 

При включенном *Мягком режиме* работы блокирование сессии пользователя с графическим интерфейсом и завершение сессии пользователя без графического интерфейса при извлечении смарт-карты не осуществляется.

- **Вести аудит блокировки сессии** – в случае установки параметра в журнале аудита фиксируется событие о выявленной блокировке сессии;

– Включить механизм «Проверка пароля в СЗИ» на клиентских компьютерах – возможность настраивать вход пользователя по паролю в

настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Проверка пароля в СЗИ»);

– Включить механизм «Пользователи с разрешением на вход в ОС» на клиентских компьютерах – возможность разрешать вход на клиентскую рабочую станцию только пользователям из списка, заданного в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Пользователи с разрешением на вход в ОС»).

0	Изменение клиентской политики: Политика клиента по умолчанию
Общее	Управление входом в OC 🗅
Windows	Список пользователей 👌 Дополнительные настройки
Linux	🗹 Блокировать сессию пользователя при извлечении смарт-карты 🗗
Управление входом в ОС	🗹 Завершать сессии без графического интерфейса при извлечении смарт-карты 🖒
Сложность паролей	🗌 Вести аудит блокировки сессии 🗗
Контроль целостности файлов	🗌 Включить механизм "Проверка пароля в СЗИ" на клиентских компьютерах 占
Очистка оперативной памяти	□ Включить механизм "Пользователи с разрешением на вход в ОС" на клиентских компьютерах ☐
Мягкий режим	
	Отмена Применить

Рисунок 7.37 – Дополнительные настройки для пользователей

### 7.13 Сложность паролей в ОС Linux

Механизм настройки сложности паролей 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.

Настройка параметров политики аутентификации пользователей заключается в установке требований к паролю пользователя, PIN-коду доступа к токену и блокировке пользователя при неудачных попытках авторизации в ОС. Описание настраиваемых параметров политики приведено в таблице 7.3.

### Таблица 7.3 – Параметры политики аутентификации пользователей

Наименование параметра	Описание	Возможные значения	По умолчанию
Пароль пользователя			
Минимальное количество символов	Требования к минимальной длине пароля	от 6 до 14 символов	6 символов
Срок действия пароля (дней)	Требования к максимальному времени действия пароля пользователя	от 1 до 999 дней	42 дня
Количество новых символов при смене пароля	Требования к изменению состава при создании нового пароля пользователя	от 1 до 24	1 символ
Запретить использование последних паролей	Запрет на использование предыдущих паролей пользователя	от 1 до 6 паролей	1 символ
Проверять пароль на соответствие требованиям сложности	Требования к сложности пароля. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Блокировать использование популярных паролей	Запрет на использование популярных и общеизвестных паролей		
PIN-код токена			
Минимальное количество символов	Требования к минимальной длине PIN-кода доступа к аппаратному идентификатору	от 6 до 20 символов.	6 символов
Срок действия PIN-кода (дней)	Требования к максимальному времени действия PIN-кода пользователя	от 1 до 365 дней	45 дня
Количество новых символов при смене PIN- кода	Требования к изменению состава при создании нового PIN-кода пользователя	от 1 до 15	3 символа
Запретить использование последних PIN-кода	Запрет на использование предыдущих PIN- кодов пользователя		3 PIN-кода
Проверять PIN-код на соответствие требованиям сложности	Требования к сложности PIN-кода. PIN-код должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Блокировать использование популярных PIN-кодов	Запрет на использование популярных и общеизвестных PIN-кодов		
Аутентификация			

 $(\mathbf{i})$ 

Наименование параметра	Описание	Возможные значения	По умолчанию
Количество попыток входа	Значение максимального количества неудачных попыток входа пользователя в ОС до его автоматической блокировки	от 3 до 999 попыток	3 попытки
Блокировать пользователя при неправильном вводе паролей на (минут)	Время (в минутах) блокировки возможности входа пользователя в ОС рабочей станции после превышения им максимального количества неудачных попыток входа в ОС	от 1 до 480 минут	5 минут

Если при установленной политике срока действия PIN-кода C3И не находит информации о времени последней смены PIN-кода, хранящейся на токене (например, при форматировании носителя эта информация была удалена), то после выдачи токена, пользователю при входе будет выведено требование о смене PIN-кода, даже при условии, что при назначении токена пользователю принудительная смена PIN-кода пользователя при первом входе не была установлена.

Для настройки параметров политики аутентификации учетных записей пользователей перейдите в раздел политики **«Сложность паролей»** в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите требующиеся параметры и их значения (рисунок 7.38).

- Политика «Сложность паролей» не применяется доменному К администратору (RID=500), кроме настройки «Количество попыток входа». При превышении максимального количества неудачных попыток входа в ОС, заданного В настройке «Количество попыток входа» доменный администратор будет заблокирован на указанное время.
- В домене FreeIPA встроенный доменный администратор (RID=500) не обладает привилегированными правами и подчиняется политике «Сложность паролей» наравне с обычными пользователями.

Для принудительного наследования установленных параметров аутентификации всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра или на всем разделе аутентификации.



💢 Изменение клиентской полити	ки: Политика клиента по умолчанию				×
Общее	Сложность паролей 🗗				
Windows	Пароль пользователя				
Linux	Минимальное количество символов	6	6		
Управление входом в ОС	Срок действия пароля (дней)	42	ď		
Сложность паролей	<ul> <li>Количество новых символов при смене пароля <sup>(3)</sup></li> <li>Запретить использование последних паролей <sup>(3)</sup></li> </ul>	1	6 6		
Контроль устройств	Проверять пароль на соответствие требованиям сложности Блокировать использование популярных паролей О		6 6		
Контроль целостности файлов					
Очистка оперативной памяти	PIN-код токена				
Мягкий режим	Иинимальное количество символов	6	6		
	Срок действия PIN-кода (дней)	45	6		
	🗌 Количество новых символов при смене PIN-кода 🛈	3	6		
	Запретить использование последних PIN-кодов <sup>(1)</sup>	3	ď		
	Проверять PIN-код на соответствие требованиям сложности		d'		
	Блокировать использование популярных PIN-кодов 3		ď		
	Аутентификация				
	Количество попыток входа ③	3	6		
	Блокировать пользователя при неправильном вводе паролей на (минут)	5	ď		
		Ок	Отмен	a	Применить

Рисунок 7.38 – Настройка сложности пароля и ПИН-кода в ОС Linux

# 7.14 Контроль устройств в OC Linux

Контроль устройств предназначен для разграничения доступа к отчуждаемым носителям информации на клиентских рабочих станциях под управлением OC Linux<sup>7</sup>. Он позволяет администратору безопасности возможность санкционировать доступ к USB-устройствам, CD/DVD-устройствам, устройствам, подключаемым через COM- и LPT-порты, а также сформировать список разрешенных устройств<sup>8</sup>, доступных для чтения/записи пользователю или группе пользователей.

### 7.14.1 Разграничение доступа к USB-устройствам

Для настройки разграничения доступа к USB-устройствам перейдите в раздел политики **«Контроль устройств»** для OC Linux в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку **USB-устройства** 

<sup>&</sup>lt;sup>7</sup> Настройка разграничения доступа к отчуждаемым носителям информации доступна только для клиентских станций под управлением РЕД ОС.

<sup>&</sup>lt;sup>8</sup> Формирование списка разрешенных устройств возможно только для классов USB-устройств: устройства хранения данных, переносные устройства.



### (рисунок 7.39).

🔀 Изменение клиентской полити	ки: Политика клиента по умолчанию		×
Общее	Контроль устройств 🗅		
Windows	🕥 Механизм выключен 🗗		
Linux	USB устройства 🗗 Другие устройст	гва 🗗 Доверенный список 🗗	
Управление входом в ОС	📀 📋 Устройства хранения данн	Правила доступа Аудит	
Сложность паролей	🥏 🏢 Переносные устройства	Доступ разрешен П	
Контроль устройств	📀 🛜 Wi-Fi и Bluetooth адаптеры		
	📀 🔟 Смарт-карты и считывате	+ 🗑 Удалить	
Контроль целостности файлов	🥏 🕛 Устройства ввода	Имя 🔺 Тип	Вид Разрешить Запретить
Очистка оперативной памяти	📀 🖳 Прочие USB устройства	🙊 Все пользоват	Чтение 🔽 🗌
Мягкий режим			Запись 🔽 🗌
			Исполнение 🔽 🗌
		всего: все пользователи	
		Ок Отм	ена Применить

Рисунок 7.39 – Настройка разграничения доступа к USB-устройствам

USB-устройства во вкладке структурированы по следующим классам USB-устройств (в зависимости от того, как устройство определяется в операционной системе):

устройства хранения данных (съемные USB-носители);

– переносные устройства (WPD-устройства: телефоны, фотокамеры, музыкальные проигрыватели);

- Wi-Fi и Bluetooth адаптеры;
- смарт-карты и считыватели;
- устройства ввода (клавиатура, мышь, планшет);

– прочие USB устройства (устройства, не структурированные ни в один из вышеперечисленных классов).

# 7.14.1.1 Настройка разграничения доступа к устройствам хранения данных и переносным устройствам

Доступ к USB-устройствам классов *Устройства хранения данных* и *Переносные устройства* разграничивается на уровне пользователей, и представляет собой список пользователей с установленными настройками доступа к таким устройствам:

- **Чтение** (возможность чтения пользователем информации с устройства);

- Запись (возможность внесения изменений в информацию на устройстве);

– *Исполнение* (возможность запускать на исполнение информацию на устройстве).

Для настройки правил доступа пользователя к устройствам хранения данных и переносным устройствам выберите в списке нужный класс устройств (рисунок 7.39) и

во вкладке **Правила доступа** по кнопке <sup>с</sup> сформируйте список пользователей в окне **Добавление пользователей** (см. раздел **«Добавление пользователей или** *групп пользователей»*), которым необходимо разграничить доступ к выбранному классу устройств и нажмите **Добавить**.

Установите требующиеся ограничения на доступ к выбранному классу устройств для каждого из добавленных пользователей (рисунок 7.40) и нажмите **Применить**.

Х Изменение клиентской полити	ки: Политика клиента по умолчанию		×		
Общее	Контроль устройств 🗅				
Windows	🔵 Механизм выключен 🗗				
Linux	USB устройства 🗗 Другие устройст	тва 🗗 Доверенный список 🖒			
Управление входом в ОС	🥑 📋 Устройства хранения данн	Э Устройства хранения данн Правила доступа Аудит			
Сложность паролей	Переносные устройства	🗹 Доступ разрешен 🛛 🖞			
Контроль устройств	<ul> <li>Wi-Fi и Bluetooth адаптеры</li> <li>Cмарт-карты и считывате</li> </ul>	+ 🔟 Удалить			
Контроль целостности файлов	<ul> <li>Устройства ввода</li> </ul>	Имя 🔺 Тип	Вид Разрешить Запретить		
Очистка оперативной памяти	📀 🖳 Прочие USB устройства	🙊 Все пользоват	Чтение 🗹 🗌		
Мягкий режим		📯 pki.local\ivanov-i Доменный пользов	Запись 🗌 🔽		
F		А pki.local∖usr Доменный пользов	Исполнение 🗌 🗸		

Рисунок 7.40 – Разграничение доступа выбранного пользователя

По умолчанию в списке пользователей добавлен псевдоним *Все пользователи,* который подразумевает, что все доменные и локальные пользователи клиентской рабочей станции имеют доступ на чтение и запись в устройство выбранного класса.

При необходимости возможно установить общий запрет или разрешение на доступ к выбранному классу устройств для всего сформированного списка пользователей, установив или сняв флаг **Доступ разрешен** (рисунок 7.40). При установке запрета

116

### 72410666.00063-04 95 01-01

использование любых подключенных к рабочей станции устройств из выбранного класса будет запрещено.

Во вкладке *Аудит* задается перечень событий аудита, которые необходимо фиксировать в журнале аудита (рисунок 7.41). Возможно фиксировать события включения/выключения устройства, успешный доступ к устройству, отказ на доступ к устройству.

Х Изменение клиентской полити	ики: Политика клиента по умолчанию		×
Общее	Контроль устройств		
Windows	🔵 Механизм выключен 🗗		
Linux	USB устройства 🖉 Другие устройства 🖉	ြ Доверенный список 🗗	
Управление входом в ОС	🕑 📋 Устройства хранения данных	Правила доступа Аудит	
Сложность паролей	🥏 🏢 Переносные устройства	Выполнять аудит событий включения/выключения устройств	
Контроль устройств	<ul> <li><sup>(2)</sup> Wi-Fi и Bluetooth адаптеры</li> <li><sup>(2)</sup> Смарт-карты и считыватели</li> </ul>	🗌 Выполнять аудит успешных операций доступа к устройствам 🛛 🗂	
Контроль целостности файлов	Устройства ввода	🛂 Выполнять аудит отказов на доступ к устройствам 🛛 🗗	
Очистка оперативной памяти	🥑 星 Прочие USB устройства		
Мягкий режим			

Рисунок 7.41 – Выбор событий, регистрируемых в журнале аудита

Принудительное наследование параметров (установка «замка») всеми политиками, являющимися дочерними по отношению к текущей, доступно:

- для всего раздела USB-устройств,
- для общего запрета/разрешения на доступ к выбранному классу устройств,
- для пользователя в сформированном списке,
- для регистрируемых событий аудита.

### 7.14.1.2 Настройка разграничения доступа к остальным классам USBустройств

Для USB-устройств классов *Wi-Fi и Bluetooth адаптеры*, *Смарт-карты и считыватели*, *Устройства ввода* и *Прочие USB устройства* предоставление или запрет доступа настраивается на уровне клиентской рабочей станции (рисунок 7.42).



118

🗙 Изменение клиентской полити	ки: Политика клиента по умолчанию		×
Общее	Контроль устройств 🗅		
Windows	🔵 Механизм выключен 🗗		
Linux	USB устройства 🖒 Другие устройства 🖯	🖯 Доверенный список 🕒	
Управление входом в ОС	🥏 📋 Устройства хранения данных	Правила доступа	
Сложность паролей	🥏 🏢 Переносные устройства	🗹 Доступ разрешен 🛛	
Контроль устройств	🥑 🛜 Wi-Fi и Bluetooth адаптеры		
Rompone yerponene	📀 🔟 Смарт-карты и считыватели	Аудит	
Контроль целостности файлов	🥑 🕦 Устройства ввода	🗌 Выполнять аудит включения/выключения устройств 🛛 🗗	
Очистка оперативной памяти	📀 🖳 Прочие USB устройства		
Мягкий режим			

Рисунок 7.42 – Настройка правил доступа для остальных классов USB-устройств

Установить запрет или предоставить разрешение на доступ к выбранному классу устройств на клиентской рабочей станции возможно установив или сняв флаг **Доступ разрешен** в области **Правила доступа** (рисунок 7.42). При установке запрета использование любых подключенных к рабочей станции устройств из выбранного класса будет запрещено.

При необходимости фиксировать в журнале аудита события включения/выключения выбранного класса устройств установите флаг **Выполнять аудит** *включения/выключения устройств* в области **Аудит**.

# 7.14.2 Разграничение доступа к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты

Для настройки разграничения доступа к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты, перейдите в раздел политики **«Контроль устройств»** для OC Linux в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку **Другие устройства** (рисунок 7.43).

Предоставление или запрет доступа для CD/DVD-приводов и устройств, подключаемым через COM- и LPT-порты, настраивается на уровне клиентской рабочей станции.

Х Изменение клиентской политики: Политика клиента по умолчанию		
Общее	Контроль устройств 🗅	
Windows	🕥 Механизм выключен 🗗	
Linux	USB устройства 🗗 Другие устройства 🗗	Доверенный список 🕒
Управление входом в ОС	📀 😓 CD/DVD-приводы	Правила доступа
Сложность паролей	📀 🔤 СОМ	☑ Доступ разрешен 🕒
Контроль устройств	S 🛱 Th	
Контроль целостности файлов		
Очистка оперативной памяти		
Мягкий режим		

Рисунок 7.43 – Настройка правил доступа для CD/DVD-устройств

Установить запрет или предоставить разрешение на доступ к CD/DVD-приводам и устройствам, подключаемым через COM- и LPT-порты, на клиентской рабочей станции возможно установив или сняв флаг **Доступ разрешен** в области **Правила доступа** (рисунок 7.43), в результате чего использование любых подключенных к рабочей станции устройств будет запрещено.

При использовании на клиентской рабочей станции программ по работе с CDи DVD-дисками (для чтения, создания, эмуляции и т.д., например, UltraISO), установленные настройки разграничения доступа к CD-/DVD-приводам будут применены только после перезагрузки рабочей станции.

### 7.14.3 Формирование доверенного списка устройств

Доступ для классов USB-устройств: *Устройства хранения данных* и *Переносные устройства* может настраиваться индивидуально для каждого устройства путем формирования доверенного списка для выбранного пользователя или группы пользователей на клиентской рабочей станции под управлением OC Linux.

После формирования доверенного списка устройств у пользователя или группы пользователей будет доступ к устройству из списка, независимо от ограничений, заданных для классов USB-устройств во вкладке **USB-устройства**. При обращении к устройству из доверенного списка формируется событие аудита на успешный доступ/отказ доступа к устройству.

Общая схема запрета/разрешения доступа пользователя к устройству при сформированном доверенном списке устройств по примеру доступа к USB-устройству приведена на рисунке 7.16.

Для добавления в список доверенных устройств доступны все устройства, которые подключены ко всем клиентским рабочим станциям сервера в настоящий момент или были подключены ранее.

### 72410666.00063-04 95 01-01

Для формирования доверенного списка устройств перейдите в раздел политики **«Контроль устройств»** для ОС Linux в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладку **Доверенный список** (рисунок 7.44).

Во вкладке **Доверенный список** возможно сформировать список устройств, доступных для выбранного пользователя или группы пользователей на клиентской рабочей станции. При этом формирование списка разрешенных устройств возможно только для классов USB-устройств: **Устройства хранения данных** и **Переносные устройства**.

🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию	×
Общее	Контроль устройств 🗗	
Windows	Механизм выключен С	
Linux	USB устройства С Другие устройства С Доверенный список С	
Управление входом в ОС	Q, Поиск	
Сложность паролей	•	
Контроль устройств		
Контроль целостности файлов		
Очистка оперативной памяти		
Мягкий режим	Устройства отсутствуют + Добавить	
	Ок Отмена Применить	

Рисунок 7.44 – Формирование доверенного списка устройств

По кнопке стироется окно **Добавление в список разрешенных устройств** (рисунок 7.45), содержащее список устройств со всех клиентских рабочих станций сервера. Устройства могут быть подключены к рабочей станции в настоящий момент (на значке устройства индикация зеленым цветом) или были подключены к рабочей станции ранее (история подключений из реестра).

🗙 Добавление в список разреши	енных устройств				×
٩	Выберите устройство и нажмите на кнопку "Дале	e"			
w09w13	Все устройства 🔹 🔍				C
	Имя	≜ Вид	Идентификатор	Серийный номер	
	• 📋 Устройства хранения данных				
	<ul> <li>JetFlash Transcend 32GB USB Device - 1</li> </ul>	Модель	VID_8564 PID_1000		
	🔓 JetFlash Transcend 32GB USB Device	Экземпляр	VID_8564 PID_1000	4012611103	

Рисунок 7.45 – Добавление устройств в доверенный список

Устройства в списке структурированы по классу, к которому они относятся (*Устройства хранения данных* и *Переносные устройства*) и по модели устройства.

Идентификатор модели устройства формируется из комбинации идентификатора производителя (*VID*) и продукта (*PID*).

Каждый экземпляр устройства идентифицируется по модели и уникальному серийному номеру устройства.

Выберите нужный экземпляр или модель устройства в окне **Добавление в список** *разрешенных устройств* и нажмите **Далее** (рисунок 7.45).

При добавлении модели устройства будут разрешены все устройства данной модели. При добавлении экземпляра, будет разрешено устройство с конкретным серийным номером.

Для формирования списка пользователей, которым разрешен доступ к выбранному

экземпляру/модели по кнопке (рисунок 7.46) перейдите в окно **Добавление** пользователей (см. раздел *«Добавление пользователей или групп пользователей»*), выберите пользователей или группу пользователей и нажмите **Добавить**.

Х Добавление в список разрешенных устройств			Х
Устройство JetFlash Transcend 32GB USB Device (Экземпляр)			
Имя устройства			
JetFlash Transcend 32GB USB Device			
Пользователи			
+ 🔟 Удалить			Q
Имя Тип	Вид	Разрешить	Запретить
pki.local\user01 Active Directory	Чтение		
pki.local\user02 Active Directory	Запись		

Рисунок 7.46 – Формирование списка пользователей, которым разрешен доступ к устройству

Установите требующиеся ограничения на доступ к выбранному устройству или модели для добавленных пользователей:

- Чтение (возможность чтения пользователем информации с устройства);

- Запись (возможность внесения изменений в информацию на устройстве);

– *Исполнение* (возможность запускать на исполнение информацию на устройстве).

По окончанию формирования списка пользователей, которым разрешен доступ к выбранному устройству/модели нажмите **Добавить**. Во вкладке **Доверенный** *список* отобразится сформированный список устройств, доступных для выбранных пользователей (рисунок 7.47).

Х Изменение клиентской пол	итики: Политика клиента по умолчанию	×
Общее	Контроль устройств	
Windows	USB устройства 🗗 Другие устройства 🗗 Доверенный список. 🖒	
Linux	Q. Поиск	
Управление входом в ОС	+ 🖬 Удалить 🖉 Изменить	🛓 Импорт 👌 Экспорт
Сложность паролей	Имя • Тип устройства Пользов Идентификатор	Серийный номер Вид
Контраль устройств	(ii) JetFlash Transcend 3 Устройства хранения да & 2 VID_8564 PID_1000	Модель

Рисунок 7.47 – Сформированный доверенный список устройств

Принудительное наследование параметров (установка «замка») всеми политиками, являющимися дочерними по отношению к текущей, доступно для всего списка доверенных устройств или для каждого из добавленных устройств отдельно.

По кнопкам 🖄 Импорт / 🖄 Экспорт доступен импорт/экспорт сформированного доверенного списка устройств. При импорте доверенного списка возможно:

– дополнить уже существующий список доверенных устройств объединением имеющегося и импортируемого списков по кнопке **Дополнить** (рисунок 7.48);

– заменить уже существующий список доверенных устройств по кнопке **Замена**<sup>9</sup>: при выполнении замены, существующий список доверенных устройств будет полностью заменен устройствами из импортированного файла.

<sup>&</sup>lt;sup>9</sup> Операция замены списка доверенных устройств может использоваться при импорте списка устройств из программно-аппаратного комплекса автоматизированного учета защищаемых носителей информации (ПАК «САУЗНИ»).

🗙 Импорт		×
! Внимание		
Дополнить список устройств? Вы также можете перезаписать список доверенных устройств, нажав на кнопку "Заменить"		
Дополнить	Заменить	Отмена

Рисунок 7.48 – Выполнение импорта списка доверенных устройств

**(;)** 

Необходимо учитывать, что при выполнении операции импорта перезапись и дополнение списка доверенных устройств будет недоступна для устройств с установленным «замком» (установка принудительного наследования параметров). Если в импортируемом списке будет обнаружено устройство идентичное устройству уже имеющемуся в списке доверенных устройств, при этом на устройстве в списке установлен «замок», изменения из импортируемого списка внесены не будут (рисунок 7.49).

🗙 Импорт		×
🛞 Ошибка		
Для следующих устройств невозможно внести изменения (закрыты замком)		
Имя 🔺 Тип устройства	Идентификатор Серийный номер	р Вид
]] JetFlash Tr Устройства хранени	VID_8564 PID_1000	Модель
	Сохранить в файл	Ок

Рисунок 7.49 – Ошибка при импорте списка доверенных устройств

# 7.15 Контроль целостности файлов в ОС Linux

Раздел клиентской политики «Контроль целостности файлов в OC Linux» предназначен для слежения за неизменностью поставленных на КЦ файлов и каталогов загружаемой OC, а также файлов и каталогов пользователя, целостность которых имеет критическое значение для безопасного функционирования OC.

Для клиентских рабочих станций под управлением ОС семейства Linux администратор может устанавливать на контроль файлы и каталоги клиентских рабочих станций, к которым применяется данная политика, и (или) формировать список исключений файлов и каталогов, контроль целостности которых не будет отслеживаться.

При нарушении целостности файлов и каталогов, установленных на контроль, в случае установки параметра *Формировать события аудита при нарушении целостности файлов* в настройках раздела клиентской политики «Контроль целостности файлов в ОС Linux», в журнале аудита фиксируется событие о выявленном нарушении.

# 7.15.1 Формирование перечня файлов для постановки на КЦ и списка исключений



Необходимо учитывать, что на контроль целостности могут быть установлены только объекты типа «обычный файл» (S\_ISREG). Другие типы файлов игнорируются.

Для постановки файлов на КЦ или формирования списка исключений перейдите в раздел политики «Контроль целостности файлов» в режиме изменения клиентской политики на сервере или в группе рабочих станций во вкладке *Основное* (рисунок 7.50).

X Изменение клиентской политики: Политика клиента по умолчанию X		
Общее	Контроль целостности файлов 🛈 🗗	
Windows	Механизм выключен	
Linux	Файлы и исключения Настройки	🛓 Импорт/рекомендуемые файлы 🔻 🖄 Экспорт
Управление входом в ОС	Контролируемые файлы	Исключения
Сложность паролей	🕞 🕑 Вручную 🔍 Поиск	🕞 🛞 Вручную 🔍 Поиск
Контроль устройств	🖉 Изменить 🛛 Удалить	🖉 Изменить 🔟 Удалить
	Путь	Путь
Контроль целостности файлов	/bin/*	/*.bmp
Очистка оперативной памяти	/etc/*.conf	/*.gif
Мягкий режим	/etc/*.config	/*.gl
	/etc/*_conf	/*.gz
	/etc/*_config	/*.help
	/etc/cron.d/logchecker	/*.info
	/etc/fs/*	/*.jar
	/etc/sudoers/*	/*.log
	/etc/X11/*	/*.msg
	/etc/fstab*	/*.out
	Bcero: 56	Bcero: 33
		Ок Отмена Применить

Рисунок 7.50 – Постановка файлов на КЦ/Формирование списка исключений

Включите механизм КЦ файлов, установив переключатель в положение <sup>С Механизм включен</sup>, и сформируйте перечень файлов и каталогов ОС Linux для постановки на КЦ в левой части вкладки в области *Контролируемые файлы*, и добавьте файлы и каталоги, которые будут исключены при проверке КЦ, в правой части вкладки в области *Исключения* (рисунок 7.51).

По умолчанию в области добавления файлов и каталогов на контроль и в области добавления исключений при проверке КЦ уже содержится перечень масок для файлов и каталогов, рекомендуемых к постановке на КЦ. При необходимости каждый пункт в перечне можно изменить или удалить.

Добавление в список файлов для постановки на КЦ/в список исключений возможно несколькими способами:

 вручную по кнопке <sup>● вручную</sup>, с последующим вводом полного пути к файлу/каталогу (рисунок 7.51) (также доступен ввод масок для файлов и каталогов);



🗙 Изменение клиентской полити	іки: Политика клиента по умолчанию	×
Общее	Контроль целостности файлов 🛈 🗗	
Windows	Механизм включен	
Linux	Файлы и исключения Настройки	🛓 Импорт/рекомендуемые файлы 🔻 🖄 Экспорт
Управление входом в ОС	Контролируемые файлы	Исключения
Сложность паролей	🕞 🕑 Вручную 🔍 Поиск	😡 🕑 Вручную 🔍 Поиск
Контроль устройств	🖉 Изменить 🗑 Удалить 🔒 Блокировать	🖉 Изменить 🗑 Удалить 🔒 Блокировать
Контроль целостности файлов	Путь	Путь
	/home/user/demo/folder1	/home/user/demo/folder1/*.txt
Очистка оперативной памяти	/home/user/demo/folder2/*.sh	
Мягкий режим	/home/user/demo/folder3/*	
	/home/user/demo/file.txt	
	Bcero: 4	Bcero: 1
		Ок Отмена Применить

Рисунок 7.51 – Добавление файлов на КЦ/в список исключений вручную

 перетаскиванием файлов/каталогов из окна Проводника в область списка файлов;

– из файловой системы одной или нескольких удалённых клиентских рабочих

станций под управлением ОС Linux по кнопке 🄤 ;

 по кнопке <sup>ч</sup> импорт</sup> доступен импорт списка файлов/каталогов для постановки на КЦ.

# 7.15.1.1 Добавление в список файлов для постановки на КЦ/в список исключений из файловой системы клиентских рабочих станций

Для добавления в список файлов для постановки на КЦ/в список исключений из файловой системы клиентских рабочих станций под управлением ОС Linux перейдите

по кнопке 🔤 в окно добавления файлов/каталогов на контроль (рисунок 7.52).



🗙 Добавление директорий/файлов контроля	×
Компьютер 🕒 Выбрать	Маски контролируемых файлов
	Э Добавить вручную Изменить Удалить
Компьютер на ОС Linux не выбран	<b>Б</b> ыберите интересующий элемент в дереве слева или добавьте его вручную
	<b>Добавить</b> Отмена

Рисунок 7.52 – Добавление директорий/файлов из файловой системы

В появившемся окне по кнопке выберите из предложенного списка нужную клиентскую рабочую станцию (рисунок 7.53) и нажмите **Добавить**.

🗙 Выбо	р компьютера		×
🗆 к	омпьютеры онлайн	Q. Поиск	
Имя		₹ OC	
<b>5</b> u	17design01	RED OS MU	ROM (7.3.1) (64 бита)
		Deferrer.	
		добавить	Отмена

Рисунок 7.53 – Выбор компьютера для добавления файлов из файловой системы

В окне добавления директорий/файлов появится файловая система выбранной рабочей станции (рисунок 7.54).

72410666.00063-04 95 01-01

GIS ГАЗИНФОРМ СЕРВИС

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

Добавление директорий/файлов контроля	X
Компьютер 😽 u17design01 😽	Маски контролируемых файлов
Place	Эдобавить вручную Изменить Удалить
🔹 😼 u17design01	Путь
• 🗅 /	» /sys/*
• 🗀 bin	» /sys/dev/*
• 🗀 run	>>
• 🗋 lib64	20
• 🗋 dev	20
▼ 🗀 sys	20
kernel	>>
> 🗅 power	30
► 🗋 class	3>
I devices	30
• 🗋 dev 🔅	20
hypervisor 5	20
▶ 🗀 fs	30
	Добавить Отмена

Рисунок 7.54 – Добавление файлов из файловой системы выбранной станции

Добавьте все файлы/каталоги в правую область окна *Маски контролируемых файлов* путем нажатия <sup>»</sup> в строке требуемого к установке файла/каталога (рисунок 7.54).

При необходимости добавления файлов/каталогов из файловой системы другой клиентской рабочей станции, по кнопке 🗟 выберите нужную рабочую станцию и после обновления файловой системы продолжите добавление нужных файлов/каталогов в правую область окна.

В правой области окна *Маски контролируемых файлов* можно изменять уже добавленные маски контролируемых файлов по кнопке *Изменить* или добавлять маски вручную.

После нажатия **Добавить** в перечне файлов для постановки на КЦ/исключений появятся объекты, добавленные из всех файловых систем рабочих станций (рисунок 7.51).

