ГАЗИНФОРМ СЕРВИС

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

Описание применения

Санкт-Петербург, 2021

Аннотация

Настоящий документ содержит описание применения средства защиты информации (СЗИ) от несанкционированного доступа «Блокхост-Сеть 4» (в дальнейшем – СЗИ от НСД «Блокхост-Сеть 4», СЗИ или средство).

В разделе «Назначение средства» приведено назначение СЗИ и дан краткий обзор основных функциональных возможностей.

В разделе «Условия применения» указаны условия, необходимые для использования СЗИ, требования к аппаратным и программным средствам серверов и клиентских компьютеров, где предполагается использование СЗИ.

В разделе «Описание задачи» указаны задачи, которые решает СЗИ и описаны функции защиты с помощью которых эти задачи решаются.

В соответствующих разделах разъясняется взаимодействие модулей программного обеспечения, для выполнения функциональных возможностей СЗИ, и описываются входные и выходные данные используемые основными функциями СЗИ.

В конце документа приведен список использованных сокращений.

Содержание

1 Назначение средства

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4» является программным средством контроля съемных машинных носителей информации, предназначенным для защиты от несанкционированного доступа к информации, АС класса защищенности 1Г, ГИС 1 класса защищенности, АСУТП 1 класса защищенности, обеспечения безопасности персональных данных 1 уровня защищенности, значимых объектов КИИ 1 категории на базе персональных компьютеров (ПК) под управлением операционных систем (далее – ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

СЗИ от НСД «Блокхост-Сеть 4» является специализированным программным СЗИ, которое обеспечивает возможность:

- идентификации и аутентификации пользователей информационной системы при попытках входа на защищаемые ПК.
- двухфакторной аутентификации пользователей информационной системы при входе на защищаемые ПК, при помощи дополнительных технических средств – персональных идентификаторов пользователя (токенов).
- контроля прав доступа пользователей информационной системы к защищаемой информации на ПК.
- контроля подключения и использования съемных машинных носителей информации на защищаемых ПК.

СЗИ от НСД «Блокхост-Сеть 4» обеспечивает:

- пятый класс защищенности для средств вычислительной техники (СВТ) в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992);
- четвертый уровень доверия в соответствии с документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утвержденный приказом ФСТЭК России от 02 июня 2020 г № 76);
- четвертый класс защиты в соответствии с методическим документом «Профиль защиты средств контроля подключения съемных машинных носителей информации четверного класса защиты ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014).

В соответствии с ГОСТ Р 50739-95 «средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» защищенность обеспечивается тремя группами требований к средствам защиты, реализуемым в СВТ:

1) Требования к разграничению доступа, предусматривающие, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа.

2) Требования к учету, предусматривающие, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации.

3) Требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

Выполнение каждой группы требований обеспечивается соответствующими механизмами защиты, представленными на рисунке 1.1.