# 7.15.1.2 Добавление в список файлов для постановки на КЦ рекомендованных файлов СЗИ

Для рабочих станций под управлением ОС Linux у администратора имеется возможность поставить на контроль целостности файлы СЗИ.

Для постановки на КЦ файлов СЗИ необходимо нажать на кнопку *Импорт/рекомендуемые файлы* → *Рекомендуемые файлы* (рисунок 7.55).

Изменение клиентской политики: Политика клиента по умолчанию		
Общее	Контроль целостности файлов 💿 🗂	
Windows	🕥 Механизм выключен 🗗	
Linux	Файлы и исключения Настройки	👱 Импорт/рекомендуемые файлы 🔺 🖄 Экспорт
Управление входом в ОС	Контролируемые файлы	Исключения
Сложность паролей	🕞 🕑 Вручную 🔍 Поиск	🔁 🕑 Вручную 🔍 Поиск
Контроль устройств	🖉 Изменить 🛛 Удалить	🖉 Изменить 🔟 Удалить
Контроль целостности файлов	Путь	Путь
	/bin/*	/*.bmp
Очистка оперативной памяти	/etc/*.conf	/*.gif
Мягкий режим	/etc/*.config	/*.gl
	/etc/*_conf	/*.gz
	/etc/*_config	/*.help
	/etc/cron.d/logchecker	/*.info
	/etc/fs/*	/*.jar
	/etc/sudoers/*	/*.log
	/etc/X11/*	/*.msg
	/etc/fstab*	/*.out
	Bcero: 56	Bcero: 33
		Отмена

Рисунок 7.55 – Постановка на КЦ рекомендованных файлов СЗИ

Список рекомендованных для постановки на контроль файлов СЗИ содержит следующие файлы:

СЗИ от НСД «Блокхост-Сеть 4»	Наименование файла
Клиентская часть СЗИ от НСД	/opt/Blockhost/client/libQt5Network.so.5.12.12
	/opt/Blockhost/client/apprunner
	/opt/Blockhost/client/gis_client_localconsoleservice
	/opt/Blockhost/client/libQt5Widgets.so.5.12.12
	/opt/Blockhost/client/libQt5Gui.so.5.12.12
	/opt/Blockhost/client/bhmemd.conf
	/opt/Blockhost/client/libQt5XcbQpa.so.5
	/opt/Blockhost/client/libDataBackup.so
	/opt/Blockhost/client/libConsoleConnector.so
	/opt/Blockhost/client/sys_s.key
	/opt/Blockhost/client/gis_client_info
	/opt/Blockhost/client/ClientDBServiceSettings.json
	/opt/Blockhost/client/libDebugLoggerT.so



/opt/Blockhost/client/libQt5Sgl.so.5 /opt/Blockhost/client/all s.crt /opt/Blockhost/client/libQt5XcbQpa.so.5.12.12 /opt/Blockhost/client/libQt5DBus.so.5.12.12 /opt/Blockhost/client/libodb-2.4.so /opt/Blockhost/client/bhmemd /opt/Blockhost/client/key /opt/Blockhost/client/libQt5Svg.so.5 /opt/Blockhost/client/all.crt /opt/Blockhost/client/sys.crt /opt/Blockhost/client/libQt5Widgets.so.5 /opt/Blockhost/client/sqldrivers/libqsqlite.so /opt/Blockhost/client/gis\_client\_trayapp /opt/Blockhost/client/libDebugLoggerA.so /opt/Blockhost/client/gis client tokensystem /opt/Blockhost/client/sys s.crt /opt/Blockhost/client/libQt5Core.so.5.12.12 /opt/Blockhost/client/libodb-qt-2.4.so /opt/Blockhost/client/libz.so.1 /opt/Blockhost/client/libDebugLoggerTs.so /opt/Blockhost/client/client init /opt/Blockhost/client/libodb-sqlite.so /opt/Blockhost/client/libQt5Network.so.5 /opt/Blockhost/client/libodb-sqlite-2.4.so /opt/Blockhost/client/gis client db /opt/Blockhost/client/libQt5Xml.so.5.12.12 /opt/Blockhost/client/libodb-qt.so /opt/Blockhost/client/libQt5Core.so.5 /opt/Blockhost/client/libQt5Concurrent.so.5.12.12 /opt/Blockhost/client/all.key /opt/Blockhost/client/libQt5Xml.so.5 /opt/Blockhost/client/bhmemk-4.15.3-2-generic.ko /opt/Blockhost/client/gis\_client\_networkclient /opt/Blockhost/client/check vermagic.py /opt/Blockhost/client/run\_local\_console /opt/Blockhost/client/gis client auditsystem /opt/Blockhost/client/gis\_client\_integrity\_checker /opt/Blockhost/client/certificate/LocalConsoleService.key /opt/Blockhost/client/certificate/LocalConsoleService.crt /opt/Blockhost/client/pinapp /opt/Blockhost/client/libQt5DBus.so.5 /opt/Blockhost/client/libodb.so /opt/Blockhost/client/bhgupt /opt/Blockhost/client/libQt5Sql.so.5.12.12 /opt/Blockhost/client/gupt /opt/Blockhost/client/imageformats/libgsvg.so /opt/Blockhost/client/imageformats/libgjpeg.so /opt/Blockhost/client/libQt5Concurrent.so.5 /opt/Blockhost/client/sys.key /opt/Blockhost/client/all s.key /opt/Blockhost/client/libTokenLib.so /opt/Blockhost/client/libz.so.1.2.13 /opt/Blockhost/client/platforms/libqminimal.so /opt/Blockhost/client/platforms/libgoffscreen.so /opt/Blockhost/client/platforms/libqxcb.so



	/opt/Blockhost/client/platforms/libqlinuxfb.so
	/opt/Blockhost/client/libQt5Gui.so.5
	/opt/Blockhost/client/LocalConsole
	/opt/Blockhost/client/LocalConsoleServiceSettings.ini
	/opt/Blockhost/client/AuditClientSettings.json
	/opt/Blockhost/client/libQt5Svg.so.5.12.12
	/opt/Blockhost/client/gis client settings dispatcher
Консоль управления	/opt/Blockhost/console/libOt5Network so 5 12 12
Консоль управлении	/opt/Blockhost/console/libQt5Widgets so 5 12 12
	/opt/Blockhost/console/libOt5Gui so 5 12 12
	/opt/Blockhost/console/libl.icenseSystemWidget.so
	/opt/Blockhost/console/lib/t5Xcb/na so 5
	/opt/Blockhost/console/console
	/opt/Blockhost/console/libOt5Charts so 5 12 12
	/opt/Blockhost/console/libConsoleConnector so
	/opt/Blockhost/console/libOt5Charts so 5
	/opt/Blockhost/console/libDebugl.oggerT.so
	/opt/Blockhost/console/libOt5XchOpa.so.5.12.12
	/opt/Blockhost/console/config
	/opt/Blockhost/console/libOt5DBus so 5 12 12
	/opt/Blockhost/console/libQt5Svg so 5
	/opt/Blockhost/console/libQt50vg.s0.5
	/opt/Blockhost/console/run_config
	/opt/Blockhost/console/libDebugl.orgerA.so
	/opt/Blockhost/console/libDebugEoggerA.so
	/opt/Blockhost/console/libgt3Core.s0.5.12.12
	/opt/Diockhost/console/lib2.so. i
	/opt/Diockhost/console/libDebugLoggerTs.so
	/opt/Diockhost/console/libQt5VmL as 5 12 12
	/opt/Blockhost/console/libdonlovmontSystemPlugin so
	/opt/Diocknost/console/libdeploymentoystemplogin.so
	/opt/Diockhost/console/libQt5Core.so.5
	/opt/Diocknost/console/libQt5Concurrent.so.5.12.12
	/opt/Diocknost/console/libQtoAmi.so.5
	/opt/Blockhost/console/libDebugLoggerD5.so
	/opt/Diocknost/console/iun
	/opt/Blockhost/console/libQt5DBus.so.5
	/opt/Blockhost/console/lib i okenSystemPlugin.so
	/opt/Biocknost/console/imageiormats
	/opt/Blockhost/console/imagelormats/libgsvg.so
	/opt/Biockhost/console/imageiormats/iibdjpeg.so
	/opt/Blockhost/console/libauditwidget.so
	/opt/Blockhost/console/libQtoConcurrent.so.5
	/opt/Biocknost/console/lib i okenLib.so
	/opt/Blockhost/console/libz.so.1.2.13
	/opt/Biocknost/console/platforms/libqxcb.so
	/opt/biocknost/console/llbQt5GUI.S0.5
0 0011 1107	
Серверная часть СЗИ от НСД	/opt/Blockhost/server/libQt5Network.so.5.12.12
	/opt/Blockhost/server/lib1CPProtocol.so
	/opt/Blockhost/server/libcryptoPlatform.so.1.18.1
	/opt/Blockhost/server/libQt5Widgets.so.5.12.12
	/opt/Blockhost/server/libQt5Gui.so.5.12.12
	/opt/Blockhost/server/libQt5XcbQpa.so.5
	/opt/Blockhost/server/gis_server_policy



/opt/Blockhost/server/libDataBackup.so /opt/Blockhost/server/libConsoleConnector.so /opt/Blockhost/server/libDebugLoggerT.so /opt/Blockhost/server/ConsoleServiceSettings.ini /opt/Blockhost/server/libQt5Sql.so.5 /opt/Blockhost/server/libpcre16.so.3.13.3 /opt/Blockhost/server/libQt5XcbQpa.so.5.12.12 /opt/Blockhost/server/libQt5DBus.so.5.12.12 /opt/Blockhost/server/legacy.so /opt/Blockhost/server/libodb-2.4.so /opt/Blockhost/server/libssh.so /opt/Blockhost/server/libQt5Svg.so.5 /opt/Blockhost/server/AuditServerSettings.json /opt/Blockhost/server/libQt5Widgets.so.5 /opt/Blockhost/server/sqldrivers/libqsqlpsql.so /opt/Blockhost/server/sqldrivers/libqsqlite.so /opt/Blockhost/server/libodb-pgsql.so /opt/Blockhost/server/libpcre16.so /opt/Blockhost/server/gis server settings dispatcher /opt/Blockhost/server/libDebugLoggerA.so /opt/Blockhost/server/libQt5Core.so.5.12.12 /opt/Blockhost/server/gis server deploymentsystem /opt/Blockhost/server/libz.so.1 /opt/Blockhost/server/db installation.ini /opt/Blockhost/server/CryptoPlatformWrap /opt/Blockhost/server/libDebugLoggerTs.so /opt/Blockhost/server/libodb-sqlite.so /opt/Blockhost/server/libQt5Network.so.5 /opt/Blockhost/server/libodb-sqlite-2.4.so /opt/Blockhost/server/dogtag requester /opt/Blockhost/server/libQt5Xml.so.5.12.12 /opt/Blockhost/server/libQt5Core.so.5 /opt/Blockhost/server/libQt5Concurrent.so.5.12.12 /opt/Blockhost/server/libQt5Xml.so.5 /opt/Blockhost/server/libDebugLoggerDS.so /opt/Blockhost/server/libTokenSystem.so /opt/Blockhost/server/libserver.so /opt/Blockhost/server/gis\_server\_tokensystem /opt/Blockhost/server/certificate/defaultKeyServer.key /opt/Blockhost/server/certificate/defaultKeyAgent.key /opt/Blockhost/server/certificate/ConsoleService.crt /opt/Blockhost/server/certificate/defaultCertAgent.crt /opt/Blockhost/server/certificate/ConsoleService.key /opt/Blockhost/server/certificate/defaultCertServer.crt /opt/Blockhost/server/libQt5DBus.so.5 /opt/Blockhost/server/libodb.so /opt/Blockhost/server/cleanup\_db\_util /opt/Blockhost/server/utils/install service.exe /opt/Blockhost/server/utils/install service /opt/Blockhost/server/utils/utils tmp /opt/Blockhost/server/utils/emptyfile.txt /opt/Blockhost/server/utils/cert auth config /opt/Blockhost/server/utils/copy\_file\_from /opt/Blockhost/server/utils/check lib /opt/Blockhost/server/utils/copy\_file\_test



/opt/Blockhost/server/libodb-pgsql-2.4.so
/opt/Blockhost/server/gis_server_consoleservice
/opt/Blockhost/server/gis_server_security_monitor
/opt/Blockhost/server/libQt5Sql.so.5.12.12
/opt/Blockhost/server/PolicyServiceSettings.json
/opt/Blockhost/server/gis_server_networkserver
/opt/Blockhost/server/imageformats/libqsvg.so
/opt/Blockhost/server/imageformats/libgjpeg.so
/opt/Blockhost/server/libQt5Concurrent.so.5
/opt/Blockhost/server/libDeploymentBHCommunication.so
/opt/Blockhost/server/libTokenLib.so
/opt/Blockhost/server/gis_server_auditsystem
/opt/Blockhost/server/libpcre16.so.3
/opt/Blockhost/server/libz.so.1.2.13
/opt/Blockhost/server/platforms/libqminimal.so
/opt/Blockhost/server/platforms/libqoffscreen.so
/opt/Blockhost/server/platforms/libqxcb.so
/opt/Blockhost/server/platforms/libqlinuxfb.so
/opt/Blockhost/server/libssh.so.4
/opt/Blockhost/server/libQt5Gui.so.5
/opt/Blockhost/server/TokenSystemSettings.json
/opt/Blockhost/server/libQt5Svg.so.5.12.12

### 7.15.2 Настройки контроля целостности файлов в ОС Linux

Во вкладке *Настройки* раздела политики «Контроль целостности файлов» доступно изменение периодичности проверки целостности файлов, установленных на контроль, и настройка формирования событий аудита при нарушении целостности (рисунок 7.56).

Задайте периодичность проверки целостности файлов, установив время в параметре **Проверять каждые (часы:минуты)**. По умолчанию проверка целостности осуществляется каждые 2 часа.

При необходимости фиксировать в журнале аудита выявленные изменения в контролируемых файлах, установите параметр **Формировать события аудита при обнаружении изменения файлов.** 



🗙 Изменение клиентской полити	ики: Политика клиента по умолчанию			×
Общее	Контроль целостности файлов 🛈 🗅			
Windows	Механизм включен 🗗			
Linux	Файлы и исключения Настройки	⊻ Импо	рт/рекомендуемые фаі	йлы 🔻 🖄 Экспорт
Управление входом в ОС	Выполнять построение отчёта каждые (часы:минуты) 02:00 С	6		
Сложность паролей	Формировать события аудита при обнаружении изменения файлов	6		
Контроль устройств				
Контроль целостности файлов				
Очистка оперативной памяти				
Мягкий режим				
			[]	
		Ок	Отмена	Применить

Рисунок 7.56 – Настройки контроля целостности файлов в ОС Linux

Для принудительного наследования установленных параметров механизма контроля целостности файлов ОС Linux всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке необходимого файла или на всем разделе *Контроль целостности файлов*.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте «*Удаление пользователей или групп пользователей*».

### 7.16 Очистка оперативной памяти в ОС Linux

- (i) Механизм очистки оперативной памяти доступен только для РЕД ОС.
  - Необходимо учитывать, что механизм очистки памяти поддерживает символьные ссылки (SymLink) только на пакет и файл. SymLink на объекты, заданные масками, не поддерживаются.

 $(\mathbf{i})$ 

Очистка памяти выполняется с целью удаления остаточной информации после завершения поставленных на контроль процессов.

Процесс перезаписи оперативной памяти происходит по следующей схеме: по окончании работы контролируемого процесса механизм очистки памяти производит захват всей свободной оперативной памяти, включая и область, освобожденную контролируемым процессом. Захваченные области оперативной памяти перезаписываются маскирующими данными. По мере перезаписи механизм очистки высвобождает перезаписанную область.

При запуске механизма очистки памяти выполняется проверка ядра и в зависимости от того, какое ядро текущее, из пакета выбирается и запускается подходящий модуль ядра.

Если ОС имеет поддерживаемое СЗИ ядро, после установки клиента Блокхост-Сеть и включения механизма очистки памяти, проверка работы механизма очистки памяти будет фиксироваться в журнале событий аудита.

Если ОС имеет не поддерживаемое СЗИ ядро после установки клиента Блокхост-Сеть возможны следующие ситуации:

 механизм очистки памяти выключен – события механизма очистки памяти не фиксируются в журнале событий аудита;

 механизм очистки памяти включен – в журнале событий аудита фиксируется сообщение от механизма очистки памяти о несовместимом ядре;

— механизм очистки памяти включен — установка клиента Блокхост-Сеть производилась на поддерживаемом СЗИ ядре, но при очередном обновлении ОС обновилась до не поддерживаемого ядра, в журнале событий аудита фиксируется сообщение от механизма очистки памяти о несовместимом ядре.

Для настройки параметров механизма очистки оперативной памяти перейдите в раздел политики **«Очистка оперативной памяти»** в режиме изменения клиентской политики на сервере или в группе рабочих станций (рисунок 7.57).



🗙 Изменение клиентской полити	ки: Политика клиента по умолчанию			×
Общее	<ol> <li>Модуль для очистки оперативной памяти доступен только </li> </ol>	для РЕД ОС		
Windows	Очистка оперативной памяти 🖒			
Linux	Механизм выключен			
Управление входом в ОС	Пакеты и исключения Настройки			
Сложность паролей	Контролируемые пакеты/исполняемые файлы	Исключения		
Контроль устройств	Бручную 🗿 🔍 Поиск	Вручную 🛈	Q Поиск	
Контроль целостности файлов				
Очистка оперативной памяти				
Мягкий режим			X×	
	Введите путь, перетащите из проводника или добавьте	Введите путь,	перетащите из прово	дника или добавьте
	каталоги/исполняемые файлы приложений Linux	каталоги/ис	сполняемые файлы п	риложений Linux
	из файловой системы 🖵 Добавить		из фаиловои систе С Добавить	мы
		Ок	Отмена	Применить

Рисунок 7.57 – Механизм очистки оперативной памяти

Включите механизм очистки оперативной памяти, установив переключатель в положение <sup>Механизм включен</sup>, и сформируйте перечень файлов/пакетов OC Linux с целью удаления остаточной информации после завершения поставленных на контроль процессов в левой части вкладки, и добавьте файлы/пакеты, которые будут исключены при удалении остаточной информации, в правой части вкладки в области *Исключения* (рисунок 7.58).

### 7.16.1 Формирование перечня файлов и списка исключений

Добавление файлов/пакетов в список контролируемых файлов/в список исключений возможно несколькими способами:

– вручную по кнопке <sup>Вручную ()</sup>, с последующим вводом полного пути к файлу/пакету (рисунок 7.58) (также доступен ввод масок);



 $(\mathbf{i})$ 

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

Общее	<ol> <li>Модуль для очистки оперативной памяти доступ</li> </ol>	ен только для РЕД ОС	
Windows	Очистка оперативной памяти 🗗		
Linux	💽 Механизм аключен 🗗		
Управление входом в ОС	Контролируемые файлы/пакеты	Исключения	
Сложность паролей	Бручную ④ Q. Поиск Б Удалить	Reprenye 0 Q. Поиск	
Контроль целостности файлов	Visit		
Очистка оперативной памяти	yelp-ssl-338.0-1.el7.noarch		
Магкий режим	bridge-utils-1.5-11.ef7386_64	X×	
		Введите путь, перетащите из проводника или доба файльц/каталоги из файловой системы	986-TC
	Bcero: 3		

Рисунок 7.58 – Добавление файлов на КЦ/в список исключений вручную

При ручном вводе допускается применение следующих масок:

\* – любое количество любых символов;

? – любой одиночный символ;

\ – символ-исключение (при этом в маске «\\*», символ «\*» будет являться именно символом, а не маской).

 перетаскиванием файлов/каталогов из окна Проводника в область списка файлов;

из файловой системы одной или нескольких удалённых клиентских рабочих
 станций под управлением ОС Linux по кнопке
 с выбором:

- добавления в список из файловой системы клиентских рабочих станций под управлением ОС Linux (описано в разделе Добавление в список файлов для постановки на КЦ/в список исключений из файловой системы клиентских рабочих станций);
- добавления в список пакетов клиентских рабочих станций под управлением OC Linux.

# 7.16.1.1 Добавление пакетов в список файлов/в список исключений из файловой системы клиентских рабочих станций

Для добавления пакетов в список файлов/в список исключений из файловой системы

рабочей станции перейдите по кнопке **Б** в окно добавления файлов/пакетов на контроль во вкладку **Пакеты** (рисунок 7.59).

пьютер 👼 u17design01 😡	Добавленные пакеты и файлы	
Файловая система	🗑 Удалить	
Поиск.		
yelp-xsl-3.38.0-1.el7.noarch	* .	
libreswan-3.32-3.el7.x86_64	»	
selinux-policy-targeted-3.14.5-50.el7.noarch	>	
frei0r-plugins-1.7.0-1.el7.x86_64	*	
bridge-utils-1.5-11.el7,x86_64	· LE	
perl-Compress-Raw-Zlib-2.093-2.el7.x86_64	» E	
man-db-2.7.6.1-1.el7.x86_64	» Выберите интересующий эл	емент
gnome-shell-3.38.1-8.el7.x86_64	» в дереве слева или добавьт	e ero
libreport-filesystem-2.14.0-2.el7.noarch	» вручную	
perl-srpm-macros-1-11.el7.noarch	>	
samba-client-libs-4.15.9-2h.el7.3.x86_64	»	
libnftnl-1.1.9-2.el7.x86_64	»	
low-memory-monitor-2.0-1.el7,x86_64	30	
gnu-free-serif-fonts-20120503-21.el7.noarch	>	
mythes-1.2.4-9.el7.x86_64	»	

Рисунок 7.59 – Добавление пакетов/файлов из файловой системы

Добавьте все пакеты в правую область окна **Добавленные пакеты и маски** путем нажатия <sup>»</sup> в строке требуемого к установке пакета.

После нажатия **Добавить** в перечне файлов для постановки на КЦ/исключений появятся объекты, добавленные из всех файловых систем рабочих станций (рисунок 7.60).



Х Изменение клиентской полити	ки: Политика клиента по умолчанию		×
Общее	<ol> <li>Модуль для очистки оперативной памяти доступен</li> </ol>	только для РЕД ОС	
Windows Linux Управление входом в ОС Сложность паролей Контроль целостности файлов Очистка оперативной памяти Мягкий режим	Очистка оперативной памяти С Механизм включен С Пакеты и исключения Настройки Контролируемые файлы/пакеты Вручную О Удалить Изменить Изме	Исключения Воучную (О) Q. Поисс Удалить & Изменить Имя Аляг/Вb64/*	
	<ul> <li>bridge-utils-1.5-11.el7.x86_64</li> <li>/ust/bin/*</li> </ul>	Bcero: 2	
		Ок Отмена	Применить

Рисунок 7.60 – Добавленные на контроль очистки памяти объекты

### 7.16.2 Настройки очистки памяти в ОС Linux

Во вкладке *Настройки* раздела политики «**Очистка оперативной памяти**» доступна настройка формирования событий аудита при очистке памяти (рисунок 7.61).

При необходимости фиксировать в журнале аудита события, поставленные на контроль при очистке памяти, установите параметр **Формировать события аудита.** При этом для дочерних процессов память будет очищаться, но события формироваться не будут.

Для формирования событий аудита при очистке памяти дочерних процессов контролируемых файлов установите параметр **Формировать события аудита при очистке памяти для дочерних процессов.** 



X Изменение клиентской полити	ики: Политика клиента по умолчанию	×
Общее	i Модуль для очистки оперативной памяти доступен только для РЕД ОС	
Windows	Очистка оперативной памяти 🗅	
Linux	■ Механизм включен — 1	
Управление входом в ОС	Пакеты и исключения Настройки	
Сложность паролей	Формировать события аудита ③	
Контроль устройств	🗌 Формировать события аудита при очистке памяти для дочерних процессов 🛈 占	
Контроль целостности файлов		
Очистка оперативной памяти		
Мягкий режим		
	Ок Отмена	Применить

Рисунок 7.61 – Настройки очистки памяти в ОС Linux

Для принудительного наследования установленных параметров механизма очистки памяти OC Linux всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке необходимого файла или на всем разделе *Контроль целостности файлов*.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте «*Удаление пользователей или групп пользователей*».

### 7.17 Мягкий режим работы

Мягкий режим работы используется для первичной настройки средства защиты, до начала эксплуатации. Данный механизм позволяет получить сведения для выявления ошибок в настройках СЗИ и корректировки устанавливаемых политик.

Работа данного механизма заключается в разрешении доступа пользователей к ресурсам, запрещенным настройками СЗИ с фиксацией всех запрещенных попыток доступа в журнале аудита. На основании этих событий, администратор безопасности

выявляет ресурсы, которые необходимо добавить в список разрешенных для данного пользователя и на основе полученных данных выполняет корректировку настроек СЗИ.

При включенном мягком режиме работы вход в операционную систему может выполнить любой доменный или локальный пользователь рабочей станции, если это не противоречит установленным в домене политикам. При этом идентификационные данные пользователя проверяются только средствами операционной системы, а СЗИ только осуществляет проверку в своей базе наличия учетной записи пользователя, выполняющего вход в ОС.

Для установки мягкого режима работы перейдите в раздел политики «**Мягкий режим**» в режиме изменения клиентской политики на сервере или в группе рабочих станций и установите параметр в состояние **Включен** (рисунок 7.62).

🗙 Изменение клиентской полити	іки: Политика клиента по умолчанию	×
Общее	Мягкий режим 🗗	
Windows	Ключен	
Linux		
Мягкий режим		
	Ок Отмена	Применить

Рисунок 7.62 – Мягкий режим работы

Для принудительного наследования возможности использования мягкого режима работы всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе «Мягкий режим».

# 8 Описание серверных политик

Серверные политики определяют параметры работы головных и подчиненных серверов. Для настройки в серверных политиках доступны следующие механизмы:

– **Доступ к серверу** (управление параметрами разграничения доступа пользователей к серверу).

– **Пароли и сессии** (управление параметрами сложности паролей встроенных пользователей Блокхост-Сеть для подключения к серверу).

- **Сбор событий по иерархии** (формирование списка событий и запуска цикла сбора событий с подчиненных серверов и клиентских рабочих станций).



Для всех серверных политик запрещено добавление в политику доменных групп:

- Destributed.

Принудительное наследование в разделах политики может быть установлено целиком на всем разделе, на списке элементов, и на отдельных элементах или группах.

Установка принудительного наследования на всем разделе запрещает изменение всех элементов раздела на нижестоящих уровнях иерархии. Вышестоящая политика наследуется в неизменном виде. Администраторам нижестоящих уровней иерархии не доступно изменение, удаление или добавление элементов (подробнее в разделе *«Принудительное наследование»*).

### 8.1 Доступ к серверу

В разделе **«Доступ к серверу»** серверной политики администратор может предоставлять административные права на доступ к серверу учетным записям пользователей или группам пользователей (рисунок 8.1).



🗙 Изменение серверной полити	іки: Политика сервера по умолчанию			×
Общее	Доступ к серверу	Разрешения		Скрыть
Доступ к серверу	Локальные и доменные пользователи не поддерживаются для доступа к серверу в OC Linux	Тип	Разрешить	Запретить
Пароли и сессии	О. Поиск пользователей	Просмотр		
Сбор событий по иерархии	+ 😈 Удалить	Изменение		
	Пользователь/Группа Тип			
	🔐 💽 Администратор Локальный пользователь			
	🔒 🖧 Администраторы Локальный пользователь			
	Пользователеи: 1 Групп: 1			
	Ок	Отмена	Пр	именить

Рисунок 8.1 – Разграничение доступа к серверу

Доступ к серверу представляет собой список пользователей и групп с сопоставленными им административными правами:

 Просмотр – привилегия просматривать текущие настройки сервера без возможности их изменения;

– **Изменение** – привилегия управлять настройками сервера.

При добавлении пользователя в список по умолчанию ему предоставлены права на просмотр и изменение настроек (рисунок 8.1).

Для всех пользователей, которые не обозначены в данном списке (напрямую или через группы) доступ к серверу будет запрещен.

Администратор может делегировать полномочия следующим типам учетных записей пользователей:

– **Пользователь Windows** – локальный пользователь Windows, созданный непосредственно на сервере;

– **Пользователь Блокхост-Сеть** – встроенный пользователь Блокхост-Сеть, аутентификационные данные которого хранятся исключительно в СЗИ, используется

для подключения к серверу.

При доступе к серверу под управлением ОС Linux поддерживаются только встроенные пользователи Блокхост-Сеть. Локальные и доменные пользователи не поддерживаются.

По умолчанию в серверной политике OC Windows в списке пользователей присутствуют:

– **Администратор** – локальный «встроенный» администратор сервера (не доступен к удалению);

- Администраторы – локальная группа администраторов сервера.

По умолчанию в серверной политике OC Linux в списке пользователей присутствует:

*admin* – встроенный администратор Блокхост-Сеть (не доступен к удалению).

Административные права для пользователя с учетом настроек групп, куда входит данный пользователь, вычисляются исходя из правил пересечения прав, описанных в разделе *«Пересечение прав»*.

### 8.1.1 Добавление пользователей или групп пользователей

Для добавления пользователей или группы пользователей, которым требуется предоставить административные права, перейдите в раздел политики **«Доступ к** 

**серверу»** в режиме изменения серверной политики на сервере, нажмите кнопку (рисунок 8.2) и выберите тип добавляемого пользователя.

🗙 Изменение серверной политики: Политика сервера по умолчанию				×
Общее	Доступ к серверу	Разрешения		Скрыть
Доступ к серверу	Локальные и доменные пользователи не поддерживаются для доступа к серверу в OC Linux	Тип	Разрешить	Запретить
Пароли и сессии	Q. Поиск пользователей	Просмотр		
Сбор событий по иерархии	+ Ш Удалить	Изменение		
	📲 Пользователь Windows 🔒			
	Х Пользователь Блокхост-Сеть окальный пользователь			
	💕 പ്പ്പ് Администраторы Локальный пользователь			

Рисунок 8.2 – Добавление пользователя или группы пользователей

При выборе типа пользователя **Пользователь Windows** появится окно добавления доменных и локальных пользователей рабочей станции, которым необходимо настроить доступ к серверу (см. раздел **«Добавление пользователей или групп** пользователей»).

После нажатия кнопки **Добавить**, добавленный пользователь или группа отобразятся в списке пользователей окна **Доступ к серверу** (рисунок 8.3).

### 72410666.00063-04 95 01-01


🔀 Изменение серверной полити	ки: Политика сервера по умолчанию		×
Общее	Доступ к серверу	Разрешения	Скрыть
Доступ к серверу	🔍 Поиск пользователей		
Пароли и сессии	+ 🗠 Сменить пароль 🔟 Удалить	Тип Разрешить	Запретить
Сбор событий по иерархии	Пользователь/Группа Тип	Изменение И	
	pki.local\user01 Active Directory	Изменение	
	💕 💽 test_user Блокхост-Сеть		
	💕 💽 w09w13\localUser Локальный пользователь		
	🖌 💽 Администратор Локальный пользователь		
	🔒 മ്പ്പ് Администраторы Локальный пользователь		

Рисунок 8.3 – Отображение добавленного пользователя

При выборе типа пользователя **Пользователь Блокхост-Сеть** появится окно (рисунок 8.4) создания нового пользователя, которому необходимо настроить доступ к серверу.

Требования к имени создаваемого пользователя и к предъявляемому паролю указаны в окне создания (рисунок 8.4):

- Пароль должен содержать от 8 до 16 символов.
- Пароль должен содержать символы как минимум из трех групп в списке ниже:
  - символы верхнего регистра (A-Z);
  - символы нижнего регистра (a-z);
  - цифры (0-9);
  - специальные символы (@ # \$ % ^ & \* \_ ! + = [ ] { } < > | : ' , . ? / \ ` ~ " ( ) ;).

– Пароль не должен содержать пробелов и символов Юникода.

Предъявляемый пароль пользователя Блокхост-Сеть проверяется на соответствие требованиям:

при создании внутреннего пользователя Блокхост-Сеть;

 при изменении пароля внутреннего пользователя Блокхост-Сеть по требованию администратора;

 при изменении пароля внутреннего пользователя Блокхост-Сеть при подключении к серверу под учетной записью этого внутреннего пользователя.

145



X Создание пользоват	еля Блокхост-Сеть	×
Имя пользователя ③		
test_user1		
Пароль		
•••••	•	$\odot$
Повторите пароль		
		$\odot$
Пароль должен содерж Пароль должен включа - символы верхнего рег - символы нижнего рег - цифры (0-9) - специальные символи	ать от 8 до 16 символов. ать символы как минимум гистра (A-Z) истра (a-z) ы (@ # \$ % ^ & *!+ = []	низ 3 групп: ] { } < >   : ' , . ? / `~ " () ;)
	Создать	Отмена

Рисунок 8.4 – Создание нового пользователя Блокхост-Сеть

Для принудительного наследования пользователя/группы пользователей всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке элемента списка.

Принудительное наследование дочерними политиками пользователей типа Локальный пользователь и Пользователь Блокхост-Сеть недоступно.

Удаление пользователей или группы пользователей в списке разграничения доступа к серверу выполняется аналогично удалению пользователей в списке настроек доступа в клиентской политике (см. раздел *«Удаление пользователей или групп пользователей»*).

## 8.2 Пароли и сессии

В разделе «Пароли и сессии» серверной политики администратор может установить параметры сложности паролей встроенных пользователей Блокхост-Сеть для подключения к серверу и параметры для подключения консоли управления к серверу Блокхост-Сеть (рисунок 8.5).

Настройка параметров сложности паролей встроенных пользователей Блокхост-Сеть заключается в установке:

 срока действия пароля, при превышении которого при следующем подключении консоли управления к серверу пользователю будет предложено сменить пароль (максимальный срок действия пароля ограничен 365 днями)

– блокировки на ранее используемые пароли пользователя (при смене пароля



пользователя будет выполнять проверка нового пароля на совпадение с пятью предыдущими паролями, используемыми пользователем).

Настройка параметров для подключения к серверу Блокхост-Сеть заключается в установке интервала времени, по истечению которого при отсутствии активности подключение консоли управления к серверу будет разорвано (максимально возможный интервал времени 24 часа). Под активностью консоли подразумеваются какие-либо действия, совершаемые администратором и приводящие к обмену данными между консолью и сервером.

🗙 Изменение серверной полити	ки: Политика сервера по умолчанию			×
Общее	Сложность паролей пользователей Блокхост	г-Сеть ©		
Доступ к серверу	Срок действия пароля (дней) ③	90	6	
Пароли и сессии	🗌 Блокировать ранее используемые пароли 🛈 🕒			
Сбор событий по иерархии	Подключения к серверу Блокхост-Сеть 🛈			
	Разрывать подключение к серверу при отсутствии активности 3	45 мин 🔹	6	
		Ок	Отмена	Применить

Рисунок 8.5 – Установка параметров сложности пароля и подключения к серверу

## 8.3 Сбор событий по иерархии

В разделе **«Сбор событий по иерархии»** серверной политики администратор может выбрать события, собираемые с подчиненных серверов и клиентских рабочих станций под управлением OC Windows/Linux; события, с клиентских рабочих станций с установленным СДЗ; определить периодичность опроса подчиненных серверов и клиентов, и задать, при необходимости, период, в который сбор событий не осуществляется (рисунок 8.6).

Настройка механизма сбора событий заключается в формировании списка событий,

#### 72410666.00063-04 95 01-01

необходимых к сбору по всей иерархии подчиненных серверов и клиентских рабочих станций, и формировании расписания сбора указанных событий.

X Изменение серверной политики: Политика сервера по умолчанию X			
Общее	Сбор событий с Windows/Linux 🗅		
Доступ к серверу	Показать всё 💌 🔍 Поиск		
Пароли и сессии	🖋 Выбрать все 🗍 Снять все 🔒 Проставить всё 🗗	Снять всё к Свернуть всё	ч <sup>л</sup> Раскрыть всё 🖄 🖄
Сбор событий по иерархии	Тип события 🔻 ОС	Уровень важности	Код
Windows/Linux	▶ АДМИНИСТРИРОВАНИЕ - 2/15		
СДЗ (Средство доверенной загрузки)	<ul> <li>АУДИТ ДОСТУПА К МЕДИАФАЙЛАМ - 1/1</li> <li>САРАНТИРОВАННОЕ УЛА ЛЕНИЕ ФАЙЛОВ - 2/4</li> </ul>		
Расписание	Гарантированное удаление файлового	і Сведения	769
	Гарантированное удаление файлового 💧	і Сведения	772
	🔒 🗹 Невозможно завершить операцию гар 📲	🗵 Ошибка	771
	🔒 🗹 Невозможно завершить операцию гар 💧	🗵 Ошибка	773
	• ДИСКРЕЦИОННЫЙ ДОСТУП - 2/4		
	<ul> <li>ЗАПУСК ПРИЛОЖЕНИЙ - 2/3</li> </ul>		
	🔒 🗹 Завершение процесса 📲	Cведения	3878
	🔒 🗹 Запуск процесса 📲	Cведения	3877
	Отказ на запуск процесса	• Предупреждение	3876
	▶ КОНТРОЛЬ ПЕЧАТИ - 2/2		
	Выбрано: 104 Всего: 211		
		Ок	мена Применить

Рисунок 8.6 – Настройка сбора событий аудита Windows/Linux

## 8.3.1 Сбор событий с Windows/Linux

Для настройки сбора событий аудита перейдите в раздел политики «Сбор событий по иерархии» в режиме изменения серверной политики.

Во вкладке *Windows/Linux* содержится полный список регистрируемых событий, структурированных по разделам.

Для каждого события в списке отображается краткое описание типа события, уровень важности события (*Сведения*, *Предупреждение* или *Ошибка*) и уникальный код типа события.

События, доступные к сбору для клиентских рабочих станций под управлением ОС Windows отмечены пиктограммой III в столбце ОС. События, доступные к сбору для клиентских рабочих станций под управлением ОС Linux отмечены пиктограммой ов столбце ОС.

Формирование списка событий с подчиненных серверов и клиентских рабочих

## 72410666.00063-04 95 01-01



станций осуществляется установкой флага в строке с требующимся типом события.

Для принудительного наследования событий всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на необходимых типах событий или на всем разделе сбора событий.

#### 8.3.2 Сбор событий с СДЗ

Для настройки сбора событий аудита перейдите в раздел политики «Сбор событий по иерархии» в режиме изменения серверной политики.

Во вкладке *СДЗ (Средство доверенной загрузки)* содержится полный список регистрируемых событий, доступных к сбору для клиентских рабочих станций с установленным СДЗ. События структурированы по разделам (рисунок 8.7).

Для каждого события в списке отображается краткое описание типа события, уровень важности события (*Сведения*, *Предупреждение* или *Ошибка*) и уникальный код типа события.

Формирование списка событий с клиентских рабочих станций осуществляется установкой флага в строке с требующимся типом события.

Для принудительного наследования событий всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на необходимых типах событий или на всем разделе сбора событий.



🗙 Изменение серверной полити	🗙 Изменение серверной политики: Политика сервера по умолчанию			
Общее	Сбор событий с СДЗ (Средства доверенной загрузки) 🗅			
Доступ к серверу	С. Поиск			
Пароли и сессии	🖋 Выбрать все 📋 Снять все 🔒 Проставить всё 🗗 Снять всё 🎽 к Свернуть всё 🖉 Раскрыть всё	± č		
Сбор событий по иерархии	Тип события 👻 Уровень важности Код			
Windows/Linux	КОНТРОЛЬ ЦЕЛОСТНОСТИ - 11/11			
СДЗ (Средство доверенной	▼ СОБЫТИЯ КЛИЕНТА СДЗ - 5/5			
загрузки)	🔒 🗹 Взятие под управление Блокхост-Сеть i Сведения 5005			
Расписание	🔒 🗹 Выход из-под управления Блокхост-Сеть i Сведения 5006			
	🔒 🗹 Загрузка ОС 🕕 Сведения 5000			
	🔒 🗹 Не удалось загрузить ОС 😢 Ошибка 5001			
	🔒 🗹 Ошибка взятия под управление Блокхо 🛞 Ошибка 5007			
	• УПРАВЛЕНИЕ ВХОДОМ В СДЗ - 4/4			
	🔒 🗹 Аутентификация пользователя 🕕 Сведения 5050			
	🔒 🗹 Отказ на аутентификацию пользователя 🌔 Предупреждение 🛛 5053			
	🔒 🗹 Смена пароля пользователя 🕕 Сведения 5052			
	🔒 🗹 Смена пин-кода токена 🕕 Сведения 5051			
	Выбрано: 20 Всего: 20			
	Ок Отмена Прим			

Рисунок 8.7 – Настройка сбора событий аудита СДЗ

## 8.3.3 Расписание опроса подчиненных серверов и клиентских компьютеров

Вкладка *Расписание* (рисунок 8.8) предназначена для настройки периодичности запуска сбора событий аудита с подчиненных серверов и клиентских рабочих станций.



🗙 Изменение серверной полити	ки: Политика сервера по умолчанию	×
Общее	Расписание сбора событий 🗅	
Доступ к серверу Пароли и сессии Сбор событий по иерархии	Подчиненные серверы பி Периодичность запуска цикла опроса 2 часа т	Клиентские компьютеры 🗅 Периодичность запуска цикла опроса 15 мин 👻 🗅
Windows/Linux	+ Исключения 🖒 🛈 Подробнее	+ Исключения 🗠 ③ Подробнее
СДЗ (Средство доверенной загрузки)	Временной интервал	
Расписание	0.00 - 01.00	
		Сраничения по сбору событий отсустсвуют Добавить
		Ок Отмена Применить

Рисунок 8.8 – Настройка расписания опроса подчиненных серверов и клиентов

**Периодичность запуска цикла опроса** – это период между окончанием предыдущей загрузки событий аудита с подчиненных серверов/клиентских компьютеров и началом следующей загрузки. Периодичность запуска цикла для подчиненных серверов варьируется в пределах 30 мин – 6 часов, для клиентских рабочих станций в пределах 5 мин – 4 часа.

При необходимости в расписание сбора событий можно добавить временной интервал или несколько интервалов, в которые сбор событий с подчиненных серверов и клиентских рабочих станций не будет осуществляться – *период запрета*.

Для добавления периода запрета сбора событий по кнопке появившемся окне время начала и время окончания периода, в который сбор событий с подчиненных серверов или клиентских рабочих станций осуществляться не будет (рисунок 8.9).

GIS газинформ сервис	СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками	152
	🔀 Добавление исключения для сбора событий 🛛 🗙	
	Период запрета не должен включать в себя уже добавленные интервалы времени	
	Период запрета 00:00 - 01:00	

Рисунок 8.9 – Ввод	интервала	времени	прерывания	загрузки	событий

Добавить

Отмена

## 8.3.4 Пересечение времени запуска цикла опроса с промежутком прерывания

Время запуска цикла опроса в соответствии с заданной периодичностью и промежуток времени, в который загрузка событий аудита осуществляться не должна (период запрета), могут пересекаться.

При этом в зависимости от точки пересечения этих параметров, цикл опроса может быть запущен и прерван, либо не начаться вообще.

Рассмотрим возможные варианты пересечения и итоговый результат на примерах.

#### Пример 1:

Время запуска следующего цикла опроса попадает в интервал времени, в который загрузка не должна осуществляться.

Время завершения предыдущего цикла опроса: 10:25 (рисунок 8.10).

Последний цикл опро	са аудита Подч	иненные сервера	Ŧ
Статус	завершен		
Время начала	10:25:39 01.12.2020		
Время завершения	10:25:40 01.12.2020		
Длительность	меньше минуты		

Рисунок 8.10 – Время завершения цикла опроса

Заданная периодичность опроса: 2 часа, промежуток прерывания: 12:00 – 13:00 (рисунок 8.11).

GIS ГАЗИНФОРМ СЕРВИС	СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1	153
	Управление политиками	
	Подчиненные сервера 🗅	
	Периодичность запуска цикла опроса 🛛 2 часа 🔹 🗗	
	+ Исключения 🖒 🛈 Подробнее	
	Временной интервал	
	12:00 - 13:00	

Рисунок 8.11 – Период исключения сбора событий

Результат: цикл опроса не будет запущен.

#### Пример 2:

Цикл следующего опроса начинается раньше интервала времени, в который загрузка не должна осуществляться, но в процессе выполнения пересекается с ним.

Время завершения предыдущего цикла опроса: 10:25 (рисунок 8.10).

Заданная периодичность: 1 час, промежуток прерывания: 11:45 – 12:45 (рисунок 8.12).

Подчиненные сервера 🗅		
Периодичность запуска цикла опроса 1 час	• 6	
+ Исключения 占	Подробнее	
Временной интервал		
11:45 - 12:45		

Рисунок 8.12 – Период исключения сбора событий

Результат: цикл опроса будет запущен в 11.25 и продлится 10 минут. В 11.45 цикл будет прерван. Последующий запуск цикла будет осуществлен в соответствии с заданной периодичностью в полном объеме.

## 9 Описание политик SafeNode System Loader

Политики SafeNode System Loader позволяют установить дополнительный этап прохождения аутентификации пользователей до загрузки ОС с помощью средства доверенной загрузки (СДЗ) «SafeNode System Loader» и определяют параметры аутентификации пользователей до загрузки ОС.

СДЗ «SafeNode System Loader» обеспечивает доверенную загрузку OC. установленных на совместимые с архитектурой Intel x86-64 ЭВМ. Результатом ОС является гарантия доверенной загрузки санкционированной загрузки зарегистрированным пользователем. Загрузка ОС на рабочую станцию выполняется только после проведения контроля целостности (КЦ) аппаратной и программной конфигурации станции, гарантирующей невозможность подмены ОС на этапе загрузки и работу пользователей с доверенной ОС в штатном режиме.

Для настройки в политиках SafeNode System Loader доступны следующие механизмы:

 Настройка ехода (управление выбором дополнительного средства аутентификации пользователей до загрузки ОС при входе на клиентские рабочие станции с помощью СДЗ «SafeNode System Loader»).

– **Управление аутентификацией** (управление параметрами аутентификации пользователей до загрузки ОС при входе на клиентские рабочие станции если в механизме **Настройки входа** установлено дополнительное средство аутентификации СДЗ «SafeNode System Loader»).

– **Сложность пароля** (управление ограничениями при задании пароля пользователя и администратора для входа на клиентские рабочие станции при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader»).

– **Контроль целостности** (управление параметрами КЦ аппаратной и программной конфигурации рабочей станции: объектами файловой системы, объектами реестра OC Windows, аппаратных устройств ЭВМ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI).

– *Настройки подключения к домену* (настройка параметров сервера LDAP через файлы конфигураций hosts, krb5.conf и ldap.conf для аутентификации пользователей, зарегистрированных на сервере LDAP).

– **Сетевой адаптер UEFI** (установка способа получения сетевых настроек на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» для взаимодействия клиента и сервера LDAP).

– *Мягкий режим* (установка режима работы клиентских рабочих станциях при котором СДЗ «SafeNode System Loader» работает в режиме установки, используется для первичной настройки до начала эксплуатации).

**S** газинформ сервис Принудительное наследование в разделах политики может быть установлено целиком на всем разделе, на списке элементов, и на отдельных элементах или группах.

Установка принудительного наследования на всем разделе запрещает изменение всех элементов раздела на нижестоящих уровнях иерархии. Вышестоящая политика наследуется в неизменном виде. Администраторам нижестоящих уровней иерархии не доступно изменение, удаление или добавление элементов (подробнее в разделе *«Принудительное наследование»*).

## 9.1 Настройка входа

Раздел политики SafeNode System Loader **«Настройка входа»** предназначен для выбора средства аутентификации пользователей при входе на клиентские рабочие станции:

 аутентификация пользователей на этапе после загрузки ОС средствами СЗИ от НСД «Блокхост-Сеть 4» (настройка описана в разделе Управление входом в ОС клиентской политики);

двухэтапная аутентификация пользователей:

- на этапе до загрузки ОС средствами СДЗ «SafeNode System Loader» (настройка описана в разделе **Управление аутентификацией** политики SafeNode System Loader);
- на этапе после загрузки ОС средствами СЗИ от НСД «Блокхост-Сеть 4» (настройка описана в разделе Управление входом в ОС клиентской политики).

Для выбора дополнительного средства аутентификации пользователей до загрузки ОС перейдите в раздел политики «Настройка входа» в режиме изменения политики SafeNode System Loader на сервере или в группе рабочих станций и установите переключатель в положение <sup>©</sup> SafeNode System Loader и Блокхост-Сеть</sup> (рисунок 9.1).

Для принудительного наследования установленных параметров всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе.



156

X Изменение политики модуля 9	SafeNode System Loader: Политика SafeNode System Loader по умолчанию	×
Общее	Настройка входа 占	
Настройка входа	Аутентификация средствами:	
Управление аутентификацией	. ● Блокхост-Сеть ③	
Сложность пароля	🚫 SafeNode System Loader и Блокхост-Сеть 🛈	
Контроль целостности		
Настройки подключения к домену		
Сетевой адаптер UEFI		
🕥 Мягкий режим 🛈 占		
	Ок Отмена Применить	

Рисунок 9.1 – Выбор дополнительного средства аутентификации пользователей

## 9.2 Управление аутентификацией

Раздел политики SafeNode System Loader **«Управление аутентификацией»** предназначен для управления параметрами аутентификации доменных пользователей и пользователей SafeNode System Loader при входе на клиентские рабочие станции с установленным и взятым под управление СДЗ «SafeNode System Loader».

Настройки входа представляют собой список пользователей с сопоставленными им настройками аутентификации. Для всех пользователей, которые не обозначены в данном списке вход на клиентские рабочие станции с установленным и взятым под управление СДЗ «SafeNode System Loader» будет запрещен.

Предусмотрены следующие возможные параметры аутентификации пользователей при входе на клиентские рабочие станции если установлено дополнительное средство аутентификации СДЗ «SafeNode System Loader» до загрузки ОС, описанные в таблице 9.1.

Аутентификация	Описание	Возможные виды	Комментарий
		входа	
Доверять	Аутентификация	Любой возможный	Данный вид входа доступен
аутентификации	доменного	поддерживаемый	только доменному
домена	пользователя,	вид входа:	пользователю.
	предполагающая	• вход по токену;	При входе пользователя
	полное доверие		идентификационные данные
	проверкам входа,	• вход по	пользователя проверяются
	выполняемым	паролю;	средствами домена, СДЗ
	доменом		«SafeNode System Loader» не
		и токену	осуществляет проверку в
		n rokony.	своей базе наличия учетной
			записи пользователя,
			выполняющего вход.
			Аутентификация будет
			проводиться в любом домене
			в соответствии с настройками
			сетевого адаптера UEFI и
			конфигурационных файлов
			krb5 и ldap (см. разделы
			Настройки сети и Сетевой
_			адаптер UEFI).
Вход с	Аутентификация	• вход по токену	При входе пользователя
использованием	возможна только с		идентификационные данные
смарт-карты	использованием		пользователя проверяются
	токена, назначенного		средствами домена, СДЗ
	10119308916110		«Salenode System Loader»
			своей базе напишия учетной
			успешности проверки
			допускает пользователя до
			входа в систему.
			Если пользователь вводит
			корректные
			идентификационные данные
			из домена, но его нет в базе
			данных СДЗ, ему будет
			отказано в аутентификации.
Дополнительная	Аутентификация	• вход по	При выборе типа
проверка	возможна только с	сертификату на	аутентификации « <b>Вход с</b>
сертификата	использованием	токене	использованием смарт-
	сертификата на		карты» с установленным
	токене, назначенного		флагом « <b>Дополнительная</b>
	пользователю		проверка сертификата»
			при входе доменного
			пользователя или

#### Таблица 9.1 – Возможные виды входа пользователя в систему

			пользователя SafeNode
			System Loader выполняется
			дополнительная проверка в
			базе данных СДЗ привязки
			сертификата на токене к
			пользователю, который его
			предъявляет.
			При первой успешной
			аутентификации
			пользователя, если
			пользователь есть в базе
			данных, но к нему не привязан
			сертификат, сертификат
			добавляется в базу данных.
Вход по паролю <sup>10</sup>	Аутентификация с	• вход по	При входе пользователя
	помощью пароля,	паролю,	SafeNode System Loader
	вводимого	вводимому	выполняет проверку
	пользователем	вручную.	введенного пароля с паролем
	вручную		пользователя, хранящимся в
			БД

## 9.2.1 Аутентификация по паролю

Аутентификация доменных пользователей и пользователей SafeNode System Loader с использованием пароля осуществляется в настройках клиентской рабочей станции, если вышестоящим сервером установлено разрешение на данную настройку. Подробное описание настройки приведено в разделе *«Проверка пароля в SafeNode»*.

Для входа доменных пользователей и пользователей SafeNode System Loader по паролю необходимо добавить пользователей в список раздела политики «Управление аутентификацией» без дополнительных настроек аутентификации (подробное описание добавления пользователей в политику описано в разделе «Добавление доменных пользователей и пользователей SafeNode System Loader»).

# 9.2.2 Добавление доменных пользователей и пользователей SafeNode System Loader

Для добавления доменных пользователей и пользователей SafeNode System Loader, которым требуется установить настройки входа, перейдите в раздел политики «Управление аутентификацией» в режиме изменения политики SafeNode System

Loader на сервере или в группе рабочих станций и нажмите кнопку 🛄 (рисунок 9.2).

<sup>&</sup>lt;sup>10</sup> Настройка входа по паролю доменных пользователей и пользователей SafeNode System Loader осуществляется в настройках клиентской рабочей станции (см. раздел **«Проверка пароля в SafeNode»**).



🗙 Изменение политики модуля	SafeNode System Loader: Поли	тика SafeNode System Loader по умолчанию			×
Общее	Управление аутен	нтификацией пользователей 🗅			
Настройка входа		0			
Управление аутентификацией	Список пользователей г	⊃ ↑ Дополнительные настройки			
Сложность пароля	+				
Контроль целостности	🚸 Из домена/компьюте	pa	Аутентификация		
Настройки подключения	💂 Вручную		Тип	Разрешить Запретить	2
кдомену		Доменный пользователь	Доверять аутентификаци домена	и 🔽 🗌	
Сетевой адаптер UEFI		Доменный пользователь	Вход с использованием смарт-карты		
	∕ <b>∕</b> ⊌ User1	Пользователь SafeNode	Дополнитеьная проверка сертификата		
🔲 Мягкий режим 🛈 占	Bcero 3				
			Ок Отмена	Применить	

Рисунок 9.2 – Управление аутентификацией

Добавление пользователей возможно из домена/компьютера или вводом имени пользователя вручную (рисунок 9.2).

#### 9.2.2.1 Добавление пользователей из домена/компьютера

Для добавления пользователей из домена/компьютера нажмите на кнопку выберите *Из домена/компьютера* (рисунок 9.2). В появившемся окне (рисунок 9.4) добавьте учетную запись пользователя которой необходимо установить настройку входа.

Для добавления доступны:

 доменные пользователи (во вкладке Домены). Для добавления доменного пользователя во вкладке Домены выберите нужный домен или, при отсутствии необходимого домена в списке, добавьте его по ссылке • Добавить домен (рисунок 9.4 а).

 локальные пользователи SafeNode (во вкладке Компьютеры). Для добавления локального пользователя перейдите во вкладку Компьютеры и выберите рабочую станцию (во вкладке отображаются только рабочие станции с установленным и взятым под управление СДЗ «SafeNode System Loader»),



локального пользователя которой требуется добавить (рисунок 9.4 б). Возможна фильтрация выбираемых рабочих станций для поиска машин только в состоянии *Онлайн,* или ввод имени рабочей станции для поиска по иерархии.

При добавлении пользователей SafeNode, если на выбранной рабочей станции не установлено или не взято под управление СДЗ «SafeNode System Loader», выбор пользователей будет недоступен (рисунок 9.3).

X Добавление пользователей			×
Домены Компьютеры Все т Q. Поиск	C	Пользователи	Будут добавлены
wBHN03			
Bcero: 1		На компьютере не установлен/не взят под управление модуль SafeNode System Loader	Выбранные пользователи отсутствуют
			Добавить Отмена

Рисунок 9.3 – На рабочей станции не установлено СДЗ «SafeNode System Loader» Домены во вкладке **Домены** подразделяются на:

- *системные* домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения. Системный домен невозможно удалить из списка.

- пользовательские домены, которые добавляются по кнопке • Добавить домен. При подключении к пользовательскому домену всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется). Пользовательский домен возможно удалить из списка.

Администратор имеет возможность выполнить подключение/переподключение к домену под нужной ему учетной записью (ввести логин/пароль).

При выборе домена или компьютера, в средней части окна отобразятся учетные записи, доступные для добавления в список пользователей. Выбранные пользователи дублируются в правой части окна.

## 72410666.00063-04 95 01-01





Домены Компьютеры	С Пользователи		Будут добавлены - 3
Домены Компьютеры	С Пользователи С Понск Имя Имя Уз User 12_430a25e90 Уз User 13_430a25e90 Уз User 14_430a25e90 Уз User 15 Уз User 16	<ul> <li>Тип пользователя</li> <li>Ос33976118eb86cdb7 SafeNode</li> <li>Ос33976118eb86cdb7 SafeNode</li> <li>Ос33976118eb86cdb7 SafeNode</li> <li>SafeNode</li> <li>SafeNode</li> <li>SafeNode</li> </ul>	Bydyr Hoodabrenai - 3         User 16         WBHN03 (SafeNode)         User 17         WBHN03 (SafeNode)         User 18         WBHN03 (SafeNode)
Bcero: 1	Image: System 17         Image: System 17	SafeNode SafeNode SafeNode c33976118eb86cdb72 SafeNode cc33976118eb86cdb7 SafeNode	
			Далее Отмена
		б)	

Рисунок 9.4 – Добавление пользователей

После нажатия кнопки **Добавить**, добавленные пользователи отобразятся в списке пользователей окна **Управление аутентификацией пользователей** (рисунок 9.5).

161



🗙 Изменение политики модуля	SafeNode System Loader: Политика	a SafeNode System Loader по умолча	чию		×
Общее	Управление аутенти	фикацией пользовател	ей 🗅		
Настройка входа					
Управление аутентификацией	Механизм включен				
Сложность пароля		Дополнительные настройки			
Контроль целостности	Т Уладиять			Аутентификация	
Настройки подключения	Пользователь	Тип		Тип	Разрешить Запретить
к домену	✓ user1	Пользователь SafeNode		Вход с использованием смарт-карты	
Cerebou adamep otri		Доменный пользователь			
	😤 Guest\pki.local	Доменный пользователь			
🕥 Мягкий режим 🛈 占	Bcero 3				
			Ок	Отмена	Применить

Рисунок 9.5 – Отображение добавленных пользователей

Для принудительного наследования списка пользователей всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке элемента списка, на всем списке или на всем разделе управления аутентификацией.

## 9.2.2.2 Добавление пользователей вручную

Для добавления пользователей вручную нажмите на кнопку <sup>+</sup> и выберите **Вручную** (рисунок 9.2). В появившемся окне (рисунок 9.6) ведите имя локального пользователя SafeNode и нажмите **Добавить**. Созданный пользователь отобразится в списке пользователей окна **Управление аутентификацией пользователей** (рисунок 9.5).

СЕРВИС	СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками	
🗙 Изменение политики модуля	SafeNode System Loader: Политика SafeNode System Loader по умолчанию	
Общее	Управление аутентификацией пользователей 🗅	
Настройка входа		
Управление аутентификацией	С Механизм включен С	
Сложность пароля	Список пользователей дополнительные настроики	
Контроль целостности		
Настройки подключения	Пользователь Тип	
Сетевой здаптер ЦЕЕТ	🄏 user1 🔀 Добавление локального пользователя SafeNode 🛛 🗙	
сегевой адаттер ост	📯 ivanov-i\pk Имя пользователя	
	S Guest/nkild UserI	

Рисунок 9.6 – Добавление пользователя вручную

#### 9.2.3 Управление настройками входа

Для доменного пользователя возможно установить тип аутентификации пользователя при входе в OC:

- доверять аутентификации домена;
- вход с использованием смарт-карты;
- вход с использованием смарт-карты с дополнительной проверкой сертификата.

Для пользователя SafeNode возможно установить тип аутентификации пользователя при входе в ОС:

- вход с использованием смарт-карты.
  - При добавлении в раздел политики SafeNode System Loader «Управление аутентификацией» локального пользователя SafeNode System Loader и назначении ему типа аутентификации Вход с использованием смарт-карты необходимо после применения политики выполнить перезагрузку рабочей станции для корректной аутентификации пользователя.

Аутентификация по паролю для доменных пользователей и пользователей SafeNode задается в настройках клиентской рабочей станции. Подробное описание настройки приведено в разделе *«Проверка пароля в SafeNode»*. Для входа доменных пользователей и пользователей SafeNode по паролю необходимо добавить пользователей в список раздела политики *«Управление аутентификацией»* без дополнительных настроек аутентификации.

Тип аутентификации **Доверять аутентификации домена** предполагает проверку идентификационных данных пользователя средствами домена, СДЗ «SafeNode

#### 72410666.00063-04 95 01-01



System Loader» не осуществляет проверку вводимых данных (пароль, сертификат) учетной записи пользователя, выполняющего вход. Аутентификация будет проводиться в любом домене в соответствии с настройками сетевого адаптера UEFI и конфигурационных файлов krb5 и ldap (см. разделы *Настройки сети* и *Сетевой адаптер UEFI*). При установке данного типа аутентификации, для пользователя возможен любой вид входа, предусмотренный средствами ОС (вход по паролю, по сертификату на токене или по паролю на токене).

Тип аутентификации **Вход с использованием смарт-карты** предполагает аутентификацию пользователя с использованием токена. При входе пользователя идентификационные данные пользователя проверяются средствами домена, СДЗ «SafeNode System Loader» осуществляет проверку в своей базе наличия учетной записи пользователя, выполняющего вход, и наличие привязанного к данной учетной записи токена, и после успешности проверки допускает пользователя до входа в систему. Если пользователь вводит корректные идентификационные данные из домена, но его нет в базе данных СДЗ, ему будет отказано в аутентификации.

При выборе типа аутентификации «**Вход с использованием смарт-карты**» с установленным флагом **«Дополнительная проверка сертификата**» при входе доменного пользователя или пользователя SafeNode System Loader выполняется дополнительная проверка в базе данных СДЗ привязки сертификата на токене к пользователю, который его предъявляет. При первой успешной аутентификации пользователя, если пользователь есть в базе данных, но к нему не привязан сертификат, сертификат добавляется в базу данных.