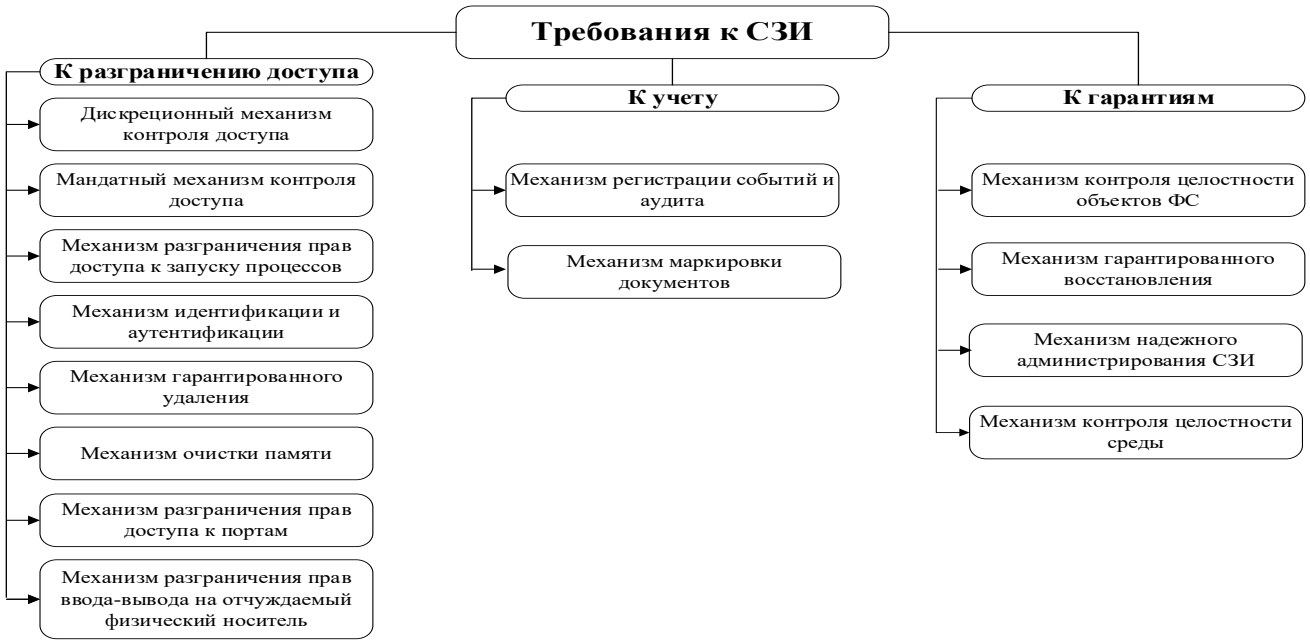

Рисунок 1.1 – Механизмы защиты, обеспечивающие выполнение требований к СЗИ

2 Условия применения

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 MS Windows, под управлением которых функционирует СЗИ, приведены в таблице 2.1.

Таблица 2.1 – Перечень поддерживаемых операционных систем MS Windows

ОС
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 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)

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 производительности	Обусловлены требованиями используемых ОС	см. таблицу 2.1
Аппаратные требования	**Использование персональных идентификаторов**	
	USB-порт	

Требования	Наименование	Примечание
Дополнительное программное обеспечение	**Обновления**	
	KB3033929, KB4474419, KB4490628	для ОС Windows 7 и Windows Server 2008/2008R2
	KB2921916	в ОС Windows 7 и Windows Server 2008/2008R2 для механизма «Контроль печати»
	Реализация аутентификации с использованием ГОСТ сертификатов – КриптоПро[1]	
	СКЗИ «КриптоПро CSP»	версии 3.6 и выше
	Драйверы токенов	
	Драйверы устройств производителей	см. таблицу 3.1.
	Программная платформа	
	распространяемый пакет Microsoft Visual C++ 2015-2019 Redistributable	
	NET Framework 4.5.2	При использовании подсистемы ГУПТ
	обновление «Remote Server Administration Tools»: • для ОС Windows 7 "Remote Server Administration Tools for Windows 7" (https://www.microsoft.com/en-us/download/details.aspx?id=7887); • для ОС Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (https://www.microsoft.com/en-us/download/details.aspx?id=28972); • для ОС 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

2.2 Ограничения при эксплуатации СЗИ

Не следует использовать СЗИ для защиты от НСД терминальных серверов.

Не рекомендуется установка серверной части СЗИ на сервер с ролью контроллера домена (Domain Controller) Microsoft Active Directory.

Перед началом установки СЗИ на ОС Windows 8.1/2012/2012R2/10/2016/2019 необходимо отключить встроенный антивирус ОС (Windows Defender).

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности должен быть открыт 999 TCP порт. Для взаимодействия сервера системы

[1] При использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

развертывания и агентов развертывания на сервере безопасности должен быть открыт 25000 TCP порт, на клиенте – 25001 TCP порт.

В некоторых случаях для корректного функционирования СЗИ необходимо понизить уровень контроля учетных записей (UAC) в ОС Windows (вплоть до полного отключения).

Для устойчивой работы СЗИ и во избежание конфликта с другими программными средствами необходимо удалить ранее установленные и не устанавливать новые программы, следящие за работой файловой системы. К таким программным средствам относятся:

- средства защиты от несанкционированного доступа;
- анализаторы файловой системы.

Допускается совместная работа СЗИ от НСД «Блокхост-Сеть 4» со следующим антивирусным ПО:

- Kaspersky Endpoint Security 10;
- Symantec Endpoint Protection v.12.

Перед установкой клиентской части СЗИ от НСД «Блокхост-Сеть 4» с включенным в установку компонентом ***Сетевой фильтр мандатного механизма*** на клиентской рабочей станции необходимо отключить механизм самозащиты «Kaspersky Endpoint Security» при наличии соответствующего антивирусного ПО на время установки СЗИ.