Во вкладке **Дополнительные настройки** (рисунок 9.7) администратор при необходимости может установить дополнительные настройки для пользователей, добавленных в список механизма управления аутентификацией, установив соответствующие флаги:

Включить механизм «Проверка пароля в SafeNode» на клиентских компьютерах – возможность настраивать вход пользователя по паролю в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Проверка пароля в SafeNode»);

– Включить механизм «Пользователи с разрешением на вход в ОС» на клиентских компьютерах – возможность разрешать вход на клиентскую рабочую станцию только пользователям из списка, заданного в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе «Пользователи с разрешением на вход в ОС»).



🔀 Изменение политики модуля SafeNode System Loader: Политика SafeNode System Loader по умолчанию X				
Общее	Управление аутентификацией пользователей 🗅			
Настройка входа				
Управление аутентификацией	Список пользователей 🗂 Дополнительные настройки			
Сложность пароля				
Контроль целостности	Механизм «Пользователи с разрешением на вход в ОС" на клиентских компьютерах ③ ြ			
Настройки подключения к домену				
Сетевой адаптер UEFI				
🔵 Мягкий режим 🛈 占				
	Ок Отмена Применить	]		

Рисунок 9.7 – Дополнительные настройки для пользователей

## 9.3 Сложность пароля

Раздел политики SafeNode System Loader **«Сложность пароля»** предназначен для управления ограничениями при задании пароля пользователя и администратора для входа на клиентские рабочие станции при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader».

Настройка ограничений при задании пароля пользователя и администратора при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader» заключается в установке требований к паролю пользователя/администратора, блокировке при неудачных попытках авторизации в ОС и установке запрета на использование заданного количества последних паролей. Описание настраиваемых параметров приведено в таблице 9.2.

Наименование	Описание	Возможные	По
параметра		значения	умолчанию
Пароль пользователя			
Минимальное количество	Требования к минимальной длине пароля	от 8 до 32	10
символов		символов	символов

Таблица 9.2 – Параметры политики аутентификации пользователей/администраторов

165

Наименование параметра	Описание	Возможные значения	По умолчанию
Контроль сложности пароля	Требования к сложности пароля. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Срок действия пароля (дней)	Требования к максимальному времени действия пароля пользователя	от 1 до 45 дней	40 дня
Минимальное число уникальных символов	Требования к изменению состава при создании нового пароля пользователя	от 4 до 16	5 символ
Пароль администратора	1		
Минимальное количество символов	Требования к минимальной длине пароля	от 8 до 32 символов	10 символов
Контроль сложности пароля	Требования к сложности пароля. Пароль должен содержать буквы верхнего и нижнего регистра, цифры и спецсимволы		
Срок действия пароля (дней)	Требования к максимальному времени действия пароля	от 1 до 45 дней	40 дня
Минимальное число уникальных символов	Требования к изменению состава при создании нового пароля	от 4 до 16	5 символ
Дополнительные настро	<b>ОЙКИ</b>		
Количество попыток ввода	Значение максимального количества неудачных попыток входа пользователя в ОС до его автоматической блокировки	от 1 до 8 попыток	5 попытки
Блокировать при неудачной попытке входа (мин)	Время (в минутах) блокировки возможности входа пользователя в ОС рабочей станции после превышения им максимального количества неудачных попыток входа в ОС	от 1 до 60 минут	15 минут
Запретить использование последних паролей	Запрет на использование предыдущих PIN- кодов пользователя	от 1 до 100 паролей	10 паролей

Для настройки ограничений при задании пароля пользователя и администратора при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader» перейдите в раздел политики **«Сложность паролей»** в режиме изменения политики SafeNode System Loader на сервере или в группе рабочих станций и установите требующиеся параметры и их значения (рисунок 9.8).

Для принудительного наследования установленных параметров аутентификации всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке параметра.

#### 72410666.00063-04 95 01-01



X Изменение политики модуля	SafeNode System Loader: Политика SafeNode System	Loader по умо	лчанию		×
Общее	Пароль пользователя				
Настройка входа	Иинимальное количество символов	10	6		
Управление аутентификацией	🗹 Контроль сложности пароля:		6		
Сложность пароля	Спецсимволы				
Пароль пользователя	<ul> <li>цифры</li> <li>Заглавные буквы</li> </ul>				
Пароль администратора	🗸 Строчные буквы				
Дополнительно	Срок действия пароля (дней)	40	6		
Контроль целостности	Иинимальное число уникальных символов	5	6		
Настройки подключения					
к домену					
Сетевой адаптер UEFI					
🕥 Мягкий режим 🛈 占					
			Ок	Отмена	Применить

Рисунок 9.8 – Настройка параметров аутентификации

## 9.4 Контроль целостности

Раздел политики SafeNode System Loader **«Контроль целостности»** предназначен для слежения за неизменностью поставленных на КЦ объектов аппаратной и программной конфигурации рабочих станций с целью обнаружения модификации ресурсов системы до загрузки ОС.

При настройке механизма КЦ администратор может задать контроль целостности следующих компонентов контролируемой рабочей станции:

- контроль целостности файловой системы – КЦ файлов и (или) каталогов загружаемой ОС, а также файлов и (или) каталогов пользователя;

контроль реестра – КЦ объектов реестра ОС семейства Windows;

- *контроль целостности загрузочных секторов* – КЦ загрузочных секторов устройств хранения данных;

– *контроль параметров UEFI* – КЦ переменных, драйверов и таблиц среды UEFI;

167

- **контроль изменения аппаратной среды** – контроль аппаратных устройств (аппаратной конфигурации) ЭВМ;

 установка алгоритма расчета контрольных сумм объектов, установленных на контроль целостности.

При нарушении целостности компонентов, установленных на контроль, в журнале аудита фиксируется событие о выявленном нарушении.

## 9.4.1 Контроль целостности файловой системы

Вкладка *Контроль целостности файловой системы* предназначена для формирования списка файлов/каталогов ОС для постановки на КЦ. Формирование списка файлов/каталогов, целостность которых имеет критическое значение для безопасного функционирования операционных систем осуществляется для каждого семейства ОС Windows/Linux в соответствующих вкладках.

При постановке файла/каталога на КЦ СЗИ рассчитывает хеш функцию файла/каталога по заданному алгоритму (см. раздел *Алгоритм расчета контрольных сумм*) и при последующем старте загрузки UEFI сравнивает сохраненный хеш с текущим, рассчитанным на момент проверки.

Для постановки файлов на КЦ перейдите в раздел политики SafeNode System Loader «Контроль целостности» во вкладку *Контроль целостности файловой системы* в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.9).



169

🗙 Изменение политики модуля	SafeNode System Loader: Политика SafeNode System Loader по умолчанию		×
Общее	Контроль целостности файловой системы 🗅		
Настройка входа	Механизм контроля файлов выключен П		
Управление аутентификацией			
Сложность пароля			
Контроль целостности	C TIOUCK	_	
Файловая система	Э Добавить Пудалить	) Рекомендованные файлы	🛃 Импорт 👌 Экспорт
Реестр	Путь к файлу/каталогу C:\Windows\explorer.exe		*
Загрузочные сектора	C:\Windows\System32\drivers\netbt.sys		
UEFI			
Аппаратная среда			
Другие параметры			
Настройки подключения к домену			
Сетевой адаптер UEFI			
О Мягкий режим ①	Bcero: 2		
		Ок Отмена	Применить

Рисунок 9.9 – Постановка файлов на КЦ

Включите механизм КЦ файлов, установив переключатель в положение <sup>(Механизм контроля файлов включен</sup> (рисунок 9.9), и сформируйте перечень файлов ОС семейства Windows и Linux для постановки на КЦ.

Сформировать список файлов для постановки на КЦ возможно вручную по кнопке <sup>•</sup> <sup>Добавить</sup>, с последующим вводом полного пути к файлу (рисунок 9.10), а также в автоматическом режиме, добавлением перечня файлов ОС Windows/Linux, рекомендуемых к установке на КЦ, из сформированного списка по кнопке <sup>•</sup> <sup>Рекомендованные файлы</sup> (рисунок 9.11).



🔀 Изменение политики модуля	SafeNode System Loader: Политика SafeNode System Loader по умолчанию			×
Общее	Контроль целостности файловой системы 🗅			
Настройка входа				
Управление аутентификацией	Механизм контроля файлов включен			
Сложность пароля	Файлы Windows ြ Файлы Linux ြ			
Контроль целостности	Q. Поиск			
Файловая система	🕀 Добавить 🖉 Изменить 🔟 Удалить	🗟 Рекомендованные файлы	🛓 Импорт	之 Экспорт
Реестр	Путь к файлу/каталогу			*
	Введите полный путь к файлу и его расширение			
Загрузочные сектора	C:\Windows\explorer.exe			
UEFI	C:\Windows\System32\drivers\netbt.sys			

## Рисунок 9.10 – Добавление файлов на КЦ вручную

🗙 Изменение политики модуля S	afeNode System Loader: Политика SafeNode System Load	er по умолчанию			$\times$
Общее	Контроль целостности файловой с	истемы 🗗			
Настройка входа	_				
Управление аутентификацией	Механизм контроля файлов включен				
Сложность пароля	Файлы Windows 🖒 Файлы Linux 🖒				
Контроль целостности	Q. Поиск				
Файловая система	Эдобавить Лименить Удалить	🖗 Рекомен	ідованные фа	йлы 🛓 Импорт 👌 Экс	:порт
Реестр	Путь к файлу/каталогу Х Импорт путей к файлам	I			×
Загрузочные сектора	C:\Windows\explorer. ← → ∨ ↑ □ « Lo C:\Windows\System3	cal > Temp.kvrkVB	ī 5 ∨	Поиск в: Temp.kvrkVB	Q
UEFI	Упорядочить 🔻 Нова	я папка			2
Аппаратная среда	🖈 Быстрый доступ	Имя I Windows		Дата изменения 21.06.2023 16:54	Тип Текст
Другие параметры	🖊 Загрузки 🖈				
Настройки подключения к домену	🔮 Документы 🖈 📰 Изображени 🖈				
Сетевой адаптер UEFI		<			:
	Имя	файла:	~ [	*.txt	~
🔵 Мягкий режим 🛈 占	Bcero: 2			Открыть Отме	на
		Ок	Отме	ена Применит	ъ

Рисунок 9.11 – Добавление файлов на КЦ из ранее сформированного списка

По кнопкам 坐 Импорт / 🖄 Экспорт доступен импорт/экспорт списка файлов для постановки на КЦ.

При каждом изменении с сохранением политики КЦ файлов происходит пересчет всех контрольных сумм файлов из списка на всех подконтрольных рабочих станциях. В

случае нарушения целостности файлов, установленных на КЦ, формируется событие аудита о нарушении КЦ файлов.

Для принудительного наследования установленных параметров механизма КЦ файлов всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке необходимого файла, на всем списке файлов Windows/Linux или на всем разделе *Контроль целостности файловой системы*.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте *«Удаление пользователей или групп пользователей»*.

#### 9.4.2 Контроль реестра

Вкладка *Контроль реестра* предназначена для формирования списка объектов реестра, целостность которых имеет критическое значение для безопасного функционирования ОС Windows, для постановки на КЦ.

При постановке объектов реестра на КЦ СЗИ рассчитывает хеш функцию объекта реестра по заданному алгоритму (см. раздел *Алгоритм расчета контрольных сумм*) и при последующем старте загрузки UEFI сравнивает сохраненный хеш с текущим, рассчитанным на момент проверки.

Для постановки объектов реестра на КЦ перейдите в раздел политики SafeNode System Loader **«Контроль целостности»** во вкладку *Контроль реестра* в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.12).



172

🗙 Изменение политики модуля S	SafeNode System Loader: Политика SafeNode System Loader по умолчанию				×
Общее	Контроль реестра 🗗				
Настройка входа					
Управление аутентификацией	Механизм контроля реестра включен — "				
Сложность пароля	Q. Поиск				
Контроль целостности	🕀 Добавить 🖉 Изменить 🗑 Удалить	🕃 Рекоменд	ованные ключи	🛓 Импорт	之 Экспорт
Файловая система	Ключи реестра				*
Реестр	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio	on\Uninstall			
Загрузочные сектора					
UEFI					
Аппаратная среда					
Другие параметры					
Настройки подключения к домену					
Сетевой адаптер UEFI					
🔵 Мягкий режим 🛈 占	Bcero: 1				
		Ок	Отмена	При	именить

Рисунок 9.12 – Постановка объектов реестра на контроль

Включите механизм контроля реестра, установив переключатель в положение Механизм контроля реестра включен (рисунок 9.12), и сформируйте объектов реестра для постановки на КЦ.

Сформировать список объектов реестра для постановки на КЦ возможно вручную по кнопке <sup>Э Добавить</sup>, выбрав значение из предустановленного списка или выбрав произвольное значение с последующим вводом пути к объекту реестра (рисунок 9.13).

Сформировать список объектов реестра в автоматическом режиме возможно добавлением перечня объектов реестра, рекомендуемых к установке на КЦ, из сформированного списка по кнопке Рекомендованные ключи (рисунок 9.14).



🗙 Изменение политики модуля S	afeNode System Loader: Политика SafeNode System Loader по умолчанию	×			
Общее	Контроль реестра 🗅				
Настройка входа					
Управление аутентификацией	Механизм контроля реестра включен				
Сложность пароля	Q. Поиск				
Контроль целостности	Э Добавить Изменить В Удалить	чи 🖄 Импорт 👌 Экспорт			
Файловая система	KING	*			
Реестр	HKEY_CURRENT_USER\ HKEY UKEY_LOCAL_MACURUP				
	HKEY_LUCAL_MACHINE\				
Загрузочные сектора	HKEY_USERS\				
UEFI	HKEY_CURRENT_CONFIG\				

## Рисунок 9.13 – Добавление объектов реестра вручную

🗙 Изменение политики модуля S	SafeNode System Loader: Политика SafeNode System Loader по умолчанию Х
Общее	Контроль реестра 🗗
Настройка входа	
Управление аутентификацией	Механизм контроля реестра включен
Сложность пароля	Q, Поиск
Контроль целостности	🟵 Добавить 🕹 Импорт 👌 Экспорт
Файловая система	Х Импорт ключей реестра Х
Реестр	← → · ↑  · Cocal > Temp.mcRKYU · Č Поиск в: Temp.mcRKYU
Загрузочные сектора	Упорядочить т Новая папка
UEFI	Имя Дата изменения Тип Вабоций сто сто Спортного Спо
Аппаратная среда	↓ Загрузки *
Другие параметры	🔮 Документы 🖈
Настройки подключения к домену	OneDrive
Сетевой адаптер UEFI	Зтат калия натая У К > Имя файла: *.txt
🕥 Мягкий режим 🛈 占	Открыть Отмена
	Ок Отмена Применить

Рисунок 9.14 – Добавление объектов реестра из ранее сформированного списка

По кнопкам 坐 Импорт / 🖄 Экспорт доступен импорт/экспорт списка объектов реестра для постановки на КЦ.

При каждом изменении с сохранением политики контроля реестра происходит пересчет всех контрольных сумм объектов реестра из списка на всех подконтрольных

рабочих станциях. В случае нарушения целостности объектов реестра, установленных на КЦ, формируется событие аудита о нарушении контроля реестра.

Для принудительного наследования установленных параметров механизма КЦ реестра всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке необходимого объекта реестра или на всем разделе *Контроль реестра*.

Удаление списочных элементов возможно только из текущей политики или из текущей и из всех политик, являющихся дочерними по отношению к текущей. Подробно логика удаления списочных элементов описана в пункте **«Удаление пользователей или** групп пользователей».

#### 9.4.3 Контроль целостности загрузочных секторов

Вкладка *Контроль целостности загрузочных секторов* предназначена для постановки на КЦ всех найденных загрузочных секторов на всех подконтрольных рабочих станциях.

При постановке загрузочных секторов на КЦ СЗИ рассчитывает хеш загрузочных секторов по заданному алгоритму (см. раздел *Алгоритм расчета контрольных сумм*) и при последующем старте загрузки UEFI сравнивает сохраненный хеш с текущим, рассчитанным на момент проверки.

Для постановки загрузочных секторов на КЦ перейдите в раздел политики SafeNode System Loader **«Контроль целостности»** во вкладку *Контроль целостности загрузочных секторов* в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.15) и включите механизм КЦ загрузочных секторов, установив переключатель в положение *Контроль целостности загрузочных секторов включен* (рисунок 9.15).



🗙 Изменение политики модуля S	afeNode System Loader: Политика SafeNode System Loader по умолчанию		×
Общее	Контроль целостности загрузочных секторов 🕒		
Настройка входа	Контроль целостности загрузочных секторов включен		
Управление аутентификацией			
Сложность пароля			
Контроль целостности			
Файловая система			
Реестр			
Загрузочные сектора			
UEFI			
Аппаратная среда			
Другие параметры			
Настройки подключения к домену			
Сетевой адаптер UEFI			
🔲 Мягкий режим 🛈 占			
	Οκ	Отмена	Применить

Рисунок 9.15 – Постановка на КЦ загрузочных секторов

При каждом сохранении политики КЦ загрузочных секторов происходит пересчет всех контрольных сумм загрузочных секторов на всех подконтрольных рабочих станциях. В случае нарушения целостности загрузочных секторов, установленных на КЦ, формируется событие аудита о нарушении КЦ загрузочных секторов.

Для принудительного наследования установленных параметров механизма КЦ загрузочных секторов всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе *Контроль реестра*.

## 9.4.4 Контроль целостности UEFI

Вкладка *Контроль целостности UEFI* предназначена для формирования списка переменных, драйверов и системных таблиц среды UEFI для постановки на КЦ.

При постановке объектов среды UEFI на КЦ СЗИ рассчитывает хеш функцию объектов по заданному алгоритму (см. раздел *Алгоритм расчета контрольных сумм*) и при последующем старте загрузки UEFI сравнивает сохраненный хеш с текущим, рассчитанным на момент проверки.

Для постановки объектов среды UEFI на КЦ перейдите в раздел политики SafeNode System Loader «Контроль целостности» во вкладку Контроль целостности UEFI

## 72410666.00063-04 95 01-01

175



в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.16).



Рисунок 9.16 – Постановка объектов среды UEFI на КЦ

Включите механизм КЦ UEFI, установив переключатель в положение Контроль UEFI включен (рисунок 9.16), и сформируйте перечень переменных, драйверов и системных таблиц среды UEFI для постановки на КЦ.



🗙 Изменение политики модуля	SafeNode System Loader:	Политика SafeNode System Loader по умолчанию	×
Общее	Контроль цел	остности UEFI 🕒	
Настройка входа	C Контроль UEFI в	ыключен 🗅	
Управление аутентификацией			
Сложность пароля	Контролируе		X
Контроль целостности	Q Поиск		
Файловая система	Э Добавить	выоерите неооходимые объекты и нажмите на кнопку. Дооавить	рт 👌 Экспорт
Реестр	Имя объекта	<ul> <li>Переменные UEFI – 2</li> </ul>	
Загрузочные сектора	<ul> <li>Переменные UEF</li> </ul>	▼ 🔽 🗀 605DAB50-E046-4300-ABB6-3DD810DD8B23	
UEFI	• 🗋 605DAB50	MokList	
Аппаратная среда	MokList	81C76078-BFDE-4368-9790-570914C01A65	
	▼ D719B2CI	SetUpdateCountVar	
Другие параметры	db	9CB2E73F-7325-40F4-A484-659BB344C3CD	
Настройки подключения к домену		SOFTWAREGUARDSTATUS	
0X UEE		▼ 🗖 🗋 D719B2CB-3D3A-4596-A3BC-DAD00E67656F	
Сетевой адаптер Осгі		Всего: 49 Выбрано: 2	
🔲 Мягкий режим 🛈 占	Bcero: 2	Добавить Отмена	
		Ок Отмена	Применить

Рисунок 9.17 – Добавление объектов среды UEFI на КЦ

По кнопкам 坐 Импорт / 🖄 Экспорт доступен импорт/экспорт списка объектов среды UEFI для постановки на КЦ.

При каждом изменении с сохранением политики КЦ UEFI происходит пересчет всех контрольных сумм объектов из списка на всех подконтрольных рабочих станциях. В случае нарушения целостности объектов, установленных на КЦ, формируется событие аудита о нарушении КЦ UEFI.

Для принудительного наследования установленных параметров механизма КЦ UEFI всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем списке контролируемых объектов или на всем разделе *Контроль целостности UEFI*.

## 9.4.5 Контроль изменения аппаратной среды

Вкладка *Контроль изменения аппаратной среды* предназначена для постановки на КЦ выборочных аппаратных устройств рабочей станции.

При постановке аппаратных устройств на КЦ СЗИ рассчитывает хеш функцию устройства по заданному алгоритму (см. раздел **Алгоритм расчета контрольных** *сумм*) и при последующем старте загрузки UEFI сравнивает сохраненный хеш с



текущим, рассчитанным на момент проверки.

Для постановки аппаратных устройств на КЦ перейдите в раздел политики SafeNode System Loader **«Контроль целостности»** во вкладку *Контроль изменения аппаратной среды* в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.18).

X Изменение политики модуля S	SafeNode System Loader: Политика SafeNode System Loader по умолчанию	×
Общее	Контроль изменения аппаратной среды 🕒	
Настройка входа	Механизм контроля изменения аппаратной среды включен	
Управление аутентификацией	🗌 Процессоры 🔓	
Сложность пароля	Оперативная память (ОЗУ)	
Контроль целостности		
Файловая система	USB-устройства 🗗	
Реестр		
Загрузочные сектора		
UEFI		
Аппаратная среда		
Другие параметры		
Настройки подключения к домену		
Сетевой адаптер UEFI		
🕥 Мягкий режим 🛈 占		
	Ок Отмена Примени	гь

Рисунок 9.18 – Постановка аппаратных устройств на КЦ

Включите механизм КЦ аппаратных устройств, установив переключатель в положение Механизм контроля изменения аппаратной среды включен (рисунок 9.18), и установите на КЦ требующиеся устройства из списка.

При каждом изменении с сохранением политики КЦ аппаратных устройств происходит пересчет всех контрольных сумм выбранных устройств из списка на всех подконтрольных рабочих станциях. В случае нарушения целостности аппаратных устройств, установленных на КЦ, формируется событие аудита о нарушении КЦ аппаратных устройств.

Для принудительного наследования установленных параметров механизма КЦ аппаратных устройств всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке необходимого устройства или на всем разделе *Контроль изменения аппаратной среды*.

#### 72410666.00063-04 95 01-01

#### 9.4.6 Алгоритм расчета контрольных сумм

Вкладка **Алгоритм расчета контрольных сумм** предназначена для установки алгоритма хеширования по которому будет выполнятся расчет контрольных сумм объектов, поставленных на контроль целостности.

Для выбора алгоритма хеширования перейдите в раздел политики SafeNode System Loader **«Контроль целостности»** во вкладку *Алгоритм расчета контрольных сумм* в режиме изменения политики на сервере или в группе рабочих станций (рисунок 9.19).

🗙 Изменение политики модуля	SafeNode System Loader: Поли	тика SafeNode System Loader по умо	олчанию		×
Общее	Алгоритм расчета	а контрольных сумм			
Настройка входа	Алгоритм хеширования	SHA-1	• d'		
Управление аутентификацией	Реакция на нарушение	Запись в журнал аудита	ď		
Сложность пароля					
Контроль целостности					
Файловая система					
Реестр					
Загрузочные сектора					
UEFI					
Аппаратная среда					
Другие параметры					
Настройки подключения к домену					
Сетевой адаптер UEFI					
🕥 Мягкий режим 🛈 占					
			Ок	Отмена	Применить

#### Рисунок 9.19 – Вкладка Алгоритм расчета контрольных сумм

Выберите из списка требующийся алгоритм хеширования по которому будет выполнятся расчет контрольных сумм объектов, поставленных на КЦ (рисунок 9.20).

СТЭ сервис		Руководство администратора Управление политиками	безопасности. Часть 1	180
🗙 Изменение политики модуля	a SafeNode System Loader: Полит	ика SafeNode System Loader по умолчанию		×
Общее	Алгоритм расчета	контрольных сумм		
Настройка входа	Алгоритм хеширования	SHA-1	6	
Управление аутентификацией	Реакция на нарушение	SHA-1	6	
	·	SHA-256		
Сложность пароля		SHA-512		
Контроль целостности				

СЗИ от НСЛ «Блокхост-Сеть 4»

Рисунок 9.20 – Выбор алгоритма хеширования

При постановке на КЦ хеш объекта, установленного на КЦ, рассчитывается по заданному алгоритму и при последующем старте загрузки UEFI сохраненный хеш сравнивается с текущим, рассчитанным на момент проверки.

Для принудительного наследования выбранного алгоритма хеширования всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» в строке алгоритма хеширования.

## 9.5 Настройки подключения к домену

ГАЗИНФОРМ

Раздел политики SafeNode System Loader **«Настройки подключения к домену»** предназначен для настройки параметров сервера LDAP через файлы конфигураций hosts, krb5.conf и ldap.conf для аутентификации пользователей, зарегистрированных на сервере LDAP, для входа на клиентские рабочие станции при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader».

При включении аутентификации LDAP (подробное описание включения аутентификации LDAP описано в разделе **Управление аутентификацией** политики SafeNode System Loader) устанавливается полное доверие домену.

Настройка параметров сервера LDAP через файлы конфигураций hosts, krb5.conf и ldap.conf возможна:

– с помощью создания файлов конфигураций hosts, krb5.conf и ldap.conf вручную;

с помощью автоматической генерации базовой настройки файлов конфигураций hosts, krb5.conf и ldap.conf.

Для настройки параметров сервера LDAP перейдите в раздел политики SafeNode System Loader **«Настройки подключения к домену»** в режиме изменения политики на сервере или в группе рабочих станций и включите механизм настройки сети, установив переключатель в положение <sup>Механизм включен</sup> (рисунок 9.21).


181

X Изменение политики модуля 9	SafeNode Syste	m Loader: Полит	тика Sa	feNode System Loader по у	молча	анию			×
Общее	Настро	йки подклн	ючен	ния к домену 🗗					
Настройка входа	C Me	канизм включен	• 6						
Управление аутентификацией	↓ Задать	значения по ум	ючанин	ю					
Сложность пароля	krb5.conf	ldap.conf	hosts	Корневые сертификаты			¥	Импорт	之 Экспорт
Контроль целостности									
Настройки подключения к домену									
Сетевой адаптер UEFI									
🕥 Мягкий режим 🛈 占									
						Οκ	Отмена	При	іменить

Рисунок 9.21 – Настройка сети для аутентификации LDAP

Для создания файлов конфигураций hosts, krb5.conf и ldap.conf вручную перейдите в соответствующие вкладки с наименованием файлов конфигураций, введите в текстовой области необходимые настройки и нажмите **Применить** (рисунок 9.22).



🗙 Изменение политики модуля	SafeNode System Loader: Политика SafeNode System Loader по умолчанию		×
Общее	Настройки подключения к домену 🕒		
Настройка входа	С Механизм включен		
Управление аутентификацией	Л Задать значения по умочанию		
Сложность пароля	krb5.conf Idap.conf hosts Корневые сертификаты	🛓 Импорт	Экспорт
Контроль целостности	[libdefaults]		
Настройки подключения к домену	default_realm = ERER		
Сетевой адаптер UEFI	<pre># The following krb5.conf variables are only for MIT Kerberos. kdc_timesync = 1 ccache_type = 4 forwardable = true proxiable = true fcc-mit-ticketflags = true pkinit_anchors = FILE:/EFI/GIS/DB/root.cer pkinit_eku_checking = kpServerAuth pkinit_kdc_hostname = ERER.ERER pkinit_identities = PKCS11:/ [realms] ERER = { kdc = erer.erer admin_server = erer.erer default_domain = ERER kpasswd_server = erer.erer } }</pre>		
🔵 Мягкий режим 🛈 占	[domain_realm] erer = FRFR		
	Ок Отмена	При	именить

Рисунок 9.22 – Формирование файлов конфигураций вручную

Для формирования базовой настройки файлов конфигураций hosts, krb5.conf и ldap.conf с помощью автоматической генерации нажмите на кнопку Задать значения по умолчанию, в появившемся окне (рисунок 9.23) введите DNS-имя контроллера домена, наименование домена и его IP-адрес в соответствующие поля и нажмите кнопку **Применить**.

182



💢 Задание значения по умолчанию	×
Основной контроллер домена (KDC)	
s09dc.pki.local	
Домен (default_realm)	
pki.local	
IP-адрес контроллера домена	
10 .72 .9 . 2	
Вход по сертификату	
Применить	Отмена

Рисунок 9.23 – Ввод DNS-имени контроллера домена и наименования домена

В результате в текстовой области отобразятся базовые настройки файлов конфигураций hosts, krb5.conf и ldap.conf (рисунок 9.24).

🗙 Изменение политики модуля S	afeNode System Loader: Политика SafeNode System Loader по умолчанию	×
Общее	Настройки подключения к домену	
Настройка входа	Механизм включен — — — — — — — — — — — — — — — — — — —	
Управление аутентификацией		
Сложность пароля	krb5.conf Idap.conf hosts Корневые сертификаты	🖞 Импорт 👌 Экспорт
Контроль целостности	#	
Настройки подключения к домену	# LDAP Defaults #	
Сетевой адаптер UEFI	BASE dc=erer URI Idaps://erer.erer #SIZELIMIT 12 #TIMELIMIT 15 #DEREF never # TLS certificates (needed for GnuTLS) TLS_REQCERT never #TLS_CACERT /etc/ssl/certs/ca-certificates.crt	
🕥 Мягкий режим 🛈 占		
	Ок Отмена	Применить

Рисунок 9.24 – Формирование файлов конфигураций автоматически

По кнопкам <sup>ч</sup> Импорт</sup> / <sup>зкспорт</sup> доступен импорт/экспорт файлов конфигураций hosts, krb5.conf и ldap.conf.

Если при аутентификации пользователей, зарегистрированных на сервере LDAP, для входа на клиентские рабочие станции при прохождении дополнительной аутентификации с помощью СДЗ «SafeNode System Loader» будет использоваться сертификат, записанный на токен, необходимо включить возможность входа по сертификату в окне задания значений по умолчанию (рисунок 9.25).

🔀 Задание значения по умолчанию	×
Основной контроллер домена (KDC)	
s09dc.pki.local	
Домен (default_realm)	
pki.local	
IP-адрес контроллера домена	
10.72.9.2	
<ul> <li>Вход по сертификату</li> <li>Корневые сертификаты</li> <li>Добавить</li> </ul>	
Применить Отмена	

Рисунок 9.25 – Добавление возможности входа по сертификату

- Необходимо учитывать, что корневой сертификат ЦС нужно предварительно скопировать с центра сертификации и перенести на сервер Блокхост-Сеть:
  - корневой сертификат ЦС MS CA располагается в оснастке certmgr.msc
     в Trusted Root Certification Authorities (перед копированием необходимо выполнить экспорт сертификата в формате Base64);
  - корневой сертификат ЦС DogTag располагается в каталоге, куда были сгенерированы сертификаты центра сертификации и подчиненных центров сертификации (при их наличии).

По кнопке <sup>• Добавить</sup> (рисунок 9.26) указать путь к необходимому корневому сертификату используемого центра сертификации.

💢 Выбор серитификата			×
← → ∽  🗔 > Эт	от компьютер » Рабочий стол »	✓ О Поиск в: Р	абочий стол 🔎
Упорядочить 🔻 Нова	ая папка		::: • 🔟 ?
🖈 Быстрый доступ	Имя	Дата изменения	Тип Раз
Пабочий стол 🖈	blockhost_client_4.3.35263.8684_astralinux_1.6_x64 Token Driver	23.05.2023 10:56 15.03.2022 15:16	Папка с файлами Папка с файлами
Загрузки Я Документы Я	📮 root_cert	21.06.2023 16:29	Сертификат безо
🔚 Изображения 🖈			
loneDrive			
💻 Этот компьютер			
💣 Сеть			
	٢		>
Имя	файла: root_cert	<ul> <li>✓ Файлы се</li> <li><u>О</u>ткры</li> </ul>	ртификатов (*.cer *.c ∨ ть Отмена

Рисунок 9.26 – Выбор корневого сертификата ЦС

Нажать Применить (рисунок 9.27).

🔀 Задание значения по умолчанию	×				
Основной контроллер домена (KDC)					
s09dc.pki.local					
Домен (default_realm)					
pki.local					
IP-адрес контроллера домена					
10.72.9.2					
<ul> <li>Вход по сертификату</li> <li>Корневые сертификаты <ul> <li>Ф</li> <li>Добавить root_cert.cer</li> <li>Г</li> </ul> </li></ul>					
Применить	Отмена				

Рисунок 9.27 – Добавление корневого сертификата ЦС

Во вкладке *Корневые сертификаты* (рисунок 9.28) появится добавленный 72410666.00063-04 95 01-01



сертификат. Аутентификация пользователей, зарегистрированных на сервере LDAP, будет возможна с использованием сертификата на токене.

🗙 Изменение политики модуля SafeNode System Loader: Политика SafeNode System Loader по умолчанию								
Общее	Настройки подключения к домену 🕒							
Настройка входа	С Механизм включен							
Управление аутентификацией	Л Задать значения по умочанию							
Сложность пароля	krb5.conf Idap.conf hosts Kope	невые сертификат	ы					
Контроль целостности	+							
Настройки подключения к домену	Издатель	Кому выдан	Серийный номер	Хэш				
Сетевой адаптер UEFI	/DC=local/DC=pki/CN=pki-S09DC-CA	pki-S09DC-CA	12AEA74B2B3C779643F1236492FC83F8	MIIDYTCCAkmgAwIB				

Рисунок 9.28 – Отображение корневого сертификата ЦС

Для принудительного наследования установленных параметров механизма настроек сети всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе *Настройка сети*.

# 9.6 Сетевой адаптер UEFI

Раздел политики SafeNode System Loader **«Сетевой адаптер UEFI»** предназначен выбора способа получения сетевых настроек (статически или динамически) на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» для взаимодействия клиента и сервера LDAP.

Для выбора способа получения сетевых настроек на клиентских рабочих станциях перейдите в раздел политики **«Сетевой адаптер UEFI»** в режиме изменения политики SafeNode System Loader на сервере или в группе рабочих станций и установите

переключатель в положение 🥌 Механизм включен (рисунок 9.29).

Получение сетевых настроек на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» доступно:

– динамически **Получать IP-адрес автоматически** (IP-адрес, маска подсети и шлюз будут заполнены автоматически);

 статически Статический IP-адрес (IP-адрес, маску подсети и шлюз необходимо задать вручную в настройках клиентской рабочей станции (подробное описание настройки приведено в разделе Сетевой адаптер UEFI).

Для принудительного наследования установленных параметров всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на всем разделе *Сетевой адаптер UEFI*.



🗙 Изменение политики модуля S	SafeNode System Loader: Политика SafeNode System Loader по умолчанию	×
Общее	Сетевой адаптер UEFI 🗠	
Настройка входа		
Управление аутентификацией	Механизм включен	
Сложность пароля	Получать IP-адрес автоматически	
Контроль целостности	Статический IP-адрес	_
Настройки подключения к домену	IP-адреса задаются в разделе "Настройки" (Сетевой адаптер UEFI) на клиентских рабочих станциях	
Сетевой адаптер UEFI		
🔵 Мягкий режим 🛈 占		
	Ок Отмена Применить	

Рисунок 9.29 – Выбор способа получения сетевых настроек

# 9.7 Мягкий режим работы СДЗ «SafeNode System Loader»

Мягкий режим работы используется для первичной настройки СДЗ «SafeNode System Loader», до начала эксплуатации, при этом СДЗ «SafeNode System Loader» работает в режиме установки. Данный механизм позволяет получить сведения для выявления ошибок в настройках и корректировки устанавливаемых в политике параметров.

Работа данного механизма заключается в разрешении доступа пользователей к ресурсам, запрещенным настройками СДЗ «SafeNode System Loader» с фиксацией всех запрещенных попыток доступа в журнале аудита. На основании этих событий, администратор безопасности выявляет ресурсы, которые необходимо добавить в список разрешенных для данного пользователя и на основе полученных данных выполняет корректировку настроек СДЗ «SafeNode System Loader».

Для установки мягкого режима работы в режиме изменения политики SafeNode System Loader на сервере или в группе рабочих станций перейдите в параметр «Мягкий режим» и установите параметр в состояние *Включен* (рисунок 9.30).

187



188

Х Изменение политики модуля SafeNode System Loader: Политика SafeNode System Loader по умолчанию X					
Общее	Имя и группа г	толитики			
Настройка входа	Наименование*	Политика SafeNode System Loader по у	молчанию		
Управление аутентификацией	Группа 🛈	🗀 Все компьютеры			
Сложность пароля					
Контроль целостности	Комментарий				
Настройки подключения к домену					
Сетевой адаптер UEFI					
💽 Мягкий режим 🛈 占					
			Ок	Отмена	Применить

Рисунок 9.30 – Мягкий режим работы SafeNode System Loader

Для принудительного наследования возможности использования мягкого режима работы всеми политиками, являющимися дочерними по отношению к текущей, установите «замок» на параметре **«Мягкий режим»**.

# 10 Настройки сервера

Настройки сервера предполагают управление параметрами работы серверов непосредственно на самих серверах, локально.

Настройки сервера задаются во вкладке *Настройки* (рисунок 10.1) при выборе в иерархии сервера.

Для локальной настройки на серверах доступны следующие параметры:

– **Резервные копии** – настройка параметров резервного копирования всех политик и настроек (за исключением локальных настроек клиентских рабочих станций) вручную или в автоматическом режиме.

– **Автоархивация событий** – настройка параметров автоархивации событий, собранных с клиентских рабочих станций и подчиненных серверов.

– *Кеш событий* – настройка параметров кеша событий для временного хранения событий подчиненных серверов/клиентских компьютеров.

 Построение иерархии серверов – настройка присоединения сервера в иерархию в качестве головного или подчиненного сервера.

– Экспорт событий в SIEM – настройка параметров экспорта событий в SIEM.

🗙 Бло	кхост-Сеть 4					_	×
ጽ	Менеджер иерархий						
к <sup>ф</sup> я	C. ú <b>3</b>	QC	🖬 W102 🗮 0	0 🖵 1 Онлайн 🖲			C
70	▼ 🐺 W102		Общее Поли	итики Настройки	Статистика События Лицензии		
	localhost		Резервные копии Автоархивация со Кеш событий Построение иера Экспорт событий	вера событий архии серверов ій в SIEM	Резервные копии Журнал Настройки С Поиск Создать копию ҈Восстановить		
E Contraction of the second se			Применить	Отмена	Резервные копии отсут	ствуют	

Рисунок 10.1 – Локальные настройки сервера

# 10.1 Резервные копии

Резервное копирование предназначено для создания вручную или в автоматическом режиме копии всех политик и настроек (за исключением локальных настроек клиентских рабочих станций) на выбранном сервере.

При выполнении резервного копирования сохраняются следующие данные:

 политики выбранного сервера, подчиненных серверов и клиентских рабочих станций;

- события аудита сервера, подчиненных серверов и клиентских рабочих станций;
- настройки сервера;
- информация об учтенных токенах и о принадлежности токенов пользователям;
- инсталляционные пакеты, задачи и агенты системы развертывания;
- иерархия групп и клиентов Блокхост-Сеть;

190

информация о лицензиях.

Во вкладке *Журнал* (рисунок 10.2) отображаются все резервные копии, сохраненные на выбранном в иерархии сервере:

- Имя наименование сохраненной резервной копии;
- Директория место сохранения резервной копии на сервере;
- Время время создание резервной копии;
- Размер размер резервной копии;

- *Статус* – отображение статуса выполнения процесса создания резервной копии.

🗙 Бло	кхост-Сеть 4			– 🗆 ×
å	Менеджер иерархий			
к <sup>†</sup> л		Q C	🗃 W102 🖹 0 🖵 1 Онлайн 🖲	C
6	• 🛱 W102		Общее Политики Настройки Статистика События Лицензии	
_	<ul> <li>Все компьютеры</li> <li>Iocalbact</li> </ul>		Настройки сервера Резервные копии	
٥			Резервные копии	
			Автоархивация событий	
			Кеш событий	
			Создать колино тросстановить Построение иерархии серверов Имя Директория Время Размер	Статус
			Экспорт событий в SIEM 🗐 2024-01-2 С:\Blockhost B 29.01.2024 16:4 250.9 M6	📀 Копия создана
Ē			Bcero: 1	
ţĝ			Применить Отмена	0

Рисунок 10.2 – Список резервных копий сервера

Во вкладке Настройки (рисунок 10.3) возможно:

 задать пароль по умолчанию, который будет использоваться при создании резервной копии вручную или автоматически в поле *Пароль по умолчанию*;

– задать директорию, в которую будут сохраняться резервные копии по умолчанию;

#### 72410666.00063-04 95 01-01



настроить автоматическое создание резервных копий;

 изменить параметры удаления резервных копий, установив максимальное количество дней, в течении которых хранится резервная копия, в параметре Удалять резервные копии старше, дней (по умолчанию срок хранения резервных копий ограничен 90 днями);

 изменить параметры отображения записей в списке резервных копий, установив необходимое значение в параметре *Максимальное количество* отображаемых записей в журнале (по умолчанию в журнале отображается 20 копий).

Автоматическое удаление резервной копии по истечению срока ее хранения, заданному в параметре Удалять резервные копии старше, дней, выполняется при очередном создании резервной копии вручную или автоматически.

🗙 Бло	окхост-Сеть 4		– 🗆 X
&	Менеджер иерархий		
кĴл		🎬 W102 🗮 0 🖵 1 Онлайн 🔍	c
ති	▼ 🛱 W102	Общее Политики Настройки	Статистика События Лицензии
10	• 🗅 Все компьютеры	Настройки сервера	Перераные колии
8	localhost	Резервные копии	
		Автоархивация событий	Журнал Настройки
		Кеш событий	Пароль по умолчанию
		Построение иерэруии серверов	
		постросние исрархии серверов	Перемещать резервные копии в
		Экспорт событий в SIEM	с:\biocknost backups
			Автоматическое создание резервных копий
			Удалять резервные копии старше, дней 90
			Иаксимальное количество отображаемых записей в журнале
E			
ţĝ		Применить Отмена	

Рисунок 10.3 – Настройка отображения списка резервных копий

Создание резервных копий доступно вручную во вкладке **Журнал** и в автоматическом режиме во вкладке **Настройки**.

## 10.1.1 Создание резервных копий вручную

Для создания резервной копии вручную во вкладке *Настройки* сервера перейдите в раздел «Резервные копии» (рисунок 10.2), во вкладку *Журнал* и нажмите на кнопку Создать копию

Выберите директорию, в которой будет сохранена резервная копия (рисунок 10.4) и нажмите на кнопку *Создать*.



Резервные копии сохраняются на выбранном <u>сервере</u>, вне зависимости от того, на какой рабочей станции запущена консоль управления.

X Создание резервной копии	×
Директория	
C:\Blockhost Backups	🖉 Изменить
Создать	Отмена

Рисунок 10.4 – Выбор директории для сохранений резервной копии

Установите пароль для резервной копии (рисунок 10.5) и нажмите Далее.

🗙 Установка пароля для р	езервных копий 🛛 🗙
Пароль	
•••••	$\odot$
Повтор пароля	
•••••	Ø
Далее	Отмена

Рисунок 10.5 – Установка пароля для резервной копии

Процесс создания резервной копии происходит в «тихом» режиме, позволяя администратору продолжать работу в консоли управления по настройке средства защиты, не дожидаясь окончания создания копии.

## 10.1.2 Удаление резервных копий вручную

Для удаления резервной копии вручную во вкладке *Список* (рисунок 10.2) в списке резервных копии установите курсор на строку резервной копии, которую необходимо удалить и нажмите кнопку <sup>Зудалить</sup>.

Подтвердите удаление резервной копии (рисунок 10.6) и нажмите Удалить.



Рисунок 10.6 – Удаление резервной копии

При выполнении операции удаления резервной копии удаляется как запись из журнала, так и сам файл резервной копии на сервере.

## 10.1.3 Автоматическое создание резервных копий

Для создания резервной копии вручную во вкладке *Настройки* сервера перейдите в раздел «Резервные копии» (рисунок 10.3), во вкладку *Настройки*.

Перед включением механизма автоматического создания резервных копии необходимо в области **Пароль по умолчанию** установить пароль, который будет использоваться при автоматическом сохранении (рисунок 10.7).



🗙 Бл	окхост-Сеть 4			- [	×
Å	Менеджер иерархий				
к <sup>†</sup> л	C. • • <b>3</b>	QC	🏭 W102 🗮 0 🖵 1 Онлайн 🔍		C
冏	- 🔛 W102		Общее Политики Настройки	Статистика События Лицензии	
-	<ul> <li>Все компьютеры</li> </ul>		Настройки сервера	Резервные копии	
	localhost		Резервные копии		
			Автоархивация событий	Пародь Парод	
			Кеш событий	Orc,     Orc,	
			Построение иерархии серверов	Переме Повтор пароля	
			Экспорт событий в SIEM	C:\Bio	op
				Пароль должен содержать от 8 до 10 символов. Пароль должен включать символы как минимум из 3 гоупп:	
				- символы верхнего регистра (А-Z) - символы нижнего регистра (а-z)	
				Уда1 - числа (0-9) - специальные символы (@ # \$ % ^ & *!+ = [] { } <	0
				Установить Отмена	

Рисунок 10.7 – Установка пароля для резервной копии

Включите механизм автоматического создания резервных копий, установив переключатель в положение <sup>С Автоматическое создание резервных копий включено</sup> (рисунок 10.8)

🗙 Бло	окхост-Сеть 4		-	
ஃ	Менеджер иерархий			
кÔя	C. • <b>9</b> 8	QC	🔛 W102 🗒 0 🖵 1 Онлайн 🔍	C
20	▼ 🛱 W102		Общее Политики Настройки <sup>*</sup> Статистика События Лицензии	
	▼ Все компьютеры		Настройки сервера Резервные копии	
	localnost		Резервные копии*	
			Автоархивация событий	
			Кеш событий 📀 Задан 🔃	
			Построение иерархии серверов Перемещать резервные копии в	
			Экспорт событий в SIEM C:\Blockhost Backups	Обзор
			Автоматическое создание резервных копий	
			Резервная копия будет создана в 10:00 30.01.2024 по локальному врем	ени сервера
			Время запуска	10:00
			Повторять каждые, дней	7
			Удалять резервные копии старше, дней	90
			Максимальное количество отображаемых записей в журнале	20
ŝ			Применить Отмена	

Рисунок 10.8 – Настройка автоматического создания резервной копии

В области **Перемещать резервные копии в** по кнопке **Обзор** выберите директорию, в которую будут сохраняться автоматически созданные резервные копии (рисунок 10.8) и нажмите на кнопку **Применить**.

Установите время запуска автоматического создания резервной копии в параметре **Время запуска** и частоту повторения запуска в параметре **Повторять каждые, дней**.

После сохранения настроек по кнопке *Применить* автоматическое создание резервных копий будет выполнять согласно заданному в настройках расписанию.

## 10.1.4 Восстановление из резервной копии

Для восстановления из резервной копии во вкладке Настройки сервера перейдите в

раздел «Резервные копии» (рисунок 10.2) и нажмите кнопку 🕅 Восстановить...

Выберите директорию, из которой будет восстановлена резервная копия (рисунок 10.9) и нажмите на кнопку **Восстановить**.

196



🔀 Восстановление из резервной копии 🛛 🗙 🗙
Имя
▼ 🕞 C:\
SRecycle.Bin
SWinREAgent
▼ 🛅 BlockHost
2023-05-13_22-52-11.bhbackup
AuditSystem
Backup
▶ 🗀 bppfw
DeploymentSystem
PrintControl
protected
System32
Восстановить Отмена

Рисунок 10.9 – Выбор директории для восстановления из резервной копии

Введите пароль к резервной копии (рисунок 10.10) и нажмите **Восстановить** для запуска процесса восстановления.

🔀 Восстановление данных из резервной копии					
Копия					
2023-05-13_22-52-11					
Пароль					
•••••	$\odot$				
Восстановить	Отмена				

Рисунок 10.10 – Ввод пароля к резервной копии



Во время процесса восстановления из резервной копии интерфейс блокируется, администратору необходимо дождаться окончания восстановления данных (рисунок 10.11) для продолжения работы в консоли управления.



Рисунок 10.11 – Успешное восстановление данных из резервной копии

#### 10.1.5 Особенности восстановления из резервных копий

При восстановлении данных из резервных копий необходимо учитывать следующие ограничения:

1) В СЗИ от НСД «Блокхост-Сеть 4» <u>не поддерживается</u> восстановление резервной копии, созданной на сервере под управлением ОС Linux, в сервер под управлением ОС Windows. При попытке восстановления такой резервной копии на сервере под управлением ОС Windows на экран будет выведена ошибка (рисунок 10.12).

Обратная ситуация – восстановление резервной копии, созданной на сервере под управлением ОС Windows, в сервер под управлением ОС Linux поддерживается.

#### 72410666.00063-04 95 01-01



🗙 Восстановление из резервной копии	×
$\bigotimes$	
При восстановлении данных произошла ошибка	
Восстановление из резервной копии сделанной в ОС Linux не поддерживается.	
	Ок

Рисунок 10.12 – Ошибка при восстановлении резервной копии созданной в OC Linux

2) При выполнении резервного копирования <u>не сохраняются</u> локальные настройки клиентских рабочих станций.

3) При восстановлении из резервной копии, созданной на сервере под управлением OC Windows, на сервер под управлением OC Linux, если в серверной политике **Доступ к серверу** (см. раздел **Доступ к серверу**) были заведены доменные или локальные пользователи, они останутся в политике после миграции, однако возможность использовать учетные записи таких пользователей для аутентификации при входе в консоль управления сервера СЗИ не поддерживается.

Для аутентификации при входе в консоль управления сервера СЗИ под управлением ОС Linux используются только встроенные пользователи Блокхост-Сеть.

4) При восстановлении из резервной копии лицензия СЗИ от НСД «Блокхост-Сеть 4» не переносится, т.к. привязана к конкретному серверу. После восстановления из резервной копии лицензию можно добавить на новый сервер. В этом случае предыдущая лицензия перестанет действовать.

5) При восстановлении из резервной копии автоархивация событий отключена. Для включения автоархивации необходимо настроить механизм автоархивации событий заново (см. раздел *Автоархивация событий*).

#### 72410666.00063-04 95 01-01

# 10.2 Автоархивация событий

Автоархивация событий предназначена для настройки параметров архивации событий, собранных с подчиненных серверов и клиентских рабочих станций на выбранном сервере.

При настройке параметров автоархивации устанавливаются время первого запуска механизма автоархивации и интервал запуска, выбираются события для перемещения в архив и действия над ними.

🗙 Бло	жхост-Сеть 4		_	
&	Менеджер иерархий			
к∱я		Q C	🔛 W102 🗒 0 🖵 1 Онлайн •	C
78	✓ ₩ W102		Общее Политики Настройки <sup>*</sup> Статистика События Лицензии	
	• 🗅 Все компьютеры		Настройки сервера Резервные копии Автоархивация событий* Автоархивация событий Автоархивация событий Автоархивация событий Сограция будет запущена по локальному времени сервера Время первого запуска Время первого запуска Операция будет запущена по локальному времени сервера Мнтервал запуска, дни 1 0 Остроение иерархии серверов Интервал запуска, дни 1 0 Остроение иерархии серверов Остроение иерархии серверов Перемещать в архив: ● Все события в хранилище ○ Только события, старше (дни): 1 Что делать с события каталоге 0 Гроверить Обз • Удалять события навсегда 0	00 ¢
EIII (ÇŞ			Применить Отмена	

Рисунок 10.13 – Настройка автоархивации хранилища событий на сервере

Для настройки автоархивации событий во вкладке *Настройки* сервера перейдите в раздел «Автоархивация событий» (рисунок 10.13) и включите механизм автоархивации событий, установив переключатель в положение Механизм включен .

Выполните настройку параметров автоархивации событий:

– **Время первого запуска** – ввод даты и времени первоначального запуска архивации хранилища событий на сервере (по локальному времени выбранного сервера);

- **Интервал запуска, дни** – период, заданный в днях, между окончанием предыдущей архивации событий на сервере и началом следующей (допустимые значения 1-365);

- **Перемещать в архив** – возможность выбора событий для перемещения в архив:

- Все события в хранилище для перемещения в архив всех событий, находящихся в хранилище;
- Только события, старше (дни) –для перемещения в архив только тех событий, которые хранятся на сервере начиная с даты, предшествующей текущей дате на введенное в поле количество дней, и по текущее время (допустимые значения 1-365);
- Выбор действий над событиями хранилища, отмеченными для архивации:
  - Создавать архивы событий в каталоге создание архива событий, хранящихся на сервере в каталоге по указанному пути;
  - Удалять события навсегда удаление событий, хранящихся на сервере (подробно удаление событий описано в разделе «Удаление событий аудита»).

При создании архива событий в каталоге возможно проверить заданный путь к каталогу по кнопке **Проверить**. Если при проверке искомый каталог не будет найден появится сообщение об ошибке (рисунок 10.14).



При необходимости создания архива событий в новом каталоге заранее создайте каталог по указанному пути.



Рисунок 10.14 – Ошибка при создании архива событий в каталоге

При создании архива событий на сетевом ресурсе, путь к нему прописывается вручную в UNC формате. Например: <u>\\Server\Share\ArchiveFolder</u>

## 10.2.1 Удаление событий аудита

В разделе **Автоархивация событий** возможно выполнить удаление событий аудита, собранных с подчиненных серверов и клиентских рабочих станций на выбранном сервере.

Для удаления событий аудита во вкладке *Настройки* сервера перейдите в раздел 72410666.00063-04 95 01-01

«Автоархивация событий» (рисунок 10.13) и включите механизм автоархивации событий, установив переключатель в положение 🤍 Механизм включен .

Установите параметры удаления событий: время запуска удаления событий, интервал запуска и выбор событий для удаления в соответствии с описанием в разделе **«Резервные копии»**.

Выберите при настройке действий над событиями хранилища **Удалять события** навсегда.

•

При удалении событий аудита происходит очистка базы данных событий. Восстановление удаленных событий невозможно!

# 10.3 Кеш событий

Раздел «Кеш событий» (рисунок 10.15), предназначен для настройки размера трансляционной базы данных, использующейся для временного хранения событий, полученных сервером с клиентских рабочих станций и со всех подчиненных ему серверов.

События хранятся в кеше событий до момента передачи на вышестоящий сервер. После передачи событий на вышестоящий сервер, кеш событий очищается.

🗙 Бло	кхост-Сеть 4			– 🗆 ×
&	Менеджер иерархий			
к <sup>†</sup> л		QC	💱 W102 🗒 0 🖵 1 Онлайн •	C
四	<ul> <li>W102</li> </ul>		Общее Политики Настройки <sup>*</sup> Статистика События Лицензии	
	<ul> <li>Все компьютеры</li> <li>Iocalhost</li> </ul>		Настройки сервера Кеш событий Резервные копии Автоархивация событий* Кеш событий Построение иерархии серверов Экспорт событий в SIEM	Подробнее

Рисунок 10.15 – Настройка размера кеша событий

Для настройки максимального размера кеша событий во вкладке *Настройки* сервера перейдите в раздел «Кеш событий» (рисунок 10.15) и установить требуемое значение (минимально допустимый размер кеша событий – 100 Гб).

В случае превышения установленного максимального размера кеша событий сбор событий с клиентских рабочих станций и подчиненных серверов будет приостановлен и возобновится в случае, когда актуальный размер кеша событий станет меньше установленного максимального значения.

# 10.4 Построение иерархии серверов

Раздел «Построение иерархии серверов» (рисунок 10.16), предназначен для просмотра общей информации текущего сервера и присоединения сервера в иерархию в качестве головного или подчиненного сервера.

🗙 Бло	окхост-Сеть 4		-	×
ጽ	Менеджер иерархий			
к <sup>ф</sup> я		Q C	🛱 W102 🗒 0 🖵 1 Онлайн •	С
ŕÐ	• 📰 W102		Общее Политики <mark>Настройки*</mark> Статистика События Лицензии	
	• Dec компьютеры		Настройки сервера Резервные копии Автоархивация событий* Кеш событий Тостроение иерархии серверо Экспорт событий в SIEM	
۵. ۵			Применить Отмена	

Рисунок 10.16 – Построение иерархии серверов

Для просмотра информации по текущему серверу во вкладке *Настройки* сервера перейдите в раздел «Построение иерархии серверов» или воспользуйтесь пунктом контекстного меню *Построение иерархии серверов*.

В поле *Статус сервера* указывается текущий статус сервера – функционирует сервер в иерархии или автономно.

В поле *IP адрес*, *порт* указывается IP-адрес и номер TCP-порта сервера, по которым будет происходить подключение в иерархию.

## 10.4.1 Настройка подключения подчиненных серверов

Для включения сервера в иерархию в качестве головного или родительского сервера, необходимо настроить возможность подключения к нему подчиненных серверов.

Для подключения подчиненных серверов к родительскому в области **Выберите вид** 

## 72410666.00063-04 95 01-01





подключения перейдите на вкладку Подчиненные серверы и нажмите кнопку Подключить

(рисунок 10.17).

🗙 Бло	кхост-Сеть 4		_	×
&	Менеджер иерархий			
к <sup>ф</sup> я		🔛 W102 🗒 0 🖵 1 Онлайн •		С
四	▼ 🔛 W102	Общее Политики Настройки* Статистика События Лицензии		
10	• 🗋 Все компьютеры	Настройки сервера		
0	localhost	Построение иерархии серверов Резервные копии		
		Статус сервера Автономный 🛈		
		Автоархивация событий* IP-адрес, порт ① 192.168.209.177:59731 □		
		Кеш событий		
		Выберите вид подключения Построение иерархии серверов		
		Подключение к мастер-серверу Подчинённые серверы		
		Подчинённые серверы отсутствуют Подключить		
Ĩ				
දිලිද		Применить Отмена		

Рисунок 10.17 – Подключение подчиненных серверов

В появившемся окне мастера подключения подчиненного сервера (рисунок 10.18) необходимо скачать сертификат текущего сервера, который будет головным для подключаемых серверов, и отправить сертификат администратору подчиненного сервера для последующей установки в консоли управления подключаемого подчиненного сервера.



🗙 Подключение подчинённого сервера		×
Отправьте данный сертификат администрат	гору подчиненного сер	вера.
Скачать сертификат текущего сери	зера	
	Далее	Отмена

Рисунок 10.18 – Запуск мастера подключения подчиненных серверов

Перед выполнением последующих действий по подключению подчиненного сервера, убедитесь, что сертификат головного сервера был получен и установлен администратором подчиненного сервера (подробнее в разделе Настройка подключения к мастер-серверу) и дождитесь получения данных подчиняемого сервера (IP-адрес/DNS-имя) от администратора.

В следующем окне мастера подключения необходимо подтвердить отправку сертификата головного сервера администратору подчиненного сервера (рисунок 10.19) и нажать кнопку **Продолжить**.

🗙 Подключение подчинённого сервера				
Внимание				
Отправьте скаченный сертификат администратору подчиненного сервера. Установка сертификата на подчиненном сервере обязательна для его включения в иерархию. Я отправил сертификат администратору подчинённого сервера				
Продолжить Отмена				





В следующем окне выберите группу для включения в нее подчиненного сервера (рисунок 10.20) и нажмите **Далее**.

Х Подключение подчинённого сервера	×
Выберите группу для включения в нее подчиненного сервера. После включения о иерархию все действующие политики выбранной группы будут применены к серв	сервера в зеру.
🗀 Все компьютеры	

Рисунок 10.20 – Выбор группы для включения подчиненного сервера

В следующем окне (рисунок 10.21) в поле *IP-адрес/DNS-имя* вставьте данные подключаемого сервера, полученные от администратора подчиняемого сервера. Поле *Порт* заполнено значением по умолчанию, задающимся в мастере настройки Блокхост-Сеть в поле *Порт сервера Блокхост-Сеть для построения иерархии серверов*, при необходимости порт можно изменить.

🔀 Подключение подчинённого сервера		×
Вставьте в поля ниже данные подчинённого	о сервера	
IP-адрес/DNS-имя		
Порт		
59731		
Назад		Отмена

Рисунок 10.21 – Ввод данных подчиняемого сервера

После нажатия **Подключить** появится окно для подтверждения параметров подключаемого сервера (рисунок 10.22). Нажмите **Ок** для включения сервера в иерархию.



🗙 Подключение подчинённого сервера	×
Проверьте параметры подчинённого сервера	
Имя сервера w09w13.pki.local Идентификатор сервера 752fa8d77180aace4116bb3de1f1f064a2bec12f	
Назад Ок	Отмена

Рисунок 10.22 – Подтверждение параметров подчиняемого сервера

При успешном завершении операции появится сообщение о добавлении сервера в иерархию (рисунок 10.23) и подчиненный сервер будет отображен в иерархии серверов (рисунок 10.24).



Рисунок 10.23 – Успешное завершение операции подключения сервера



🗙 Бло	кхост-Сеть 4		×
&	Менеджер иерархий		
к <sup>ф</sup> я	Ci 🗊 🛱 🔍 C	№ w09w13	;
70	▼ III SERV1	Общее Политики Настройки Статистика События Лицензии	
۲	<ul> <li>w09w13</li> <li>Все компьютеры</li> </ul>	Автоархивация событий Статус сервера Подчиненный <sup>(</sup> )	
	🖬 localhost	Кэш событий IP-адрес, порт ① 10.72.9.62:59731 □ Построение иерархии серверов	
		Экспорт событий в SIEM Выберите вид подключения Подключение к мастер-серверу Подчинённые серверы	
Ĩ		Подчинённые сервера отсутствуют Одключить	
ŝ		Применить Отмена	

Рисунок 10.24 – Отображение подчиненного сервера в иерархии

Для вывода подчиненного сервера из иерархии перейдите на сервер в менеджере иерархий (рисунок 10.25) и выберите пункт **Вывести из иерархии** в контекстном меню сервера.