Для проверки совместимости СЗИ от НСД «Блокхост-Сеть 4» с другим антивирусным программным обеспечением (ПО) необходимо последовательно выполнить следующие действия:

1) Установить СЗИ от НСД «Блокхост-Сеть 4» на ПК.

2) Установить антивирусное ПО.

3) Выполнить регламентное тестирование СЗИ от НСД «Блокхост-Сеть 4» в соответствии с Приложением 3 к документу «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками».

4) В случае совпадения результатов выполнения тестов с ожидаемыми результатами из эксплуатационной документации разрешается совместное использование СЗИ от НСД «Блокхост-Сеть 4» и используемого антивирусного ПО.

Для эксплуатации и эффективного применения СЗИ от НСД «Блокхост-Сеть 4» необходимо использование лицензионного системного ПО.

Для корректной работы СЗИ от НСД «Блокхост-Сеть 4» необходимо отсутствие динамических дисков на компьютере.

Настройку параметров СЗИ должен выполнять только администратор безопасности.

Установка СЗИ от НСД «Блокхост-Сеть 4» должна выполняться на ПК защищаемой локальной вычислительной сети.

Вариант СЗИ от НСД «Блокхост-Сеть 4» с удаленным управлением может функционировать в локальной сети без доменной инфраструктуры Microsoft Active Directory.

Установка СЗИ от НСД «Блокхост-Сеть 4» должна выполняться на диск C:\. На жестком диске не должно быть других установленных операционных систем.

Мягкий режим работы СЗИ от НСД «Блокхост-Сеть 4» и аутентификация средствами ОС Windows используются для первичной настройки средства защиты до начала эксплуатации. В данном режиме СЗИ не обеспечивает выполнение заявленных функций безопасности. Эксплуатировать СЗИ в мягком режиме для защиты ПК **запрещено**.

Перед началом использования необходимо ознакомиться с эксплуатационной документацией, входящей в комплект поставки изделия.

Установка СЗИ от НСД «Блокхост-Сеть 4» автономного варианта, должна проводиться в соответствии с документом «СЗИ от НСД «Блокхост-сеть 4. Руководство по инсталляции».

Установка СЗИ от НСД «Блокхост-Сеть 4» с удаленным управлением, должна производиться в соответствии с документами:

- «СЗИ от НСД «Блокхост-Сеть 4. Руководство по инсталляции».
- «СЗИ от НСД «Блокхост-Сеть 4. Руководство администратора безопасности. Часть 2. Развертывание и аудит».

Настройка подсистемы управления токенами должна производиться в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4. Руководство администратора безопасности. Часть 3. Настройка подсистемы управления токенами».

Работа администратора должна осуществляться в соответствии с документами:

- «СЗИ от НСД «Блокхост-Сеть 4. Руководство администратора безопасности. Часть 1. Управление политиками».
- «СЗИ от НСД «Блокхост-Сеть 4. Руководство администратора безопасности. Часть 2. Развертывание и аудит».
- «СЗИ от НСД «Блокхост-Сеть 4. Руководство администратора безопасности. Часть 4. Управление токенами»

Работа пользователя должна осуществляться в соответствии с документом «СЗИ от НСД «Блокхост-Сеть 4. Руководство пользователя».

Встроенная в ОС учетная запись «Администратор» должна использоваться под

контролем сотрудника, ответственного за обеспечение информационной безопасности, только в следующих случаях:

- для создания специальной учетной записи администратора безопасности СЗИ;
- для разрешения проблем отказа аппаратного или программного обеспечения ПК, при которых невозможен вход в систему в штатном режиме.

Локальному пользователю встроенной в ОС учетной записи «Администратор» и администратору безопасности СЗИ **запрещается** участвовать в процессе обработки информации.

При настройке мандатного механизма разграничения доступа и эксплуатации СЗИ от НСД «Блокхост-Сеть 4» **запрещено** создание вложенных объектов, для которых в объекте с низкой классификационной меткой может быть размещен объект с более высокой классификационной меткой. Изменение классификационных меток объектов должно проводиться под контролем сотрудника ответственного за обеспечение информационной безопасности.

При работе с защищаемой информацией, в качестве персональных электронных идентификаторов могут использоваться электронные идентификаторы (токены), имеющие соответствующие сертификаты ФСТЭК, ФСБ.