🔀 Бло	кхост-Сеть 4					-	×
ጽ	Менеджер иерархий						
кĴя		🔐 w09w13 🗮 0 🖵	1 Онлайн 🔍				G
冏	▼ E SERVI	Общее Политики	Настройки	Статистика События	Лицензии		
	все компьютеры           •	Настройки сервера		Построение иера	архии сер	оверов	
	► Всек ⊕ Создать политику			Статус сервера		Подчиненный 🛈	
	🐖 localhost 🗠 Запустить внеплановую	загрузку событий аудита 🕨		IP-адрес, порт 🛈		10.72.9.62:59731	
	🛱 Построение иерархии се	рверов	💀 Вывести	из иерархии	ючения		
	④ О сервере		🛱 Подклю	чить подчинённый сервер	рверу Г	Тодчинённые серверы	
			🗍 Скопирс	овать IP-адрес и порт сервера Сертификат мастер-серв	sepa <b>Eo</b>		
				Мастер-сервер	10.72.9.	65 :	
				<ul> <li>Данные для валидац</li> </ul>	ии текущего	сервера	
Ē							
ŝ		Применить С					

Рисунок 10.25 – Вывод подчиненного сервера из иерархии

#### 10.4.2 Настройка подключения к мастер-серверу

Для включения сервера в иерархию в качестве подчиненного сервера, необходимо настроить возможность подключения его к родительскому серверу.

Для настройки подключения подчиненного сервера к родительскому в области **Выберите вид подключения** перейдите на вкладку **Подключение к мастер**-

серверу и нажмите кнопку (рисунок 10.26).

209

🗙 Бло	кхост-Сеть 4	_	×
ጽ	Менеджер иерархий		
кĴя		💱 W102 🗒 0 🖵 1 Онлайн •	С
28	▼ 🛱 W102	Общее Политики Настройки* Статистика События Лицензии	
10	<ul> <li>Все компьютеры</li> </ul>	Настройки сервера	
	localhost	Резервные копии	
		Автоархивация событий*	
		IP-адрес, порт ① 192.168.209.177:39731 _] Кеш событий	
		Выберите вид подключения	
		Подключение к мастер-серверу Подчинённые серверы	
		Данный сервер не подключен к мастер-серверу	
Ē			
ţĝ		Применить Отмена	

Рисунок 10.26 – Подключение подчиненного сервера к родительскому

В появившемся окне мастера подключения к родительскому серверу (рисунок 10.27)

необходимо по кнопке • Добавить сертификат... установить сертификат головного сервера, полученного от администратора родительского сервера и нажать кнопку Продолжить.



🔀 Подключение к мастер-серверу				
Добавьте сертификат, полученный от администратора мастер-сервера				
Сертификат мастер-сервера				
Продолжить Отмена				

Рисунок 10.27 – Добавление сертификата головного сервера

В следующем окне отобразятся данные сервера для подключения к родительскому серверу (рисунок 10.28). Необходимо скопировать и отправить данные администратору родительского сервера.

	S STILLAR S	
🗙 Подключение к масте	р-серверу	<
Скопируйте и отправьте сервера	следующие данные администратору мастер-	
IP-адрес, порт	10.72.9.62:59731	
Имя сервера	w09w13.pki.local	
Идентификатор сервера	bd6791ed346ae5ef03b07a88c91c3633b71d2937	
	Ок Скопировать	

Рисунок 10.28 – Копирование сертификата головного сервера

В следующем окне появится сообщение о успешном добавлении сертификата (рисунок 10.29). Подчиняемый сервер будет добавлен в иерархию после выполнения администратором родительского сервера необходимых настроек (подробнее в разделе *Настройка подключения подчиненных серверов*).



Рисунок 10.29 – Успешное добавление сертификата головного сервера

# 10.5 Экспорт событий в SIEM

Раздел **«Экспорт событий в SIEM»** предназначен для настройки параметров экспорта событий аудита в SIEM (рисунок 10.30). Настройки раздела отличаются в зависимости от того головной сервер выбран в иерархии или подчиненный.

Включение/выключение механизма экспорта событий аудита в SIEM и выбор событий для экспорта осуществляется только на <u>головном сервере</u> иерархии. Изменение параметров работы механизма на подчиненных серверах не доступно.

Передача событий в SIEM осуществляется в CEF-формате. Формат каждого события можно уточнить в Приложении 1 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит».

#### 10.5.1 Экспорт событий в SIEM головного сервера

При включении механизма экспорта событий аудита в SIEM, на головном сервере активируется механизм, выполняющий передачу событий аудита в SIEM.

При выключенном механизме передачи событий в SIEM головной сервер продолжает выполнять сбор событий аудита с клиентских рабочих станций и подчиненных серверов для сохранения в собственные хранилища событий.

🗙 Бло	кхост-Сеть 4					-	×
ጽ	Менеджер иерархий						
к <sup>†</sup> л	C. 🛍 📮 🖫	QC	🎛 W102 🗮 0 🖵 1 Онлайн 🖲				C
c四	▼ 🛱 W102		Общее Политики Настройки	Статистика События Лиценз	и		
٢u	• 🗀 Все компьютеры		Настройки сервера				
ē	🔢 localhost		Резервные копии	Экспорт событий в SIEM			
			Автоархивация событий*	Передавать события аудита			
				IP-адрес SIEM	192.168.100.1		
			Кеш событий	Порт SIEM	0		
			Построение иерархии серверов	Протокол	ТСР		
			Экспорт событий в SIEM	События Выбрано 39			
				Передавать события в SIEM только	с клиентов этого сер	вера 🛈	
				Передавать статистику о состояни	и иерархии 🛈		

Рисунок 10.30 -	Раздел	«Экспорт	событий	вSIEM»
-----------------	--------	----------	---------	--------

Для настройки экспорта событий в SIEM во вкладке *Настройки* головного сервера перейдите в раздел «Экспорт событий в SIEM» (рисунок 10.29) и включите передачу в SIEM установив флаг в параметре *Передавать события аудита* (рисунок 10.31).

🗙 Бло	кхост-Сеть 4					-		×
ጽ	Менеджер иерархий							
кĴя	C. @ \$	Q C	🎬 W102 🗮 0 🖵 1 Онлайн 🖲					C
(周	▼ 🛱 W102		Общее Политики Настройки*	Статистика События Лицензи	и			
٢u	• 🗀 Все компьютеры		Настройки сервера					
٦	🔚 localhost		Резервные копии	Экспорт событий в SIEM				
			Автоархивация событий*	🦲 Передавать события аудита				
			Vau activity	IP-адрес SIEM	192.168.100.1			
			кеш событии	Πορτ SIEM	0			
			Построение иерархии серверов	Протокол	тср 🔹			
			Экспорт событий в SIEM*	События Выбрано 39				
				Передавать события в SIEM только с клиентов этого сервера ③				
				Передавать статистику о состояни	и иерархии ③			

Рисунок 10.31 – Настройка экспорта событий в SIEM

Определите перечень событий аудита, собираемых с подчиненных серверов и клиентских рабочих станций под управлением ОС Windows/Linux; событий, с клиентских рабочих станций с установленным СДЗ, в окне **Выбор событий аудита** *для SIEM* (рисунок 10.32) по кнопке **События**.

Во вкладке *Windows/Linux* содержится полный список регистрируемых событий, структурированных по разделам.

События, доступные к сбору для клиентских рабочих станций под управлением ОС Windows отмечены пиктограммой 🎟 в столбце ОС. События, доступные к сбору для

клиентских рабочих станций под управлением ОС Linux отмечены пиктограммой 🤷 в столбце ОС.

Во вкладке *СДЗ (Средство доверенной загрузки)* содержится полный список регистрируемых событий, доступных к сбору для клиентских рабочих станций с установленным СДЗ. События структурированы по разделам.

🔀 Выбор типов событий для передачи в SIEM			×
Обратите внимание, что некоторые события отсутствуют в списке, так как не пе	редаются в S	FM	
Windows/Linux СДЗ (Средство доверенной загрузки)	редаются в о	an 1 7 1	
Показать всё 🔻 🔍 Поиск			
✓ Выбрать все П Снять все <sup>ч</sup> с Свернуть всё <sup>ч</sup> Раскрыть всё			
Наименование	ос	Уровень важности	Код
События клиента СЗИ – 11/18			
События сервера СЗИ – 10/19			
<ul> <li>Управление входом в ОС – 13/20</li> </ul>			
Ayтентификация через RunAs или открытие сессии		і Сведения	3892
Вход в систему по RDP	==	і Сведения	3888
Выход пользователя из системы	==	і Сведения	1029
Доступ к сетевому ресурсу	==	і Сведения	3890
Запись безопасного пароля пользователя на токен	= ◊	і Сведения	3991
Локальный вход в систему	= ◊	і Сведения	3880
Отказ в возобновлении сеанса пользователя	==	<ol> <li>Предупреждение</li> </ol>	3896
Выбрано: 41 Всего: 151			
		Ок	Отмена

Рисунок 10.32 – Выбор событий для передачи в SIEM

Настройте параметры для передачи событий в SIEM:

*IP-адрес SIEM* – ввод IP-адреса сервера, на котором установлена SIEM;

– **Порт SIEM** – ввод значения порта, по которому осуществляется работа сервера, с установленной SIEM;

– **Протокол** – выбор протокола для передачи данных в SIEM (TCP или UDP).

При установке флага **Передавать события в SIEM только с клиентов этого сервера** сбор данных в SIEM будет осуществляться только с клиентов головного сервера, не учитывая клиентов подчиненных серверов.

При установке флага **Передавать статистику о состоянии иерархии** в SIEM будут передаваться помимо выбранных событий аудита, данные о типе аутентификации, статусе и режиме работы клиентов в иерархии серверов.

## 72410666.00063-04 95 01-01

## 10.5.2 Экспорт событий в SIEM подчиненного сервера

Настройка передачи собираемых событий с подчиненного сервера осуществляется во вкладке *Настройки* подчиненного сервера в разделе «Экспорт событий в SIEM» (рисунок 10.33).

2 8 <b>0</b>	Q C	🔤 SBHNC-W2019 🔛 0 🖵 1 Онлайн ө			
SSHNC-W2019		Общее Политики Настройки	Статистика Событи	а Лиценския	
<ul> <li>Bce компьютеры</li> <li>SBHNC-W2019.BH.App.Dev</li> </ul>	Настройки сервера Автоаринация событий Клш событий Построение иерариии серверов Эколорт событий в SIEM		Канал передачи событий в SIEM В Передавать события аудита на вышестоящий сервер Передавать события аудита в SIEM Адрес SIEM ©		
		10	IP-appec SIEM	192.168.100.1	
			Flop# SIEM	514	

Рисунок 10.33 – Настройка передачи событий подчиненного сервера

По умолчанию экспорт событий в SIEM с подчиненных серверов осуществляется через родительский сервер (установлен флаг *Передавать события аудита на вышестоящий сервер*). При этом события аудита, собранные текущим сервером со своих клиентских компьютеров и подчиненных серверов, будут переданы на родительский сервер или сохранены в кеш событий (в случае отсутствия родительского сервера).

При включенном на головном сервере механизме экспорта событий в SIEM-систему, на подчиненном сервере возможен экспорт в SIEM напрямую. Для этого необходимо установить флаг **Передавать события аудита в SIEM** и выполнить настройку параметров для передачи событий в SIEM:

- *IP-адрес SIEM* – ввод IP-адреса сервера, на котором установлена SIEM;

– **Порт SIEM** – ввод значения порта, по которому осуществляется работа сервера, с установленной SIEM.



При установке флага **Передавать события аудита в SIEM** сбор данных на родительский сервер не будет осуществляться, события будут передаваться напрямую в SIEM.

# 11 Настройки клиента

Настройки клиента предполагают управление параметрами работы клиентских рабочих станций непосредственно на самих рабочих станциях, локально.

Настройки клиента задаются во вкладке *Настройки* (рисунок 11.1) при выборе в иерархии клиентской рабочей станции.

Настройки клиентских рабочих станций разделены на вкладки **Блокхост-Сеть** и **SafeNode** для управления настройками клиентских рабочих станций под управлением СЗИ от НСД «Блокхост-Сеть 4» и настройками клиентских рабочих станций с установленным и взятым под управление СДЗ «SafeNode System Loader».

На вкладке **Блокхост-Сеть** для локальной настройки на клиентских рабочих станциях доступны следующие механизмы:

– *Дискреционный доступ* (настройка доступа пользователей к объектам файловой системы: логическим дискам, каталогам и файлам).

- **Замкнутая программная среда** (формирование списка разрешенных для запуска процессов, доступных для выбранного пользователя на клиентской рабочей станции).

 Контроль печати (разграничение прав печати для указанных приложений, простановка специального колонтитула по шаблону печати для указанных приложений).

- *Контроль целостности файлов с восстановлением* (отслеживание изменений в перечне заданных файлов и восстановление их из резервных копий).

- **Мандатный доступ** (настройка доступа пользователя к файловым ресурсам станции с помощью присвоения пользователям и ресурсам определенных меток).

- **Проверка пароля в СЗИ** (настройка возможности входа пользователя в систему с использованием пароля).

 Пользователи с разрешением на вход в ОС (формирование списка пользователей, которым будет предоставлена возможность входа на клиентскую рабочую станцию).
ХБл	жхост-Сеть 4		D X
*	Менеджер иерархий		
* 10 E	СВОЛОС • Пе W101 • СВсекомпьютеры Ge localhost	<ul> <li>№ №101 Онлайн</li> <li>Общее Токены Пользователь Настройки События</li> <li>В Блокхост-Сеть SafeNade</li> <li>Анскреционный доступ</li> <li>Замкнутая программиная среда</li> <li>Контроль целостнюсти файлов с восстановлением</li> <li>Мандатный доступ</li> <li>Проверка пароля в СЗИ</li> <li>Пользователи с разрешением на вход в ОС</li> </ul>	С
		Boero: 1	

Рисунок 11.1 – Локальные настройки клиента Блокхост-Сеть

На вкладке **SafeNode** для локальной настройки на клиентских рабочих станциях доступны следующие механизмы:

– **Пользователи СДЗ (Средства доверенной загрузки)** (удаленное управление разблокировкой пользователей на клиентских рабочих станциях с установленным СДЗ «SafeNode System Loader», заблокированных после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей);

 Сетевой адаптер UEFI (настройка на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» сетевого адаптера UEFI для взаимодействия клиента и сервера LDAP при выборе способа получения сетевых настроек статически).

 Проверка пароля в SafeNode (настройка возможности входа пользователя в систему с использованием пароля).

– **Пользователи с разрешением на вход в ОС** (формирование списка пользователей, которым будет предоставлена возможность входа на клиентскую



рабочую станцию).

🗙 Бло	кхост-Сеть 4		- 🗆 X		
ጽ	Менеджер иерархий				
кĴя		🙀 W102 Онлайн	C		
冏	▼ ∰ W102	Общее Токены Пользов	атель Настройки События		
8	<ul> <li>Все компьютеры</li> <li>localhost</li> </ul>	🐰 Блокхост-Сеть 🛛 💋 SafeNo	de		
		Пользователи СДЗ (Средства доверенной загрузки)	Пользователи СДЗ (Средства доверенной загрузки)		
		Сетевой адаптер UEFI	<i>©</i> Разблокировать		
		Проверка пароля в SafeNode	Имя пользователя 🔻 Статус		
		Пользователи с разрешением	☆ user1		
		на вход в ОС	☆ ivanov-i@pki.local		
			은 Guest@pki.local		
E			Bcero: 3		
£633		Пряменить Отмена			

Рисунок 11.2 – Локальные настройки клиента SafeNode

# 11.1 Дискреционный доступ

Дискреционный доступ представляет собой настройку доступа всех пользователей к объектам файловой системы (логические диски, каталоги и файлы).

**(;** 

Для настройки дискреционного доступа на рабочей станции под управлением OC Windows предварительно должен быть установлен модуль «Контроль файловой системы». На рабочие станции под управлением OC Linux данный модуль устанавливается при установке клиента.

**i** 

В сообщениях аудита дискреционного доступа в ОС Linux из-за настроек ОС имя доменного пользователя может быть отображено без домена. Чтобы имя доменного пользователя отображалось с доменом необходимо в конфигурационном файле /etc/sssd/sssd.conf установить следующий параметр:

```
use_fully_qualified_names = True
```

Возможны следующие виды доступа пользователей к объектам файловой системы:

– **Просмотр** – санкционируется возможность чтения пользователем информации из объекта и возможность копирования объекта в любое место файловой системы незапрещенное данным, либо другим механизмом защиты информации.

 Изменение – санкционируются такие действия контролируемых пользователей, которые приводят к изменениям информации в объекте: удалению, переименованию и перемещению объекта.

По умолчанию в список объектов файловой системы дискреционного механизма добавлен файловый объект **Все файлы**, который подразумевает под собой все логические диски, доступные пользователю при работе, с правом полного доступа к ним всех пользователей. Параметры доступа, определенные для файлового объекта **Все файлы**, будут применены для всех явно не добавленных в список ресурсов дискреционного механизма логических дисков рабочей станции.

Параметры дискреционного доступа, указанные для диска/каталога, автоматически распространяются и на вложенные в него файлы и каталоги. Для изменения параметров доступа к вложенным объектам необходимо добавить их в список объектов дискреционного механизма и указать требуемые параметры доступа.

**О** Дискреционный доступ разграничения доступа построен по принципу – что явно не разрешено, то запрещено.

Разграничение доступа к контролируемым объектам выполняется сочетанием политик доступа к объектам файловой системы операционной системы и СЗИ. При этом необходимо учитывать следующее:

 дискреционный механизм дополняет, но не исключает действующей политики разграничения NTFS;

 права доступа к объектам, заданные дискреционным механизмом, распространяются на вложенные в них папки и файлы, при отсутствии отличных прав доступа к ним;

 для исключения вложенного объекта из действующего разграничения доступа, заданного дискреционным механизмом, данный объект указывается с иными правами доступа к нему.

Особенность работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа описана в Приложении 1 к настоящему документу.

Разграничение доступа к объектам файловой системы представляет собой список объектов с сопоставленными им пользователями и группами пользователей с установленными настройками доступа к объектам: **Просмотр** и **Изменение.** 

Для настройки дискреционного механизма разграничения доступа во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Дискреционный доступ» (рисунок 11.3).

Х Бл	окхост-Сеть 4				- 0	×
&	Менеджер иерархий					
\$ 10	С. В. В. В. С. • Б. моэміз • D. Все компьютеры	<ul> <li>PC1 Онлайн</li> <li>Общее Токены Пользов</li> <li>Блокхост-Сеть SafeNo</li> </ul>	атель <mark>Настройки"</mark> События de			c
	<ul> <li>C: Fpynna 1</li> <li>C: Fpynna 2</li> <li>C: Fpynna 3</li> </ul>	Дискреционный доступ* Замкнутая программная среда	Дискреционный доступ			() Под
	PCI	Контроль печати Контроль целостности файлов	🔸 🖉 Изменить 🐨 Удалить Имя файлов	* Аудил	Пользователей/гр	улл
		Мандатный доступ	ВСЕ ФАЙЛЫ		Все пользовате	пи
		Проверка пароля в СЗИ				

Рисунок 11.3 – Настройка дискреционного механизма

По кнопке сформируйте список файловых объектов для которых необходимо разграничить доступ (рисунок 11.4) и включите механизм дискреционного доступа, установив переключатель в положение С Механизм включен.



Рисунок 11.4 – Добавление файлов для разграничения доступа



Для добавления пользователей или группы пользователей, которым устанавливается или ограничивается доступ к выбранному файловому объекту, перейдите в строку с

добавленным объектом и нажмите кнопку Изменить (рисунок 11.3).

В появившемся окне Изменение доступа к каталогу <имя каталога> (рисунок

11.5) по кнопке сформируйте список пользователей или групп пользователей (см. раздел *«Добавление пользователей или групп пользователей»*) которым необходимо разграничить доступ к выбранному файловому объекту и нажмите *Добавить*.

🔀 Изменение доступа к каталогу "С:\Temp"			
+ 🔟 Удалить	Разрешения	Скрыть	
Пользователь/Группа Тип			
മ്റ്ര് Все пользователи	Тип Разрешить	Запретить	
pki.local\user02 Active Directory	Просмотр 🔽		
pki.local\user01 Active Directorv	Изменение 🔽		

Рисунок 11.5 – Формирование списка пользователей для разграничения доступа к файлу

При добавлении пользователей в список, по умолчанию им предоставлен доступ на просмотр и изменение выбранного файлового объекта (рисунок 11.5).

В области **Разрешения** (рисунок 11.5) установите требующиеся ограничения на доступ к выбранному файловому объекту для каждого из добавленных пользователей и нажмите **Применить**.

Доступ для пользователя с учетом настроек групп, куда входит данный пользователь, вычисляются исходя из правил пересечения прав, описанных в разделе *«Пересечение прав»*.

При необходимости фиксировать в журнале аудита доступ к указанным напрямую объектам файловой системы, установите параметр *Аудит* в строке с требуемым объектом (рисунок 11.3).

## 11.1.1 Ограничение доступа к файлам СЗИ

Для рабочих станций под управлением ОС Linux у администратора имеется возможность ограничить доступ к файлам СЗИ используя дискреционное разграничение.

Для добавления в список файлов СЗИ необходимо нажать на кнопку **Добавить** *файлы* СЗИ (рисунок 11.6).



•		Блокхо	ост-Сеть 4	- 🖉 🔀
Å	Менеджер иерархий			
.¢. 10	С; Ш Д В Q С • E redos6.freeipa.local • С Все компьютеры Бсе komnьютеры	<ul> <li>№ redos6.freeipa.local</li> <li>Онлайн</li> <li>Общее</li> <li>Токены</li> <li>Пользователь</li> <li>№ Блокхост-Сеть</li> <li>Вабкост-Сеть</li> <li>Забкости Дисси</li> <li>Замкнутая программная</li> </ul>	Настройки События креционный доступ Механизм выключен	С О Подробнее
		среда Проверка пароля в СЗИ Пользователи с разрешением на вход в ОС	Изменить	Q
<u>لا</u>		Применить Отмена	A	

Рисунок 11.6 – Добавление файлов СЗИ

Рекомендуемые для ограничения файлы СЗИ будут добавлены в список (рисунок 11.7).

• Блокхост-Сеть 4				- 🖉 🔀	
å	Менеджер иерархий				
¢.	С в б б с Q C < C C C C C C C C C C C C C C C C C C C	<ul> <li>redos6.freeipa.local</li> <li>Онлайн</li> <li>Общее</li> <li>Токены</li> <li>Пользон</li> <li>Ж Блокхост-Сеть</li> <li>Бабехост-Сеть</li> <li>Бабехост-Сеть</li> </ul>	аатель <mark>Настройки*</mark> События ode Дискреционный доступ		С Подробнее
		Замкнутая программная среда Проверка пароля в СЗИ Пользователи с разрешением на вход в ОС	Механизм выключен         Уласнизм выключен         Уласнизм выключен         Уменчить       Удалить       Добавить фа         Имя факлов       *         ВСЕ ФАЙЛЫ       *         /opt/Blockhost/server/transfer.db       /opt/Blockhost/server/certificate         /opt/Blockhost/server/TokenSystem.db       /opt/Blockhost/server/TokenSystem.db         /opt/Blockhost/server       /opt/Blockhost/cerver         /opt/Blockhost/client/sys_s.key       /opt/Blockhost/client/sys_s.crt         /opt/Blockhost/client/sys.key       /opt/Blockhost/client/sys.key         /opt/Blockhost/client/sys.crt       /opt/Blockhost/client/sys.crt         /opt/Blockhost/client/sys.crt       /opt/Blockhost/client/sys.crt         /opt/Blockhost/client/sys.crt       /opt/Blockhost/client/sys.crt	Аудит         Пользователей/групп           Все пользователи         Все пользователи           Все пользователи         Все пользователи	٩

Рисунок 11.7 – Список добавленных файлов СЗИ

Для добавленных файлов СЗИ для псевдонима **Все пользователи** будет действовать следующее дискреционное разграничение доступа:

Наименование файла	Разграничение доступа
/opt/Blockhost/client	только чтение
/opt/Blockhost/server	только чтение
/opt/Blockhost/console	только чтение
/opt/Blockhost/client/policy.db	запрет чтение запись
/opt/Blockhost/client/messages.db	запрет чтение запись
/opt/Blockhost/client/sys_s.key	запрет чтение запись
/opt/Blockhost/client/sys_s.crt	запрет чтение запись
/opt/Blockhost/client/sys.key	запрет чтение запись
/opt/Blockhost/client/sys.crt	запрет чтение запись
/opt/Blockhost/client/client.db	запрет чтение запись
/opt/Blockhost/client/certificates	запрет чтение запись
/opt/Blockhost/client/key	запрет чтение запись
/opt/Blockhost/server/transfer.db	запрет чтение запись
/opt/Blockhost/server/auditserverParameters.db	запрет чтение запись
/opt/Blockhost/server/TokenSystem.db	запрет чтение запись
/opt/Blockhost/server/certificate	запрет чтение запись

# 11.2 Замкнутая программная среда

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 <u>вручную</u> путем добавления процессов в список разрешенных для выбранных пользователей или <u>автоматически</u> (все процессы, необходимые пользователю, анализируются в течение некоторого временного промежутка во время работы пользователя, и по завершению анализа добавляются в список ЗПС автоматически).



Список разрешенных процессов в обязательном порядке должен включать системные процессы, необходимые для запуска и функционирования операционной системы клиентской рабочей станции.

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.

Запуск процессов, отсутствующих в списке разрешенных для пользователя будет запрещен. При попытке запуска процесса, отсутствующего списке разрешенных для

пользователя, формируется событие аудита на запрет запуска.

Для настройки ЗПС во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Замкнутая программная среда» (рисунок 11.8).

ХЕл	okzect-Cets 4		-	×
ቆ	Менеджер иерархий			
	C B G G Q Q C • E Will • D Bcc Kownworepu • I locelhost	Ваникнутая программная среда         Анкереционный доступ*         Замкнутая программная среда         Эликироль целостности файлов         сосстановленный доступ*         Механизы выслючен         Общее то по программная среда         Эликироль целостности файлов         сосстановленный доступ         Пользователи средования         Механизы выслючен         Эликироль целостности файлов         сосстановленный доступ         Пользователи средованием         Механизы выслючен         Эликироль целостности файлов         Пользователи средованием         Пользователи средователи средованием         Пользователи средованием <t< th=""><th></th><th>c</th></t<>		c
		Прилаенить Отглена		

Рисунок 11.8 – Замкнутая программная среда

Включите механизм ЗПС, установив переключатель в положение 🥌 Механизм включен ,

и по кнопке <sup>1</sup> выберите способ формирования замкнутой программной среды: вручную по кнопке **Стандартный режим** или автоматически по кнопке **Режим автоформирования среды** <sup>11</sup>(рисунок 11.9).



Рисунок 11.9 – Выбор режима формирования ЗПС

<sup>&</sup>lt;sup>11</sup> При отключенном механизме ЗПС режим автоформирования среды работать не будет.

## 11.2.1 Стандартный режим формирования ЗПС

Стандартный режим формирования ЗПС позволяет вручную добавить необходимые процессы в список разрешенных для выбранных пользователей.

Для формирования среды в стандартном режиме выберите в окне создания группы программ (рисунок 11.9) *Стандартный режим* и нажмите *Далее*.

В появившемся окне (рисунок 11.10) во вкладке **Наименование** введите имя создаваемой группы программ. Группа программ представляет собой сущность, включающую соотношение списка пользователей к списку процессов, разрешенных к запуску для пользователей.

🗙 Создание группы программ			
Наименование	Наименование		
Программы	Имя группы программ		
Пользователи	Группа программ 1		

Рисунок 11.10 – Создание группы программ

Во вкладке **Программы** (рисунок 11.11) по кнопке <sup>с</sup> формируется список процессов, доступных к запуску для заданного в категории списка пользователей.

🗙 Создание группы про	×	
Наименование	Программы	
Программы	+ 🔟 Удалить	🛃 Импорт 🚊 Экспорт
Пользователи	Q. Поиск	

Рисунок 11.11 – Вкладка Программы

В окне добавления процессов/программ (рисунок 11.12):

– во вкладке **Приложения** доступны к выбору все исполняемые файлы, зарегистрированные в приложениях, установленные на клиентской рабочей станции;

 во вкладке Запущенные процессы доступны к выбору все процессы, запущенные зарегистрированными пользователями на клиентской рабочей станции (системные процессы, запущенные из-под системных учетных записей, не отображаются в списке);

 во вкладке Файловая система доступны к выбору файлы с расширением «.exe» из файловой системы клиентской рабочей станции.



Х Добавление процессов/программ		×
Приложения Запущенные процессы Файловая система		
Q. Поиск		
Название • Путь		
🗌 🖹 Все процессы		
▶ □ <a>E BHNetDeploymentAgent</a>		
▶		
・ 🗆 岩 Litoria Desktop 2		
▶ 🔽 🔁 Microsoft .NET Framework 4.5.2		
▶ 🗹 된 Microsoft .NET Framework 4.5.2 (RUS)		
▶ 🗌 🔁 Microsoft Visual Studio 2015 Update 3 Diagnostic Tools		
▶ 🗌 🖹 Microsoft Visual Studio 2015 Update 3 Performance Coll		
・ 🗌 🔁 Microsoft Visual Studio 2015 Update 3 Remote Debugger		
▶ □ <a>E</a> SafeNet Authentication Client 8.1 SP1		
. 「 句 <b></b>		
Всего: 130 Выбрано: 37		Всего выбрано: 37
	Добавить	Отмена

Рисунок 11.12 – Формирование списка процессов

Во вкладке **Пользователи** (рисунок 11.13) по кнопке формируется список учетных записей пользователей, которым разрешен запуск процессов, заданных в группе программ (см. раздел **«Добавление пользователей или групп пользователей»**).

💢 Создание группы про	×	
Наименование	Пользователи	
Программы	Q. Поиск	
Пользователи	-	🛃 Импорт 👌 Экспорт



По кнопкам 坐 Импорт / 🖄 Экспорт возможен импорт/экспорт списка пользователей и списка процессов.

## 72410666.00063-04 95 01-01

226

По окончании формирования соотношения пользователь <-> процесс сохраните созданную группу программ по кнопке **Создать**. В списке категорий раздела «Замкнутая программная среда» появится созданная группа (рисунок 11.14) с указанием количества включенных в нее пользователей и сопоставленных им процессов.

ХБл	окхост-Сеть 4				-	×
ቆ	Менеджер иерархий					
÷		🖬 PC1 Онлайн •	Harrowing*	Columna		с
10 E	<ul> <li>Ещ w09w13</li> <li>Все компьютеры</li> <li>Группа 1</li> <li>Группа 2</li> <li>Группа 2</li> </ul>	Сощее токении пользо Х Блоккост-Сеть SafeNo Дискреционный доступ Замконутая программикая	de Замкнутая про	ограммная сред	a	
	PCI	средя" Контроль печати Контроль целостности файлов с восстановлением	нисанный выни Изменить Имя группы	Удалить இ Авто • Программы	формирование 🛈	
		Мандатный доступ Проверка пароля в СЗИ	Группа программ 1	j 2	گ 1	



## 11.2.2 Режим автоформирования среды

Режим автоформирования среды позволяет установить точный перечень процессов, запускаемых во время обычных действий пользователя на рабочей станции (запуск приложений, работа с документами, доступ к локальным и сетевым ресурсам), а также процессов, необходимых для работы ОС (в противном случае пользователь, к которому применено ограничение, не сможет работать в системе).