После установки СЗИ от НСД «Блокхост-Сеть 4» для устранения уязвимости операционной системы администратору безопасности необходимо отключить среду восстановления ОС Windows. Отключение среды восстановления ОС Windows описано в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности».

Все используемые персональные электронные идентификаторы подлежат обязательному учету и маркировке.

Для поддержания необходимого уровня защищенности ПК и информационных ресурсов, эксплуатации и эффективного применения системы защиты дополнительно требуется выполнение следующих организационно-технических мероприятий:

- обеспечение физической сохранности (целостности) ПК, наличие физической охраны помещения, в котором эксплуатируется ПК и исключение возможности несанкционированного доступа к ПК посторонних лиц;
- наличие администратора безопасности, отвечающего за ее установку и правильную эксплуатацию;
- соблюдение принципа минимизации привилегий пользователей ПК, при котором пользователям предоставляются только те права доступа, которые необходимы им для выполнения служебных обязанностей. Привилегии локальных администраторов ПК допускается предоставлять только пользователям, выполняющим функции

администратора безопасности СЗИ;

- хранение в секрете паролей (кодов), а также – PIN-кодов персональных электронных идентификаторов администратора и пользователей системы;
- периодическая смена паролей и PIN-кодов пользователей и администратора безопасности;
- учет носителей информации (съемных подключаемых носителей, персональных электронных идентификаторов и т.п. устройств);
- периодическое тестирование функций СЗИ от НСД «Блокхост-Сеть 4» в соответствии с Приложением 3 «СЗИ от НСД «Блокхост-сеть 4. Руководство администратора безопасности. Часть1. Управление политиками»;
- использование в ПК сертифицированных технических и программных средств;
- проверка носителей информации на наличие вирусов.

Администратору безопасности необходимо обеспечить контроль наличия и создания дополнительных ссылок на объекты, поддерживаемых файловой системой.

Должны быть установлены все актуальные обновления безопасности среды функционирования СЗИ от НСД «Блокхост-Сеть 4». При эксплуатации Изделия в среде операционных систем Windows 7/ Server 2008R2 обязательна установка расширенных обновлений безопасности в рамках программы технической поддержки Extended Security Updates Microsoft.

Установка и эксплуатация экземпляра СЗИ от НСД «Блокхост-Сеть 4» должна выполняться только с действующей лицензией на использование. СЗИ от НСД «Блокхост-Сеть 4» не выполняет функции защиты после истечения срока действия лицензии на использование.

При эксплуатации СЗИ «Блокхост-Сеть 4» в государственных информационных системах 1 класса защищенности для обеспечения усиления 4б меры защиты РСБ.1 реализована возможность передачи событий безопасности в систему, не входящую в состав средства защиты.

При эксплуатации изделия следует учесть следующие ограничения механизма контроля печати.

- запрещается включение механизма контроля печати СЗИ на рабочих станциях с установленным DLP-агентом Symantec Data Loss Prevention – при включении механизма контроля печати происходит аварийное завершение процесса explorer.exe;
- для устойчивого функционирования АРМ, с установленным СКЗИ «КриптоПро CSP», при использовании механизма контроля печати СЗИ, версия сборки СКЗИ должна быть 3.9.8293 или 4.0.9589 (Gauss) и выше;
- блокируется возможность печати содержимого страницы браузера Internet

Explorer (версия 11) при включенном контроле учетных записей (UAC);

- печать на принтерах общего доступа (локальных принтерах рабочих станций, доступ к которым предоставлен пользователям сети) возможна только при включении на клиентской рабочей станции, которая обращается к принтеру общего доступа, механизма контроля печати с простановкой специального колонтитула по шаблону печати;
- печать на принтерах общего доступа (локальных принтеров рабочих станций, доступ к которым предоставлен пользователям сети) возможна, только если на рабочей станции, с которой предоставляется общий доступ к принтеру (принт-сервере), СЗИ не установлено;
- необходимо использовать драйверы печати Windows Type 3, загруженные с веб-сайта производителя принтера.

При эксплуатации изделия следует учесть следующие ограничения подсистемы гарантированного удаления по требованию (ГУПТ) [2]:

- в подсистеме ГУПТ недоступно гарантированное удаление по требованию файлов, находящихся на SSD и USB-носителях;
- для полной очистки SSD и USB-носителей возможно использование операции очистки свободного пространства данных накопителей информации.

[2] Ограничения касаются модуля ГУПТ *GIS.WipeFiles<номер версии>.msi* устанавливаемого отдельно на клиентскую рабочую станцию.

3 Описание задачи

СЗИ от НСД «Блокхост-Сеть 4» является программным средством контроля съемных машинных носителей информации и защиты от несанкционированного доступа к информации, предназначенным для защиты информации АС класса защищенности 1Г, ГИС 1 класса защищенности, АСУТП 1 класса защищенности, обеспечения безопасности персональных данных 1 уровня защищенности, значимых объектов КИИ 1 категории на базе ПК под управлением ОС Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

СЗИ от НСД «Блокхост-Сеть 4» является специализированным программным СЗИ, которое обеспечивает возможность:

- идентификации и аутентификации пользователей информационной системы при попытках входа на защищаемые ПК.
- двухфакторной аутентификации пользователей информационной системы при входе на защищаемые ПК, при помощи дополнительных технических средств – персональных идентификаторов пользователя (токенов).
- контроля прав доступа пользователей информационной системы к защищаемой информации на ПК.
- контроля подключения и использования съемных машинных носителей информации на защищаемых ПК.

СЗИ от НСД «Блокхост-Сеть 4» содержит клиентскую часть, которая устанавливается на клиентские рабочие станции, серверную часть, которая устанавливается на серверы безопасности, и консоль управления, которая устанавливается на рабочее место администратора.

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

- вариант №1 - автономный вариант СЗИ, при котором СЗИ устанавливается на ПК с 32/64 разрядной ОС MS Windows и используется локально;
- вариант №2 - вариант с удаленным управлением СЗИ, при котором СЗИ устанавливается на ПК с 32/64 разрядной ОС MS Windows, и работает под управлением сервера безопасности.

В состав варианта №1 входят консоль управления, серверная и клиентская части СЗИ, функционирующие на одном ПК. 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;

- серверная часть СЗИ от НСД «Блокхост-Сеть 4», которая устанавливается на серверы безопасности,
- консоль управления, которая устанавливается на рабочее место администратора и позволяет управлять развертыванием СЗИ на клиентах, подключением клиентских частей к серверной части и настройками сбора событий безопасности.

Поддерживаемые СЗИ от НСД «Блокхост-Сеть 4» дополнительные технические средства (персональные электронные идентификаторы пользователей), которые используются для двухфакторной идентификации и аутентификации пользователей на ПК приведены в таблице 3.1.

Таблица 3.1 – Поддерживаемые СЗИ от НСД «Блокхост-Сеть 4» персональные идентификаторы

Носитель	Производитель	Наименование носителя
eToken	ЗАО «АЛАДДИН Р.Д.»	eToken Pro, eToken Pro (Java), eToken ГОСТ, eToken NG-FLASH, eToken NG-FLASH (Java), eToken NG-OTP, eToken NG-OTP (Java), eToken GT (Java), eToken PRO (Java) SC,eToken PRO SC
SafeNet eToken	ООО «Сертифицированные информационные системы»	SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205, SafeNet eToken 7200, SafeNet eToken 7300, SafeNet eToken 4100
ruToken	ЗАО «Актив Софт»	ruToken, ruToken S, ruToken Lite, ruToken ЭЦП
JaCarta	ЗАО «АЛАДДИН Р.Д.»	JaCarta PRO, JaCarta ГОСТ, JaCarta PKI
JaCarta-2	ЗАО «АЛАДДИН Р.Д.»	JaCarta-2 nano ГОСТ JC-006, смарт-карта JaCarta-2 PRO/ГОСТ 334, смарт-карта JaCarta-2 ГОСТ JC-306, USB JaCarta-2 PRO/ГОСТ 234, USB JaCarta-2 ГОСТ 206
JaCarta LT	ЗАО «АЛАДДИН Р.Д.»	JaCarta LT
eSmart Token	ООО «Интеллектуальные системы управления бизнесом»	ESMART Token (USB-ключ и смарт-карта)
Avest Token (AvBign)	ЗАО «Авест» Республика Беларусь	Avest Token (AvBign)

Клиентская часть СЗИ от НСД «Блокхост-Сеть 4» обеспечивает следующие функциональные возможности безопасности СЗИ:

- идентификация и аутентификация администратора безопасности и пользователей, работающих на ПК с СЗИ от НСД «Блокхост-Сеть 4», в том числе с применением персональных электронных идентификаторов, приведенных в таблице 3.1;
- возможность двухфакторной аутентификации пользователей средствами СЗИ, при входе в ОС Windows с использованием цифровых сертификатов пользователей

(сертификаты могут храниться на вышеуказанных персональных электронных идентификаторах);

- аудит и регистрация событий безопасности при обращении к защищаемым ресурсам ПК;
- контроль устройств (съемные USB-устройства; CD/DVD-устройства; устройства, подключаемые через COM- 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.