Для автоформирования среды выберите в окне создания групп программ (рисунок 11.9) **Режим автоформирования среды** и нажмите **Далее**.

В появившемся окне (рисунок 11.15) введите имя создаваемой группы и по кнопке сформируйте список пользователей, для которых будет осуществляться сбор сведений об используемых процессах (см. раздел *«Добавление пользователей или групп пользователей»*).



🗙 Создание группы программ					×
Задайте имя для г	руппы				
Во время работы автоформирования ограничений на запуск программ для выбранных пользователей не будет.					
Блокхост-Сеть будет вести наблюдение за тем, какие программы используют пользователи в ходе работы. На основании полученного списка программ может быть сформирована замкнутая программная среда.					
Имя группы программ	Группа программ 2				
Добавьте пользов	ателей, для которых будет вестис	ь отслежи	вание запуска	программ	
+ Q Поиск					
	Пользователи отсутству	ют			
		Назад		Отмена	

Рисунок 11.15 – Создание группы с автоформированием среды

По окончанию добавления пользователей сохраните группу программ и запустите режим автоформирования среды по кнопке **Запустить**. В списке категорий раздела **«Замкнутая программная среда»** появится созданная группа (рисунок 11.16) с указанием количества включенных в нее пользователей и запущенных процессов, выявленных в ходе работы пользователей.

Во время запуска режима автоформирования среды у выбранных пользователей не будет запрета на запуск процессов, но все запущенные процессы будут фиксироваться в журнале аудита.



На клиентских рабочих станциях под управлением OC Linux при автоформировании замкнутой программной среды могут возникать блокировки при перезагрузке и в процессе работы, так как некоторые системные приложения запускаются и работают из-под других пользователей,

которые не были добавлены в список пользователей ЗПС. В этом случае необходимо добавить разрешение на процесс вручную или добавить пользователя, из-под которого запускается процесс в список.

Х Бл	окост-Сеть 4	- 0	×
ቆ	Менеджер иерархий		
♦	С В С С • В О С С • В Секомпьютеры • С Группа 1 • С Группа 2 С Группа 3	PC1       Онлайн         Общее       Токены       Пользователь       Настройки*       События         X       Блоккост-Сеть       SafeNode         Дискрещиконный доступ       Замкнутая программная среда         Замкнутая программная       События	c
	Fig PC1	Контроль печати         С Изменить         Удалить         Остановить           Контроль целостности файлов с восстановлением         Иния группы         • Програмиы         Пользователи           Мандатный доступ         Группа программ 1         Е 2         & 1           Проверка парола в СЗИ         Группа программ 2         Е 0         & 1	

Рисунок 11.16 – Отображение группы с автоформированием среды

По прошествии времени, достаточного для анализа всех процессов, запускаемых в ходе работы пользователя, остановите режим автоформирования среды по кнопке <sup>О Остановить</sup> (рисунок 11.17) или выбором в контекстном меню группы **Завершить** автоформирование.

6 Find	жкост-Сеть 4					-	×
8	Менеджер иерархий						
<ul><li>◆</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li><li>○</li></ul>	<ul> <li>В В В В</li> <li>• В се компьютеры</li> <li>• Группа 3</li> <li>• Группа 3</li> <li>• Группа 2</li> </ul>	<ul> <li>₩18РКЮ7.diff.pki</li> <li>Общее Токены Пользов</li> <li>Х Блокост-Сеть SafeN</li> <li>Настройки клиента</li> <li>Дискреционный доступ*</li> <li>Замкоутая программиея среда*</li> <li>Контроль целостности файлов с востялов печати</li> </ul>	атель Настройки" Событ ode Замкнутая програм С Механизм включен С Механизм включен С Изменить © Удал Имя группы – Группа программ 1	ия мная среда амть <u>Остановит</u> Программы По 1 &	ъ ользователи 1		c
		Мандатный доступ	🗵 Группа программ 2	R 0 &	2		

Рисунок 11.17 – Остановка режима автоформирования среды

Появится окно со списком процессов, которые были запущены заданными в категории пользователями во время сеанса работы при включенном режиме автоформирования среды (рисунок 11.18).

При необходимости можно откорректировать сформированный список разрешенных к запуску процессов, сняв флаг с процессов, запуск которых должен быть запрещен.

🗙 Результат автоформирования	×					
Программы, запущенные полы	Программы, запущенные пользователями					
Выберите программы для замкнутой программной среды. 👌 Экспор						
Q. Поиск						
Название	Путь					
☑ 名 XPSRCHVW.EXE	C:\WINDOWS\SYSTEM32\XPSRCHVW.EXE					
	C:\WINDOWS\SYSTEM32\WLRMDR.EXE					
	C:\WINDOWS\SYSTEMAPPS\INPUTAPP_CW5N1H2TXYEWY\WIN					
☑ ► VM3DSERVICE.EXE	C:\WINDOWS\SYSTEM32\VM3DSERVICE.EXE					
	C:\WINDOWS\SYSTEM32\USERINIT.EXE					
Z 名 TASKHOSTW.EXE	C:\WINDOWS\SYSTEM32\TASKHOSTW.EXE					
☑ ᢓ SYSTEMSETTINGS.EXE	C:\WINDOWS\IMMERSIVECONTROLPANEL\SYSTEMSETTINGS.E>					
☑ ᢓ SVCHOST.EXE	C:\WINDOWS\SYSTEM32\SVCHOST.EXE					
	C:\WINDOWS\SYSTEMAPPS\MICROSOFT.WINDOWS.STARTMEN					
	C:\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE					
SMARTSCREEN.EXE	C:\WINDOWS\SYSTEM32\SMARTSCREEN.EXE					
Bcero: 45						
Отмена Заверши	ть без добавления Добавить в категорию (45)					

Рисунок 11.18 – Список программ, запущенных в режиме автоформирования среды

Важно отметить, что для любой группы программ, сформированной вручную стандартным режимом формирования ЗПС, возможно запустить автоформирование среды.

Для любой группы программ, сформированной в режиме автоформирования среды, можно добавить процессы вручную, открыв группу на редактирование.

После создания списка разрешенных процессов заданные в группе пользователи

## 72410666.00063-04 95 01-01

 $(\mathbf{i})$ 

230

смогут запускать только те процессы, которые добавлены в список. Запуск процессов, отсутствующих в списке разрешенных для пользователя будет запрещен.

# 11.3 Контроль печати

Механизм **«Контроль печати»** позволяет управлять расширенными возможностями контроля печати на клиентской рабочей станции, в частности: разграничение прав печати для указанных приложений, простановка специального колонтитула по шаблону печати для указанных приложений, ведение расширенного аудита печати.

Особенности настройки СЗИ для корректной работы механизма контроля печати описаны в Приложении 2 к настоящему документу.

Разграничение прав печати для указанных приложений реализуется путем формирования списка процессов с правом на печать на конкретной клиентской рабочей станции. Печать из процессов, не добавленных в список, будет невозможна.

Расширенный аудит позволяет выполнять аудит успешной печати из процессов, добавленных в список разрешенных к печати и/или аудит отказа от печати из процессов, не добавленных в сформированный список.

Простановка специального колонтитула по шаблону печати позволяет добавлять на страницы распечатываемого документа дополнительные сведения, настраиваемые по шаблону печати. Настроенный шаблон будет применен к распечатываемым документам из сформированного списка процессов с правом на печать, если установлена соответствующая настройка.

Если в клиентской политике для рабочей станции включен базовый аудит печати (раздел «Аудит печати») и расширенный контроль печати одновременно, настройки расширенного контроля печати действуют в приоритетном порядке.

По умолчанию в списке процессов с правом на печать добавлен элемент **Все процессы,** который подразумевает, что все процессы клиентской рабочей станции доступны к печати.

Для настройки расширенного контроля печати во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Контроль печати» (рисунок 11.19).



ХБло	окхост-Сеть 4						×
*	Менеджер иерархий						
* 18		Q C	Эте W101         Онлайн           Общее         Токены         Пользов           Х         Блокхост-Сеть         SafeN           Дискрецисновый доступ"         Замконутая программиная среда"         SafeN           Контроль целостности файлов с восстановлением         Контроль целостности файлов с восстановлением           Мандатный доступ         Проверка пароля в СЗИ           Пользователи с разрешением на вход в ОС         С	атель Настройки* События ode Контроль печати Механизм выключен Выполнять аудит успешной печати из проце Выполнять аудит отказа печати из проце Процессы с правом на печать Ф Удалить Наказник ВСЕ ПРОЦЕССЫ	Настроить шаблон печати роцессов, добавленных в список оссов, не добавленных в список шив	мон ]	c
				Bcero: 1			
0			United	<u> </u>			

Рисунок 11.19 – Контроль печати

Включите механизм контроля печати, установив переключатель в положение

Механизм включен и по кнопке сформируйте список процессов с правом на печать и (рисунок 11.20).



🔀 Добавление процессов/программ для контроля печати				
Приложения Запущенные процессы Файловая система				
Q. Поиск				
Название	Путь			
🗌 🛅 Все процессы				
BHNetDeploymentAgent				
▶ 🗌 🗿 SafeNet Authentication Client 10.3				
・ 🗌 🖹 VMware Tools				
Блокхост-Сеть Клиент				
Драйверы Рутокен				
ト 二 名 КриптоПро СSP				
Bcero: <b>50</b>				
		Отмена		

Рисунок 11.20 – Добавление процессов с правом печати

Во вкладке *Приложения* доступны к выбору все приложения, установленные на клиентской рабочей станции и поддерживаемые механизмом контроля печати.

Во вкладке **Запущенные процессы** доступны к выбору все процессы, запущенные зарегистрированными пользователями на клиентской рабочей станции (системные процессы, запущенные из-под системных учетных записей, не отображаются в списке).

Во вкладке **Файловая система** доступны к выбору файлы с расширением *ехе* из файловой системы клиентской рабочей станции.

При необходимости ведения расширенного аудита успешной печати из процессов, добавленных в список разрешенных к печати и/или аудита отказа от печати из процессов, не добавленных в сформированный список, установите соответствующие параметры Выполнять аудит успешной печати из процессов, добавленных в список и/или Выполнять аудит отказа печати из процессов, не добавленных в список.

Регистрируемое событие содержит:

дату и время совершенной печати (или попытки печати);

## 72410666.00063-04 95 01-01

233

- наименование принтера;
- имя пользователя, запустившего процесс печати;
- наименование рабочей станции;
- приложение из которого производилась печать;
- размер, количество страниц, наименование и метку документа.

## 11.3.1 Настройка шаблона печати

В СЗИ от НСД «Блокхост-Сеть 4» реализована возможность выборочной простановки специального колонтитула по шаблону при печати документов из списка сформированных процессов.

Настроенный шаблон будет применен к распечатываемым документам из сформированного списка процессов, если установлен соответствующий флаг *Шаблон* в строке с процессом.

При печати документа с использованием шаблона на каждой странице документа выводится специальный колонтитул, который может содержать следующие поля:

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

 порядковый номер в формате «текущий номер страницы из общего числа листов»;

- имя пользователя, производившего печать документа;
- имя рабочей станции, с которой производилась печать документа;
- имя принтера, с которого производилась печать документа.

Для настройки содержимого колонтитулов, выводимых при печати документа из процессов с правом на печать, перейдите в окно **Редактирование шаблона печати** по кнопке **Редактирование (**рисунок 11.21).



X Редактирование шаблона печати X					
Верхний колонти	итул				
Шрифт	Times New Roman	(12) 🖉			
Выравнивание	По правому краю				
Иетка докум	ента	"Метка докум	иента: <Мандат	гдокумента>"	
И Компьютер		Компьютер:	<Имя компью	тера>"	
🔽 Пользовател	ь	"Пользовател	ть: <Имя польз	ователя>"	
Иапечатано		Напечатано:	<Время>"		
🗾 Документ		Документ: <	Имя документа	a>"	
Нижний колонти	итул				
Шрифт	Times New Roman	(12) 🖉			
Выравнивание	По правому краю				
🗸 Страница		"Страница: <	Номер страни	цы>"	
ИЗ		"из <Количес	тво страниц>"		
🔽 Принтер		Принтер: <И	1мя принтера>	н	
				Отмена	Применить

Рисунок 11.21 – Настройка шаблона печати

Список маркеров шаблона печати и их описание:

## Верхний колонтитул:

– **Шрифт** – выбора шрифта, которым будет напечатан верхний колонтитул (шрифт, начертание, размер шрифта, эффекты и система письма).

- **Выравнивание** – каким образом верхний колонтитул будет размещен на странице (по левому краю, по центру, по правому краю).

– Метка документа – добавление в верхний колонтитул мандатной метки

235

документа, выводимого на печать. 12

- *Компьютер* – добавление в верхний колонтитул имени рабочей станции, с которой была произведена печать.

– **Пользователь** –добавление в верхний колонтитул имени пользователя, под учетной записью которого была произведена печать.

- **Напечатано** – добавление в верхний колонтитул даты вывода документа на печать.

– **Документ** – добавление в верхний колонтитул имени файла документа, который был отправлен на печать.

#### Нижний колонтитул:

– *Шрифт* – выбор шрифта, которым будет напечатан нижний колонтитул (шрифт, начертание, размер шрифта, эффекты и система письма).

- **Выравнивание** – каким образом верхний колонтитул будет размещен на странице (по левому краю, по центру, по правому краю).

 Страница – добавление в нижний колонтитул номера текущей страницы, выводимой на печать.

 из – добавление в нижний колонтитул общего количества страниц, отправленных на печать.

– *Принтер* – добавление в нижний колонтитул имени принтера, на котором производится печать.

При печати документа из списка процессов, разрешенных к печати, с использованием шаблона, документ будет выглядеть следующим образом (рисунок 11.22).

<sup>&</sup>lt;sup>12</sup> Обозначение мандатной метки документа и последующих маркеров можно оставить заданным по умолчанию, например: «*Метка документа:*», изменить или удалить, оставив поле пустым.

GIS ГАЗИНФОРМ СЕРВИС	СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками Верхний колонтитул	37
	Матка документя 1; Компьютер TESTUSER; Полькователь admin; Напачатаво 18:24-14 26-01-2021; Документ Таот пачати	
	Tearnewaw	
	Нижний колонтитул	
	1 Cryanness 1; no 1; Принтор CansPDF Wither	

Рисунок 11.22 – Печать документа с настроенным шаблоном

## 11.4 Контроль целостности файлов с восстановлением

Механизм **«Контроль целостности файлов с восстановлением»** позволяет своевременно обнаруживать и устранять несанкционированное изменение контролируемых объектов файловой системы путем их восстановления их резервных копий до исходного состояния.

Неизменность контролируемых файлов проверяется каждый раз при запуске СЗИ. Целостность поставленных на контроль файлов обеспечивается путем проверки контрольных сумм, вычисленных при постановке файлов на контроль. Период проверки контрольных сумм задается администратором безопасности на основе требований политики безопасности. При несоответствии полученных контрольных сумм файлов эталонным значениям происходит восстановление контролируемых файлов: файлы заменяются их исходными версиями из резервной папки.

Не рекомендуется ставить на контроль файлы большого объема (>500 Mb). Так как при периодической проверке вычисленных контрольных сумм файлов, в зависимости от используемого аппаратного обеспечения, возможно снижение производительности системы вплоть до некоторого «зависания» компьютера.



 Файлы нулевой длины (имеющие размер 0 байт) невозможно поставить на контроль целостности!

Для настройки параметров контроля и восстановления файлов во вкладке

*Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Контроль целостности файлов с восстановлением» (рисунок 11.23).

🗙 Бло	жхост-Сеть 4		– 🗆 X
윦	Менеджер иерархий		
<u>~</u> 	Менеджер иерархий В В С С • В В В С С • Все компьютеры • Іссаlhost	<ul> <li>W102 Онлайн</li> <li>Общее Токены Пользова</li> <li>Х. Блокхост-Сеть SafeNor</li> <li>Дискреционный доступ</li> <li>Замкнутая программная среда</li> <li>Контроль печати</li> <li>Контроль целостности файлов с восстановлением</li> <li>Мандатный доступ</li> <li>Проверка пароля в СЗИ</li> <li>Пользователи с разрешением на вход в ОС</li> </ul>	С тель Настройки События de
			Файлы контроля отсутствуют Добавить
ŝ		Применить Отмена	

Рисунок 11.23 – Контроль и восстановление файлов

По кнопке <sup>с</sup> сформируйте список файлов для постановки на контроль и включите механизм контроля и восстановления файлов, установив переключатель в положение Механизм включен .

Задайте периодичность проверки целостности файлов, установив время в параметре **Проверять каждые (чч:мм**). По умолчанию проверка целостности осуществляется каждые 2 часа.

По кнопкам 🖄 Импорт / 🖄 Экспорт доступен импорт/экспорт списка файлов для контроля и восстановления.

При необходимости фиксировать в журнале аудита выявленные изменения в контролируемых файлах и их восстановление, установите параметр **Формировать события аудита при нарушении целостности файлов.** 

При выявлении нарушений целостности в контролируемых файлах, если восстановить контролируемый файл в исходное состояние не удалось, возможно

## 72410666.00063-04 95 01-01

блокировать сессию пользователя установкой параметра **Блокировать сессию** пользователя, если не удалось восстановить файл.

Администратор может выполнить пересчет контрольных сумм файлов, в которых были выявлены нарушения, по кнопке <sup>(Э)</sup> Пересчитать контрольные суммы (рисунок 11.23).

После пересчета КС файлов, при последующей проверке целостности КС файлов соответствуют эталонным значениям, фиксация событий в журнале аудита не производится.

# 11.5 Мандатный доступ

Мандатный механизм разграничения доступа – это специфический режим контроля доступа пользователя к файловым ресурсам станции с помощью присвоения пользователям и ресурсам определенных меток – совокупности уровней доступа и категорий.

**Уровень доступа** – это числовое значение от 1 до 10, которое присваивается учетным записям пользователей и файловым ресурсам в соответствии с уровнем допуска пользователя или уровнем конфиденциальности ресурса (чем числовое значение уровня доступа больше, тем выше степень конфиденциальности). По умолчанию всем пользователям и ресурсам присваивается уровень доступа 0.

*Категория* – это символьное значение от A до L, которое позволяет задать ограничения на доступ пользователей к файловым ресурсам не иерархически, а напрямую, сопоставлением категории пользователя и категории ресурса.

Принципы разграничения доступа при использовании уровней доступа:

 если уровень доступа пользователя совпадает с уровнем доступа ресурса (УДп=УДР), то пользователь получает <u>полный доступ</u> к ресурсу;

если уровень доступа пользователя меньше уровня доступа ресурса (УДп<УД<sub>Р</sub>),
 то пользователь получит доступ только на <u>запись</u>, но не получит доступ на чтение, в
 том числе и на просмотр содержимого ресурса;

 если уровень доступа пользователя выше уровня доступа ресурса (УД<sub>П</sub>>УД<sub>Р</sub>), то пользователь получит права <u>чтения</u> и <u>просмотра</u> ресурса, но не получит право на запись.

При определении уровня доступа ресурса соблюдается правило наследования: все вложенные в него объекты (любой степени вложенности) получают тот же уровень только в том случае, если им не определен никакой другой уровень.

Принцип разграничения доступа при назначении категорий:

– если категория, назначенная пользователю, включают в себя все категории ресурса (КП=КР), то пользователь получает <u>полный доступ</u> к ресурсу;



 если категория, назначенная пользователю, не совпадает с категорией ресурса (КП≠КР), то пользователь не имеет доступ к ресурсу.

Пользователь или ресурс может иметь только один уровень доступа, и неограниченное число категорий.

Мандатное разграничение доступа заключается в сопоставлении метки, присвоенной пользователю (комбинация уровня доступа пользователя и доступных ему категорий) метке файлового ресурса:

 если уровень доступа пользователя не меньше уровня доступа ресурса, к которому выполняется попытка доступа, и категории, доступные пользователю, включают в себя все категории ресурса, то пользователь получит права <u>чтения</u> и <u>просмотра</u> ресурса;

 если уровень доступа пользователя совпадает с уровнем доступа ресурса и категория, назначенная пользователю, включают в себя все категории ресурса, то пользователь получает <u>полный доступ</u> к ресурсу.

Для настройки мандатного механизма разграничения доступа во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Мандатный доступ» (рисунок 11.24).

X En	окхост-Сеть 4		- 🗆 X
ಹಿ	Менеджер иерархий		
↓ 10 ■	C: B d d Q C - Et W101 - D Bce xoansworepus - Iocalhost	••••••••••••••••••••••••••••••••••••	Сатель Настройки" События tode Мандатный доступ & Импорт & Экспорт Механизма выколючен Уровния доступа!Категории Пользователи Каталоги Устройства Раз С Уровния доступа!Категории Пользователи Каталоги Устройства Раз С Каталоги Сизаение данные 2 Конфиденцикальные данные 3 Персональные данные 3 Персональные данные 3 С Секретно 3 Красональные данные 3 С Сонфиденцикальные данные 3 Красональные данные 3 С Конфиденцикальные данные 3 С Секретно 3 С Секретно
		Применить Отмена	Эленный
٢			

Рисунок 11.24 – Настройка мандатного механизма

Включите мандатный механизм, установив переключатель в положение С Механизм включен

## 11.5.1 Справочник уровней доступа и категорий

Вкладка *Уровни доступа/Категории* представляет собой справочник уровней и категорий, доступных к назначению для пользователей и файловых ресурсов.

По умолчанию в справочнике уровней доступа уже созданы 5 уровней доступа, в справочнике категорий созданы 5 категорий (рисунок 11.24).

Уровень доступа Открытые данные со значением **1** недоступен для удаления. Этому уровню доступа по умолчанию сопоставляются все ресурсы (объекты файловой системы жестких дисков и подключаемых накопителей), которые присутствуют на рабочей станции в момент установки клиентской части СЗИ.

Для добавления уровня доступа или категории в справочник в области **Уровни** *доступа/Категории* нажмите кнопку <sup>• Добавить</sup> .

При добавлении уровня доступа появится окно **Создание уровня доступа** в котором задается наименование уровня доступа и выбирается из списка числовое значение, соответствующее добавляемому уровню (рисунок 11.25). При этом в списке числовых значений не будут отображаться числа уже заведенных в справочнике уровней.

💢 Создание уровня доступа	×
Имя уровня доступа	
Цифра 2 т	
Отмена	

Рисунок 11.25 – Создание уровня доступа

При добавлении категории появится окно **Создание категории** в котором задается наименование категории и выбирается из списка символьное обозначение категории (рисунок 11.26). При этом в списке символьных обозначений не будут отображаться символы уже заведенных в справочнике категорий.



X Создание категории		×
Имя категории		
[ ] 5		
Буква Синий	Ŧ	
	Отмена	

Рисунок 11.26 - Создание категории

## 11.5.2 Присвоение меток пользователям

Для работы с конфиденциальными ресурсами пользователи должны иметь соответствующую метку, задаваемую комбинацией числового значения уровня доступа и множеством категорий. Метка присваивается пользователю в разделе «Мандатный доступ» во вкладке *Пользователи*.

По умолчанию в списке пользователей добавлен псевдоним **Все пользователи** с присвоенной меткой с уровнем доступа **1** без назначенных категорий, означающий, что все локальные и доменные пользователи клиентской рабочей станции имеют доступ ко всем ресурсам с аналогичным уровнем доступа.

Для добавления пользователя в список нажмите кнопку <sup>• Добавить</sup> (рисунок 11.27) и в появившемся окне (см. раздел *«Добавление пользователей или групп пользователей»*) добавьте учетную запись локального или доменного пользователя, которому необходимо присвоить метку.

GIS	ГАЗИНФОРМ СЕРВИС		СЗИ от НСД «Бло Руководство адми Управление полит	кхост-Сеть 4» нистратора безопасности. Часть 1 гиками	243
Х Бло	жжет-Сеть4 Менеджер иерархий				- 0 X
ф.	C1 8 8 8 8	Q C	🖬 PC1 Онлайн 🔹		c
8	<ul> <li>новина</li> <li>Все компьютеры</li> <li>Со болого 1</li> </ul>		Общее Токены Пользов Х Блокхост-Сеть 🖇 SafeNod	атель Настройки <sup>*</sup> События	
	<ul> <li>Pynna 1</li> <li>Pynna 2</li> <li>Pynna 3</li> </ul>		Дискреционный доступ Замкнутая программная среда"	Мандатный доступ Механизм включен	🛓 Импорт 👌 Экспорт
	PC1		Контроль печати	Уровни доступа\Категории Пользователи*	Каталоги Устройств
			Контроль целостности файлов с восстановлением Мандатный доступ"	<ul> <li>Q. Поиск</li> <li>Э. Добавить В. Удалить</li> <li>Учетная запись * Уровень доступа</li> </ul>	Категории
			Проверка пароля в СЗИ	aos Все пользователи 💿 1 Открытые данни	ые
			Пользователи с разрешением на вход в ОС	pki.local\user02 Ø 1 Открытые данни	ые 00

Рисунок 11.27 – Добавление пользователей

Для назначения метки пользователю выберите в списке пользователя, которому нужно назначить метку и нажмите <sup>В назначить метку</sup>. В появившемся окне (рисунок 11.28) выберите из списка уровень доступа и по кнопке **Выбрать** добавьте категории, разрешенные пользователю.

🗙 Назначение метки	×
Учетная запись 💽 diff.pki\user01	
Уровень доступа	
Открытые данные	•
Категории	
Выбрать 🕒 Оранжевый 🗙 🧿 Желтый 🗙	
О Зеленый ×	
Наризиить Отмена	
Отмена	

Рисунок 11.28 – Назначение пользователю уровня доступа и категорий

## 11.5.3 Сопоставление меток каталогам

Для разграничения доступа к каталогам (файловым объектам и логическим дискам), необходимо присвоить им соответствующую метку, задаваемую комбинацией числового значения уровня доступа и множеством категорий. Метка присваивается в разделе **«Мандатный доступ»** во вкладке *Каталоги*.

По умолчанию в списке каталогов добавлен элемент **Все каталоги** с присвоенной меткой с уровнем доступа **1** без назначенных категорий, подразумевающий под собой

## 72410666.00063-04 95 01-01

все логические диски с расположенными на них объектами (файлами и каталогами), которые доступны пользователю при работе в операционной системе.

Метка присвоенная каталогу автоматически распространяется и на вложенные в него объекты (файлы и каталоги). Для изменения метки вложенных объектов необходимо явно присвоить им необходимую метку.

Для добавления каталога в список нажмите кнопку <sup>Э добавить</sup> (рисунок 11.29) и в появившемся окне добавьте файловый объект, которому необходимо присвоить метку.

ХБл	окост-Сеть 4		- 0
ጽ	Менеджер иерархий		
ا¢ 8	С: В Д Д Q C • В w09w13 • □ Все компьютеры	<ul> <li>РСІ Онлайн •</li> <li>Общее Токены Пользов</li> <li>Х блоккост-Сеть SafeNor</li> </ul>	атель <mark>Настройки"</mark> События de
	<ul> <li>C [pynna 1</li> <li>C [pynna 2</li> <li>C [pynna 3</li> </ul>	Дискреционный доступ Замкнутая программная среда"	Мандатный доступ 🕹 Импорт 👌 Экспор
	FE PC1	Контроль печати Контроль целостности файлов	Уровни доступа\Категорни Пользователи* Каталоги* Устройств С Q. Поисс 3
		Мандатный доступ"	<ul> <li>Добавить छ Удалить</li> <li>Каталог * Уровень доступа Категории Аудиг</li> </ul>
		проверка парола в СЗИ	🖹 Все каталоги 🥥 1 Открытые данные

Рисунок 11.29 – Добавление каталогов и файловых объектов

Для назначения метки выберите в списке каталог или файловый объект, которому нужно назначить метку и нажмите <sup>В назначить метку</sup>. В появившемся окне (рисунок 11.30) выберите из списка уровень доступа, и по кнопке **Выбрать** добавьте категории, сопоставляемые выбранному ресурсу.

🗙 Назначение метки	×
Каталог 🗀 С:\Тетр	
Уровень доступа Л Открытые данные Категории Выбрать В Оранжевый × С Желтый × Э Зеленый ×	Ŧ
Назначить Отмена	

Рисунок 11.30 – Сопоставление уровня доступа и категорий выбранному каталогу

При необходимости фиксировать в журнале аудита доступ к заданному каталогу, установите параметр *Аудит* в строке с требуемым ресурсом (рисунок 11.29).

Особенности работы с жесткими и символьными ссылками при настройке мандатного механизма разграничения доступа описаны в Приложении 1 к настоящему документу.

## 11.5.4 Сопоставление меток устройствам

Для разграничения доступа к USB-устройствам, необходимо присвоить им соответствующую метку, задаваемую комбинацией числового значения уровня доступа и множеством категорий. Метка присваивается в разделе **«Мандатный доступ»** во вкладке *Устройства*.

Устройства во вкладке структурированы по следующим классам USB-устройств:

устройства хранения данных (съемные USB-носители);

• переносные устройства (WPD-устройства: телефоны, фотокамеры, музыкальные проигрыватели).

По умолчанию в списке устройств добавлены элементы **Все устройства хранения данных** и **Все переносные устройства** с присвоенной меткой с уровнем доступа **1** без назначенных категорий, подразумевающий под собой все USB-устройства с расположенными на них объектами (файлами и каталогами), которые доступны пользователю.

Для добавления устройства в список нажмите кнопку <sup>• Добавить</sup> (рисунок 11.31) и в появившемся окне (рисунок 11.32) добавьте устройство, которому необходимо присвоить метку.



Рисунок 11.31 – Вкладка Устройства

🗙 Изменение параметров разрешенного устройст	ва		Х
Все устройства 🔹 🔍			C
Имя	≜ Вид	Идентификатор Серийный номер	
<ul> <li>Устройства хранения данных</li> </ul>			
<ul> <li>Multiple Card Reader USB Device - 1</li> </ul>	Модель	VID_058f PID_63	
Multiple Card Reader USB Device	Экземпляр	VID_058f PID_63 058F63666438	
🔹 📋 Generic Flash Disk USB Device - 1	Модель	VID_058f PID_63	
Generic Flash Disk USB Device	Экземпляр	VID_058f PID_63 851FE7CC	
<ul> <li>StoreJet Transcend USB Device - 1</li> </ul>	Модель	VID_152d PID_2	
StoreJet Transcend USB Device	Экземпляр	VID_152d PID_2 322849ABA163	

Рисунок 11.32 – Добавление устройств

Для назначения метки выберите в списке устройство, которому нужно назначить метку и нажмите <sup>В назначить метку</sup>. В появившемся окне (рисунок 11.33) выберите из списка уровень доступа, и по кнопке **Выбрать** добавьте категории, сопоставляемые выбранному устройству.

🔀 Назначение метки	×
Устройство 📋 Multiple Card Reader USB Device	
Уровень доступа	
Э Персональные данные	r
Категории	
Выбрать 🕒 Оранжевый 🛛 🧿 Желтый 🗙	
	_
Назначить Отмена	

Рисунок 11.33 – Сопоставление уровня доступа и категорий выбранному устройству

При необходимости фиксировать в журнале аудита доступ к заданному устройству, установите параметр *Аудит* в строке с требуемым устройством (рисунок 11.31).

## 11.5.5 Разделяемые файлы

Некоторые приложения (например, приложения, входящие в пакет программ Microsoft



Office: Microsoft Word, Microsoft Excel), для улучшения быстродействия своей работы и с целью сохранности данных создают временные файлы. Для работы с такими временными файлами, приложениям, создавшим их, требуется полный доступ к файлам и каталогам, в которых эти файлы создаются, независимо от мандатной метки вошедшего пользователя.

Для предоставления приложениям доступа к таким файлам и каталогам необходимо присвоить им **динамическую мандатную метку**, равную мандатной метке вошедшего пользователя путем добавления таких файлов и каталогов в список раздела **«Мандатный доступ»** во вкладке **Разделяемые файлы** (рисунок 11.34). В результате такого назначения приложения получат полный доступ к добавленным файлам и каталогам, независимо от мандатной метки родительского ресурса.

5.nc	xxxxxr-Cens 4			- 0
	Менеджер иерархий			
	다 홈 레 레 Q C • 팀 v18PK07	₽ w18PK007.diff.pki Онлайн Ф Общее Токены Пользов	атель Настройки" События	(
	Bce компьютеры     D    Epyrna 1     W18PK007.dff.pki	🗶 Блоккост-Сеть 👂 Safe Настройки клиента	Node Мандатный доступ	🛓 Импорт 👌 Экспор
	<ul> <li>C Fpynna 3</li> <li>C Fpynna 2</li> </ul>	Дискреционный доступ* Замюнутая программиная среда*	Механизм включен Уровни доступа/Категории Пользователи" Каталоги" Устройств	а Разделяемые файлы!
		Контроль печати Контроль целостности файлов с восстановлением	О, Поиск © Добавить • 👿 Удалить Путь к файлам/паткам	🛓 Импорт 👌 Экспор * Аздин
		Мандатный доступ <sup>+</sup> Проверка пароля в СЗИ	C\BlockHost\Backup\BlockHost\System32\BhDiskMon.sys	

Рисунок 11.34 – Добавление разделяемых файлов

Для определения файлов и каталогов, доступ к которым требуется приложениям, необходимо предоставить возможность работы клиентской рабочей станции в мягком режиме (раздел *«Мягкий режим работы»*) в течении времени, достаточного для выполнения пользователем своих обычных операции на рабочей станции (запуск приложений, работа с документами, доступ к локальным и сетевым ресурсам).

Во время работы в мягком режиме в журнале аудита фиксируются все запрещенные попытки доступа к ресурсам. На основании анализа событий журнала аудита клиентской рабочей станции, администратор безопасности выявляет список файлов и каталогов, доступ к которым требуется приложениям, и вносит их в список разрешенных во вкладке **Разделяемые файлы**.

Добавление файлов и каталогов в список разрешенных доступно:

 по кнопке <sup>• добавить</sup> (рисунок 11.34) выбором необходимых файлов в окне добавления файлов (рисунок 11.4);

вручную по кнопке Добавить вручную (рисунок 11.35) вводом пути к нужному



## файлу или каталогу (рисунок 11.36);

с помощью импортирования сформированного списка по кнопке <sup>ч</sup> Импорт (рисунок 11.37).

X En	okxocr-Ceni 4			- 0 X
å	Менеджер иерархий			
*	다 용 최 리 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	🛱 РСІ Онлайн 🔹 Общее Токены Пользов	ызтель Настройки" События	c
70	<ul> <li>Все компьютеры</li> <li>Группа 1</li> <li>Группа 2</li> </ul>	🗶 Блоккост-Сеть 💋 Sat Дискреционный доступ	feNode Мандатный доступ	<ol> <li>Импорт &amp; Экспорт</li> </ol>
	C) (pynna) 🖬 PCI	Замкнутая программная среда" Контроль печати	Меканном включен Уровни доступа\Категории Пользователи* Каталоги* Устройства	Разделяемые файлы" 🗘
		Контроль целостности файлов с восстановлением Мандатный доступ"	О, Поисх © Добавить + 🛛 Удалить	🛓 Импорт 👌 Экспорт
		Проверка пароля в СЗИ	Crys s dailoas/hamase	- Appen

Рисунок 11.35 – Добавление разделяемых файлов вручную

🔀 Ручное добавление	×
Введите нужные пути вручную и нажмите на кнопку "Добавить"	
🕀 Добавить 🔟 Удалить	
Путь к файлу	
C:\temp.exe	
Отмена Добавить	

Рисунок 11.36 – Ввод пути к разделяемому файлу или каталогу вручную



🗙 Импорт файлов	×
Q. Поиск	
✓ Выбрать всё ☐ Снять всё	
Путь	▼ Аудит
C:\pagefile.sys	
Bcero: 1	
Отмена	Імпортировать (1)

Рисунок 11.37 – Импорт списка разделяемых файлов и каталогов

По кнопке 🖄 Экспорт возможен экспорт сформированного списка файлов и каталогов, доступ к которым требуется в работе приложений.

При необходимости фиксировать в журнале аудита доступ к файлу или каталогу из списка, установите параметр *Аудит* в строке с требуемым ресурсом (рисунок 11.34).

# 11.5.6 Ограничения при использовании мандатного разграничения доступа

Содержимое <u>каталогов</u> с временными файлами затирается по завершению сеанса работы пользователя. Необходимо быть внимательным при настройке этого механизма, чтобы в процессе работы СЗИ не была удалена нужная информация и не нарушилась работа установленных в системе приложений.

Разделяемые файлы и каталоги доступны к добавлению в список разрешенных только с системных дисков.

При использовании мандатного разграничения сетевой доступ на устройства хранения данных блокируется во избежание утечки информации.

При запуске приложений под учетной записью другого пользователя (использование команды *RunAs*), сессия запускается с мандатной меткой текущего пользователя.

Во избежание утечки информации администратор обязан:

– установить на контроль целостности все <u>файлы</u>, добавленные в список



разделяемых файлов (постановка файлов на контроль целостности описана в разделе Контроль целостности файлов с восстановлением);

 настроить запрет на доступ ко всем <u>устройствам</u>, кроме USB-устройств классов
 Устройства хранения данных, Переносные устройства и Устройства ввода (настройка запрета на доступ к устройствам описана в разделе Контроль устройств).

# 11.6 Проверка пароля в СЗИ

Раздел «Проверка пароля в СЗИ» позволяет задать список пользователей, для которых будет задействован особый режим аутентификации – вход по паролю. В этом случае доменный или локальный пароль пользователя при первом входе пользователя сохраняется в базу данных СЗИ, и при последующих входах пользователя введенный пароль сверяется с копией, хранящейся в базе данных СЗИ. Если введенный и сохраненный в БД пароли не совпадают, пользователю будет отказано во входе.



Настройка проверки пароля В СЗИ для клиентских рабочих станций под управлением ОС семейства Linux аналогична проверке для ОС семейства Windows приведенной в данном разделе.

Установить настройки входа пользователя по паролю возможно только в том случае, если вышестоящим сервером установлено разрешение на данную настройку в разделе **«Управление входом в ОС»** клиентской политики (подробное описание приведено в пункте **«Управление настройками входа»**).

Для настройки входа пользователя по паролю во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Проверка пароля в СЗИ» (рисунок 11.38).

🗙 Бло	жхост-Сеть 4			_	o x
ጽ	Менеджер иерархий				
кĴя		🔂 W102 Онлайн			C
ř	<ul> <li>Т W102</li> <li>Bce компьютеры</li> <li>Iocalhost</li> </ul>	Общее Токены Пользов Х Блокхост-Сеть SafeNo	атель Настройки* События de		
		Дискреционный доступ Замкнутая программная	Проверка пароля в СЗИ Э добавить 🗠 Сброс пароля 🗑 Удали	Ть	
		среда Контроль печати	Пользователь	<ul> <li>Тип</li> <li>Ломенный пользователя</li> </ul>	
		Контроль целостности файлов с восстановлением Мамаатный аостого		доменный пользователе	
		Проверка пароля в СЗИ*			
		Пользователи с разрешением на вход в ОС			
E			Bcero: 1		
ŝ		Применить Отмена			

Рисунок 11.38 – Настройка аутентификации по паролю

Для добавления пользователей по кнопке <sup>• Добавить</sup> сформируйте список пользователей которым необходимо установить возможность входа по паролю (см. раздел *«Добавление пользователей или группы пользователей»*) и нажмите *Добавить*.

• В разделе «Проверка пароля в СЗИ» можно добавлять в список только отдельных пользователей, входа по паролю для группы пользователей недоступен.

Для всех пользователей в списке будет принудительно включен режим входа по паролю с сохранением копии пароля в базе данных СЗИ, даже если клиентскими политиками предписан иной тип аутентификации на клиентской рабочей станции.

Администратор имеет возможность выполнить сброс пароля пользователя, сохраненного в БД СЗИ, по кнопке Сброс пароля (рисунок 11.38). Необходимость сброса пароля может возникнуть в случае ошибки при синхронизации текущего пароля, предъявляемого пользователем при входе, с паролем пользователя, сохраненным в БД СЗИ.

После выполнения операции сброса пароля (рисунок 11.39) автоматически запустится

## 72410666.00063-04 95 01-01

251



мастер синхронизации паролей и при первом входе пользователя в OC, предъявленный им пароль будет записан в БД СЗИ.

🗙 Сброс пароля 🛛 🗙	
Текущий пароль пользователя Блокхост-Сети будет сброшен	
Пользователь сможет изменить текущий пароль при входе	
Сбросить	Отмена

Рисунок 11.39 – Сброс пароля пользователя

# 11.7 Пользователи с разрешением на вход в ОС

Раздел «Пользователи с разрешением на вход в OC» позволяет задать список пользователей, которым будет предоставлена возможность входа на клиентскую рабочую станцию. Пользователям, не добавленным в список, при попытке входа на клиентскую рабочую станцию будет отказано во входе.

Задать ограничивающий список пользователей возможно только в том случае, если вышестоящим сервером установлено разрешение на данную настройку в разделе «Управление входом в ОС» клиентской политики (подробное описание приведено в пункте «Управление настройками входа»).

Для создания ограничивающего списка пользователей во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *Блокхост-Сеть* в раздел «Пользователи с разрешением на вход в ОС» (рисунок 11.40).
🗙 Бло	кхост-Сеть 4		- 🗆 X
ጽ	Менеджер иерархий		
кĴя		🔁 W102 Онлайн ●	C
ŕÐ	<ul> <li>П Все компьютеры</li> </ul>	Общее Токены Пользов	атель <mark>Настройки*</mark> События
٦	ि localhost	Дискреционный доступ Замкнутая программная	Пользователи с разрешением на вход в ОС Q. Поиск
		среда Контроль печати	О Добавить         Удалить         & Автодобавление         У Импорт         Экспорт
		Контроль целостности файлов с восстановлением	ж Все пользователи
		Мандатный доступ	
		Проверка пароля в СЗИ*	
		Пользователи с разрешением на вход в ОС	
Ē			Bcero: Все пользователи
ŝ		Применить Отмена	

Рисунок 11.40 – Создание ограничивающего списка пользователей для рабочей станции

По умолчанию в ограничивающем списке пользователей добавлен псевдоним **Все пользователи**, который подразумевает, что все локальные и доменные пользователи имеют возможность входа на клиентскую рабочую станцию.

По кнопке сформируйте список пользователей которых необходимо внести в ограничивающий список (см. раздел *«Аутентификация по цифровому сертификату на токене»*).

По кнопке <sup>® детодобавление</sup> возможно сформировать ограничивающий список пользователей из списка пользователей, когда либо осуществлявших вход на клиентскую рабочую станцию (рисунок 11.41).



СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

🔀 Автодобавление в ограничивающий список 🛛 🕹 🗙						
Пользователи, когда-либо использовавшие компьютер						
Выберите пользователей, которых необход	Выберите пользователей, которых необходимо добавить в ограничивающий список					
Q. Поиск						
🖉 Выбрать все 🗍 Снять все						
Учетная запись	⊾ Тип					
DIFF\Administrator	Active Directory					
DIFF\serviceCA3	Active Directory					
DIFF\serviceCA_vam	Active Directory					
DIFF\testaib	Active Directory					
	Active Directory					
w18PKI07.diff.pki\testlocal	Локальный пользователь					
Bcero: 6						
	Отмена	Добавить (2)				

Рисунок 11.41 – Автодобавление в ограничивающий список пользователей

По кнопкам 坐 Импорт / 🖄 Экспорт возможен импорт сформированного ранее списка или экспорт созданного списка пользователей.

#### 11.8 Пользователи СДЗ

Раздел **«Пользователи СДЗ»** позволяет удаленно управлять разблокировкой пользователей на клиентских рабочих станциях с установленным СДЗ «SafeNode System Loader», заблокированных после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей.

Для разблокировки пользователей СДЗ во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *SafeNode* в раздел «Пользователи СДЗ» (рисунок 11.42).

Менеджер иерархий	×
<ul> <li>В се компьютеры</li> <li>В</li></ul>	
User 6_430a25e90c33976118eb86c          User 5_430a25e90c33976118eb86c          User 4_430a25e90c33976118eb86c          User 3_430a25e90c33976118eb86c          User 3_430a25e90c33976118eb86c          User 4_430a25e90c33976118eb86c          User 4_430a25e90c33976118eb86c          User 1_430a25e90c33976118eb86c          User 19          User 18          User 17	C
Всего: 20	

Рисунок 11.42 – Разблокировка пользователей СДЗ

В списке пользователей отобразятся все пользователи, добавленные на клиентских рабочих станциях с установленным СДЗ «SafeNode System Loader».

В строке пользователя, заблокированного в результате выявленных нарушений КЦ или ошибок в процессе идентификации и аутентификации, отобразится статус **Заблокирован**. Для разблокировки пользователя нажмите на кнопку

После разблокировки при входе на рабочую станцию до загрузки ОС пользователю будет доступен ввод идентификационных и аутентификационных данных в соответствии с назначенной политикой аутентификации.

## 11.9 Сетевой адаптер UEFI

Раздел «Сетевой адаптер UEFI» позволяет настроить на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» сетевой адаптер UEFI для взаимодействия клиента и сервера LDAP при выборе способа получения сетевых настроек статически.

Задать настройки сетевого адаптера возможно только в том случае, если вышестоящим сервером установлено разрешение на данную настройку в разделе «Сетевой адаптер UEFI» политики SafeNode System Loader (подробное описание приведено в пункте «Сетевой адаптер UEFI» политики SafeNode System Loader).

#### 72410666.00063-04 95 01-01

Если в политике SafeNode System Loader не установлено разрешение настройка сетевого адаптера будет недоступна (рисунок 11.43).



Рисунок 11.43 – Настройка сетевого адаптера недоступна

Для настройки сетевого адаптера во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *SafeNode* в раздел «Сетевой адаптер UEFI» и включите настройку сетевого адаптера, установив переключатель в положение — Настроить сетевой адаптер (рисунок 11.44).

Введите вручную в настройках клиентской рабочей станции IP-адрес, маску подсети и шлюз в соответствующих полях и нажмите кнопку *Применить* (рисунок 11.44).

Х Бло	жхост-Сеть 4				_	×
*	Менеджер иерархий					
◆ 80 E		••••••••••••••••••••••••••••••••••••	натель Настрой же Сетевой а, Геневой а	ол События даптер UEFI ть сетевой адаптер 10.80.9.30 255.255.255.0 10.80.92.54		°
0						

Рисунок 11.44 – Настройка сетевого адаптера

После установки настроек сетевого адаптера получение сетевых настроек клиентской рабочей станцией будет осуществляться по заданному статическому IP-адресу и параметрам.

# 11.10 Проверка пароля в SafeNode

Раздел **«Проверка пароля в SafeNode»** позволяет задать список пользователей, для которых будет задействован особый режим аутентификации – вход по паролю. В этом случае пароль доменного или локального пользователя SafeNode при первом входе сохраняется в базу данных СДЗ, и при последующих входах пользователя введенный пароль сверяется с копией, хранящейся в базе данных СДЗ. Если введенный и сохраненный в БД пароли не совпадают, пользователю будет отказано во входе.

Настройка проверки пароля в SafeNode доступна только в случае, если на клиентской рабочей станции установлено и взято под управление СДЗ «SafeNode System Loader». При отсутствии СДЗ на клиентской рабочей станции настройка будет невозможна (рисунок 11.45).

СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

**i** 

Добавление пользователей в раздел «Проверка пароля в SafeNode» включает у пользователя проверку пароля, но не добавляет пользователя в список доступа на рабочую станцию. Для входа доменных пользователей и пользователей SafeNode System Loader по паролю необходимо добавить пользователей в список раздела политики «Управление аутентификацией» без дополнительных настроек аутентификации (подробное описание добавления пользователей в политику описано в разделе «Добавление доменных пользователей и пользователей SafeNode System Loader»).

🔀 Блоккост-Сеть 4		-	×
& Менеджер иерархий			
Менеджер иерархий	Image: State with the state		С
(b)	Применить		

Рисунок 11.45 – Настройка проверка по паролю SafeNode недоступна

Установить настройки входа пользователя по паролю возможно только в том случае, если вышестоящим сервером установлено разрешение на данную настройку в разделе **«Управление аутентификацией»** клиентской политики (подробное описание приведено в пункте **«Управление аутентификацией»**) (рисунок 11.46).



259

С

Пользователи СДЗ (Средства доверенной загрузки) Сетевой адаптер UEFI Проверка пароля в SafeNode Пользователи с разрешением на вход в ОС	Проверка пароля в SafeNode
 Применить Отмена	

Рисунок 11.46 – Механизм проверки пароля выключен в политике

Для настройки входа пользователя по паролю во вкладке Настройки клиентской рабочей станции перейдите во вкладку SafeNode в раздел «Проверка пароля в SafeNode» (рисунок 11.47).



Рисунок 11.47 – Настройка аутентификации по паролю

Для добавления пользователей по кнопке <sup>О Добавить</sup> сформируйте список пользователей которым необходимо установить возможность входа по паролю.

При добавлении локальных пользователей SafeNode, после нажатия кнопки **Далее**, (рисунок 11.48) необходимо задать пароль для пользователей (рисунок 11.49).

\$ \$

Доласны Компьютеры             С             Пользователи             Пользователя	<b>IS</b> сервис		СЗИ от Н Руководи Управле	НСД «Блокхост-Сеть 4» ство администратора безопасности. Часть 1 ние политиками	
Домены Компьютеры       С         Image: Comment C	🗙 Добавление пользователей				
Image: Imag	Домены Компьютеры	С	Пользователи	Будут добав	лены - 1
	₩102	6	Q. Поиск	o user1 W102 (Sat	ieNode)
SafeNode			Имя	▲ Тип пользователя	
			🗹 🏂 user1	SafeNode	
bcelo, 1 bcelo, 1	Bcero: 1		Bcero: 1		
				Далее	Отмена

Рисунок 11.48 – Добавление пользователя SafeNode

С помощью переключателя в верхней части вкладки можно выбрать единый пароль для всех добавляемых пользователей SafeNode (рисунок 11.49 а) или установить отдельный пароль для каждого пользователя (рисунок 11.49 б).

Задайте пароли для пользова	Задайте пароли для пользователей SafeNode. Пароль будет изменен при первом входе.					
п задания пароля 🦲 Один д	иля всех пользователей 🔵 Отдел	ьный для каждого пользователя		Новый пароль		
8	Тип					
🗴 User 16	SafeNode			Повтор пароля		
S User 17	SafeNode					
S User 18	SafeNode					
ro: 3						
			· · ·			
			Назад	Добавить	Отмена	



СЗИ от НСД «Блокхост-Сеть 4» Руководство администратора безопасности. Часть 1 Управление политиками

пользователей    Отдельный для каж, Пароль Введите пароль Введите пароль	ого пользователя Повтор пароля	ароль	Tun O Cristian	
Введите пароль	<ul> <li>Повторите г</li> </ul>	тароль	C-C-N-J-	
Введите пароль			SaleNode	
	• Повторите г	пароль	O SafeNode	
Введите пароль	<ul> <li>Повторите г</li> </ul>	тароль	<ul> <li>SafeNode</li> </ul>	
	Введите пароль	Введите пароль 💿 Повторите г	Введите пароль	Введите пароль SafeNode

б)

Назад

Рисунок 11.49 – Задание пароля для пользователей SafeNode

После добавления пользователей нажмите Добавить (рисунок 11.50).

262

Отмена

🗙 Бло	окхост-Сеть 4				_	×
ጽ	Менеджер иерархий					
÷. ₽	Менеджер иерархий □ : ::::::::::::::::::::::::::::::::::	<ul> <li>Шизаранная</li> <li>Общее Токены Пользова</li> <li>Блокхост-Сеть SafeNo</li> <li>Блокхост-Сеть SafeNo</li> <li>Пользователи СДЗ (Средства доверенной загрузки)</li> <li>Сетевой адаптер UEFI</li> <li>Проверка пароля в SafeNode*</li> <li>Пользователи с разрешением на вход в ОС</li> </ul>	атель Настройки* События de Проверка пароля в SafeNode	Тип SafeNode Доменный		C
(j) (j)		Применить Отмена	Bcero: 2			

Рисунок 11.50 – Добавление пользователям аутентификации по паролю

Для всех пользователей в списке будет принудительно включен режим входа по паролю с сохранением копии пароля в базе данных СДЗ, даже если клиентскими политиками предписан иной тип аутентификации на клиентской рабочей станции.

Администратор имеет возможность выполнить сброс пароля пользователя, сохраненного в БД СДЗ, по кнопке Сброс пароля (рисунок 11.50). Необходимость сброса пароля может возникнуть в случае ошибки при синхронизации текущего пароля, предъявляемого пользователем при входе, с паролем пользователя, сохраненным в БД СДЗ.

После выполнения операции сброса пароля (рисунок 11.51) автоматически запустится мастер синхронизации паролей и при первом входе пользователя в ОС, предъявленный им пароль будет записан в БД СДЗ.

263

🗙 Бло	жхост-Сеть 4				- 1	×
ጽ	Менеджер иерархий					
☆	Менеджер иерархии	••••••••••••••••••••••••••••••••••••	натель Настройки* Собл de Проверка пароля Ф добавить С Сброс Пользователь: А pki.local/user6 А pki.local/user72 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 А pki.local/user12 В pki.	в SafeNode Сброс пароля Имя пользователя User 18 Новый пароль Повтор пароля Лорименить Отмена Доменный SafeNode SafeNode	×	c
		Примения	A User 16 A User 15 Bcero: 12	SafeNode SafeNode		
ද්දුවු		Отмена				

Рисунок 11.51 – Сброс пароля пользователя

## 11.11 Пользователи с разрешением на вход в ОС

Раздел «Пользователи с разрешением на вход в OC» позволяет задать список пользователей, которым будет предоставлена возможность входа на клиентскую рабочую станцию. Пользователям, не добавленным в список, при попытке входа на клиентскую рабочую станцию будет отказано во входе.

Настройка разграничения входа в ОС доступна только в случае, если на клиентской рабочей станции установлено и взято под управление СДЗ «SafeNode System Loader». При отсутствии СДЗ на клиентской рабочей станции настройка будет невозможна (рисунок 11.52).

Добавление пользователей в раздел «Пользователи с разрешением на вход в ОС» включает пользователя в ограничивающий список, но не (;) добавляет пользователя в список доступа на рабочую станцию. Для входа доменных пользователей и пользователей SafeNode System Loader по паролю необходимо добавить пользователей В список раздела политики аутентификацией» «Управление без дополнительных настроек аутентификации (подробное описание добавления пользователей в политику В разделе «Добавление доменных пользователей описано И пользователей SafeNode System Loader»).



Рисунок 11.52 – Настройка разграничения доступа в ОС недоступна Задать ограничивающий список пользователей возможно только в том случае, если

вышестоящим сервером установлено разрешение на данную настройку в разделе «Управление аутентификацией» клиентской политики (подробное описание приведено в пункте «Управление аутентификацией») (рисунок 11.53).

-



	<ul> <li>Все компьютеры</li> </ul>	🕅 Блокхост-Сеть 🛛 💋 SafeNo	de
	localhost		
0	Cocalhost	24. Блокхост-Сеть SafeNor Пользователи СДЗ (Средства доверенной загрузки) Сетевой адаптер UEFI Проверка пароля в SafeNode Пользователи с разрешением на вход в ОС	Пользователи с разрешением на вход в ОС
			$\checkmark$
			Механизм выключен. Для настройки необходимо включить его в политике группы, в котопой маходится компьтер.
			См. в разделе «Политики» - «Политика SafeNode System Loader» -
			«Управление аутентификацией» - «Дополнительные настройки»
E			
		Применить Отмена	
£03			

Рисунок 11.53 – Механизм разграничения доступа в ОС выключен в политике

Для создания ограничивающего списка пользователей во вкладке *Настройки* клиентской рабочей станции перейдите во вкладку *SafeNode* в раздел «Пользователи с разрешением на вход в ОС» (рисунок 11.54).

🗙 Бло	🗙 Блокхост-Сеть 4 — 🗆 🗙					
Å	Менеджер иерархий					
к <sup>†</sup> л		🙀 W102 Онлайн 🔍	C			
ŕð	▼ 🛱 W102	Общее Токены Пользова	атель Настройки* События			
	<ul> <li>Все компьютеры</li> </ul>	🕅 Блокхост-Сеть 🛛 💋 SafeNo	de			
	ten localhost	Пользователи СДЗ (Средства доверенной загрузки) Сетевой адаптер UEFI	Пользователи с разрешением на вход в ОС Q. Поиск			
		Проверка пароля в SafeNode*	<ul> <li>О Добавить 😨 Удалить இ Автодобавление 🛓 Импорт பိ Экспорт</li> </ul>			
		Пользователи с разрешением	Учетная запись 🔺 Тип			
		на вход в ОС	<b>ж</b> Все пользователи			
			Всего: Все пользователи			
ĘĜ		Применить Отмена				

Рисунок 11.54 – Создание ограничивающего списка пользователей для рабочей станции

По умолчанию в ограничивающем списке пользователей добавлен псевдоним **Все пользователи,** который подразумевает, что все локальные и доменные пользователи имеют возможность входа на клиентскую рабочую станцию.

По кнопке **Добавить** сформируйте список пользователей, которым необходимо разграничить доступ в ОС.

Для добавления доступны:

 доменные пользователи (во вкладке **Домены**). Для добавления доменного пользователя во вкладке **Домены** выберите нужный домен или, при отсутствии необходимого домена в списке, добавьте его по ссылке <sup>О Добавить домен</sup> (рисунок 11.55 а).

– пользователи SafeNode (во вкладке Компьютеры). Для добавления локального пользователя перейдите во вкладку Компьютеры и выберите рабочую станцию, локального пользователя которой требуется добавить (рисунок 11.55 б). Возможна фильтрация выбираемых рабочих станций для поиска машин только в состоянии Онлайн, или ввод имени рабочей станции для поиска по иерархии.

#### 72410666.00063-04 95 01-01

группы пользователей Все пользователи (во вкладке Псевдонимы).
 Псевдоним Все пользователи подразумевает всех доменных и пользователей
 SafeNode клиентской рабочей станции (рисунок 11.55 в).

X	🔀 Добавление пользователей для группы "Все компьютеры" 🗧 🗧				
Домены Компьютеры < >		Пользователи	Будут добавлены - 2		
•	Pki.local (AD)	🔍 Введите запрос и нажмите Enter		o ivanov-i pkilocal	
	• 🗀 12	Имя	▲ ΦΝΟ	sky pkilocal	
	🗀 Builtin	pki.local\Administrator (	отсу		
	Computers	pki.local\Guest (отсутств pki.local\ivanov-i	ует		
	Domain Controllers		sky		
	ForeignSecurityPrincipals	□	usr		
	Managed Service Accounts				
	🗀 Special				
	🗀 Users				
0	Добавить домен	Bcero: 5			
				Добавить Отмена	

a)

#### 🔀 Добавление пользователей × Пользователи Будут добавлены - 3 C Домены Компьютеры Q. Поиск User 16 2 ø wBHN03 wBHN03 (SafeNode) Имя Тип пользователя User 17 2 wBHN03 (SafeNode) User 12\_430a25e90c33976118eb86cdb7... SafeNode User 18 wBHN03 (SafeNode) 2 User 13\_430a25e90c33976118eb86cdb7... SafeNode User 14\_430a25e90c33976118eb86cdb7... SafeNode User 15 SafeNode 🔽 🎤 User 16 SafeNode 🔽 🏂 User 17 SafeNode 🔽 🎤 User 18 SafeNode User 19 SafeNode User 1\_430a25e90c33976118eb86cdb72... SafeNode → User 2 430a25e90c33976118eb86cdb7... SafeNode Bcero: 1 Bcero: 20 Отмена



в)

Рисунок 11.55 – Добавление пользователей

После нажатия кнопки **Добавить**, добавленные пользователи отобразятся в списке пользователей окна **Пользователи с разрешением на вход в ОС** (рисунок 11.54).

По кнопке <sup>© Автодобавление</sup> возможно сформировать ограничивающий список пользователей из списка пользователей, когда либо осуществлявших вход на клиентскую рабочую станцию (рисунок 11.56).



🔀 Бло	кхост-Сеть 4			- 🗆 X
윦	Менеджер иерархий			
* 19	Image: Big Ima	С инный онлайн • Х Автодобавление в ограничивающий спи Пользователи SafeNode Выберите пользователей, которых необходи С Поиск Выбрать все С Снять все Учетная запись • Учетная запись • Выбрать все С Слять все • Учетная запись • Выбрать все С С Снять все • Учетная запись • Учетная запись • Выбрать все С С Снять все • Учетная запись • Выбрать все С С Зарабанае • Выбрать все • Выбрать все С С Зарабанае • Выбрать все • Выбрать все • Выбрать все • С нять все • С яв 11,430а25е90с33976118еb • Учетная • Вобрать все • Вобрать	ксок X имо добавить в список Turi SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode SafeNode	С ВХОД В ОС ВХОД ВХО
			Добавить - 20 Отмена	нный пользователь
ţ		Применить Отмена		

Рисунок 11.56 – Автодобавление в ограничивающий список пользователей

По кнопкам 坐 Импорт / 🖄 Экспорт возможен импорт сформированного ранее списка или экспорт созданного списка пользователей.

# Перечень сокращений

BIOS	_	Basic Input Output System (базовая система ввода-вывода)
CD/DVD	_	Compact Disc (оптический носитель информации), Digital Versatile Disc (универсальный цифровой диск)
СОМ	_	Communication Port (порт, работающий по стандарту RS-232)
DNS	_	Domain Name System (система распределения имен доменов)
LPT	_	Line Print Terminal (международный стандарт параллельного интерфейса для подключения периферийных устройств персонального компьютера)
NTFS	-	New Technology File System (файловая система новой технологии)
PIN	-	Personal Identification Number (личный идентификационный номер)
SIEM	_	Security Information and Event Management (управление информацией о безопасности и управление событиями безопасности)
TCP/IP	-	Transmission Control Protocol/Internet Protocol (протокол управления передачей данных)
UAC	_	User Account Control (контроль учётных записей)
VID/PID	_	Process IDentifier (уникальный идентификатор процесса)
WPD	_	Windows Portable Devices (портативные устройства)
БВПП	_	Безопасный вход по паролю
БД	_	База данных
ЗПС	_	Замкнутая программная среда
НСД	_	Несанкционированный доступ
OC	_	Операционная система
ПК	_	Программный комплекс
ПО	_	Программное обеспечение
СЗИ	_	Средство защиты информации
СКЗИ	_	Средство криптографической защиты информации
УЦ	_	Удостоверяющий центр