Серверная часть (сервер безопасности) СЗИ от НСД «Блокхост-Сеть 4» обеспечивает следующие функциональные возможности безопасности СЗИ:

- 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-систему;
- управление персональными электронными идентификаторами пользователя (токенами) на протяжении всего жизненного цикла;
- сбор данных о правах мандатного доступа пользователей, при входе пользователей на ПК.

3.1 Механизм идентификации и аутентификации

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

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

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

Предусмотрены следующие возможные виды входа пользователя в систему, описанные в таблице 3.2.

Таблица 3.2 – Возможные виды входа пользователя в систему

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

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

- проверка не является ли пользователь встроенным администратором;

- проверка режима функционирования рабочей станции (включен/отключен «мягкий» режим работы) и проверка наличия лицензии у клиентской рабочей станции;
- проверка соответствия введенных аутентификационных данных требованиям сложности, установленным в политике аутентификации;
- проверка наличия учетной записи пользователя в списке клиентской политики в разделе «Управление входом в ОС»;
- при предъявлении токена выполняется проверка разрешен ли пользователю вход по токену, и в случае разрешения:
  - принадлежит ли токен пользователю;
  - валиден ли токен.
- при предъявлении пользователем пароля выполняется:
  - проверка установки у пользователя типа аутентификации «Доверять аутентификации Windows»;
  - 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 СЗИ (в случае разрешенной аутентификации пользователя по паролю);
- при включенном механизме, ограничивающим вход на клиентскую рабочую станцию, выполняется проверка наличия учетной записи пользователя в списке раздела «Пользователи с разрешением на вход в ОС».

Подробная схема проверок при аутентификации пользователя приведена на рисунке 3.1.

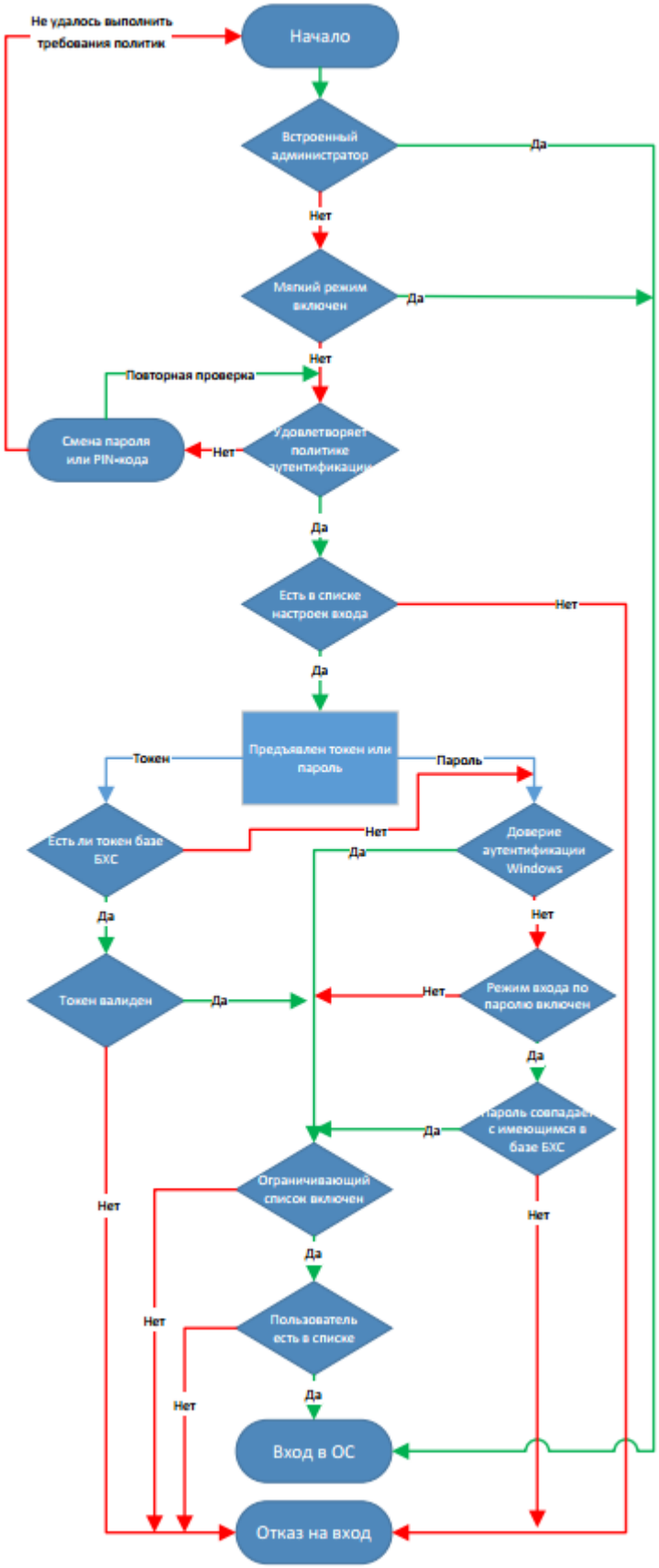

Рисунок 3.1 – Схема аутентификации пользователя

Если все проверки завершены успешно, пользователю разрешается вход в

операционную систему.

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

В ***Мягком режиме работы*** СЗИ (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками») установленные настройки механизма идентификации и аутентификации не учитываются.

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.

Мягкий режим работы должен использоваться только для первичной настройки средства защиты, до начала эксплуатации. В данном режиме средство защиты не обеспечивает выполнение заявленных функций безопасности. Эксплуатировать СЗИ в мягком режиме для защиты станции **запрещено**.

3.2 Механизм контроля целостности среды

Механизм контроля 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.

С помощью механизма контроля целостности среды 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 программно-аппаратной среды с указанием эталонного и текущего состояния раздела конфигурации, в котором выявлено нарушение.

Соответствие контролируемых устройств и полей, по которым осуществляется контроль изменения конфигурации, описаны в таблице 3.2.

Таблица 3.2 – Соответствие устройств и параметров изменения конфигурации

Контролируемое устройство	**Контроль изменения конфигурации осуществляется по следующим полям**
Процессор	• Name (модель процессора; например «Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz»); • DeviceID (ИД в компьютере).
Жесткий диск	• Model (модель диска; например «WDC WD1600AAJS-00M0A0 ATA Device»); • SerialNumber (серийный номер диска); • InterfaceType (тип аппаратного интерфейса; например SCSI, HDC, IDE, USB); • Size (размер диска, в байтах); • Manufacturer (производитель устройства); • DeviceID (ИД в компьютере).
CDROM	• SerialNumber (серийный номер); • Manufacturer (производитель устройства); • MediaType (тип поддерживаемых носителей; например «DVD Writer»); • DeviceID (ИД в компьютере).
Сетевой адаптер	• ProductName (модель сетевого адаптера; например «Сетевая карта Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet NIC (NDIS 6.20)»); • Manufacturer (производитель сетевого адаптера; например Realtek, Microsoft); • AdapterType (тип сетевого адаптера; например, Ethernet 802.3, Token Ring 802.5, Wireless); • MACAddress (MAC-адрес); • GUID (GUID); • DeviceID (ИД в компьютере).
Материнская плата	• Manufacturer (производитель мат. платы; например «Gigabyte Technology Co., Ltd.»); • Model (модель мат. платы); • PartNumber (идентификатор партии мат. плат, назначенный заводом-изготовителем); • Product (идентификатор партии мат. плат, назначенный производителем; например «G31M-S2L»); • SerialNumber (серийный номер мат. платы); • Version (версия мат. платы, назначенная заводом-изготовителем).
Видеокарта	• AdapterRAM (объем памяти видеоконтроллера, в байтах); • Name (модель видеоконтроллера; например Intel(R) G33/G31 Express Chipset Family); • VideoProcessor (тип видеопроцессора; например Intel GMA 3100);

	• DeviceID (ИД в компьютере).
Модуль оперативной памяти	• BankLabel (метка банка, в котором находится память; например Bank0/1); • Capacity (объем модуля оперативной памяти, в байтах); • Model (модель модуля оперативной памяти); • Name (метка физического элемента); • Manufacturer (Производитель устройства); • SerialNumber (Серийный номер).

3.3 Контроль целостности файлов

Механизм контроля изменения файлов предназначен для слежения за неизменностью контролируемых файлов. Он 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!

3.4 Механизм контроля печати

Механизм контроля печати осуществляет разграничение прав печати для указанных приложений, простановку специального колонтитула по шаблону печати, ведение аудита печати.

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.

Аудит процесса печати подразумевает регистрацию всех фактов печати документов, в том числе и факты запрета печати в соответствии с настройками механизма контроля печати.

Простановка специального колонтитула по шаблону печати позволяет добавлять на

страницы распечатываемого документа дополнительные сведения, настраиваемые по шаблону печати. При печати документа с использованием шаблона на каждой странице документа будет выводиться 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.

3.5 Аудит запуска приложений и доступа к медиафайлам

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

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.

3.6 Гарантированное удаление файлов и очистка оперативной памяти

Гарантированное удаление файлов 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 по специальному алгоритму, исключающему считывание остаточной информации на диске после их удаления.

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.

3.7 Контроль устройств

В СЗИ от НСД «Блокхост-Сеть 4» реализован механизм контроля устройств, предназначенный для разграничения доступа пользователей к отчуждаемым носителям информации.

Реализация механизма контроля устройств заключается в предоставлении администратору безопасности возможности санкционировать доступ каждого пользователя к следующим устройствам:

- съемным USB-устройствам;
- CD/DVD-устройствам;
- устройствам, подключаемым через COM- и LPT-порты;

а также в возможности формирования списка разрешенных для пользователя устройств. После формирования доверенного списка устройств у пользователя будет доступ к устройству из списка, независимо от ограничений, заданных администратором в механизме контроля устройств для клиентской рабочей станции.

3.8 Механизм сбора событий

Механизм регистрации событий и аудита предназначен для отслеживания событий и регистрации обращения к защищаемым ресурсам, а также при срабатывании всех механизмов защиты.

Настройка механизма сбора событий заключается в формировании списка событий, необходимых к сбору по всей иерархии подчиненных серверов и клиентских рабочих станций, и формировании расписания сбора указанных событий.

Сформированные события содержат следующую информацию:

- дата и время;
- источник записи;
- категория доступа;
- тип сообщения (успешное или неуспешное);
- код (ID);
- пользователь;

- имя компьютера;
- имя пользователя;
- метка пользователя;
- имя объекта;
- метка объекта;
- тип доступа;
- привилегии.

В подсистеме сбора событий администратору доступны следующие функции:

- формирование сводного отчета с информацией о состоянии клиентов, подключенных к серверам иерархии;
- сбор событий аудита с клиентов на сервер СЗИ;
- просмотр и фильтрация событий аудита, собранных с клиентских компьютеров на сервер;
- просмотр и фильтрация событий аудита напрямую из журнала клиентского компьютера;
- передача событий аудита вверх по иерархии серверов вплоть до головного сервера с последующей передачей в SIEM-систему.

3.9 Дискреционный механизм контроля доступа к ресурсам

Дискреционный механизм контроля доступа к ресурсам осуществляет контроль доступа пользователей к защищаемым объектам файловой системы (логическим дискам, каталогам и файлам) в соответствии с заданной для пользователей и объектов файловой системы «матрицей дискреционного доступа».

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.

Матрица доступа представляет собой список объектов файловой системы с сопоставленными им пользователями с установленными настройками доступа к объектам: ***Просмотр*** и ***Изменение.***

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.

Дискреционный механизм 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.

Возможность санкционированного изменения прав разграничения доступа, в том числе возможность санкционированного изменения списка пользователей и списка объектов файловой системы в дискреционном механизме разграничения доступа предоставляется только администратору безопасности.

3.10 Формирование замкнутой программной среды

Механизм позволяет накладывать ограничения на запуск определенных процессов пользователями. Под запуском процесса понимается попытка открытия исполняемого файла. Механизм замкнутой программной среды (ЗПС) работает по принципу ***«белого списка»***:

- администратор формирует для пользователя список разрешенных к запуску процессов (программ);
- 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;
- пользователь может запускать процессы только из списка, сформированного администратором.

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

Список разрешенных процессов в обязательном порядке должен включать системные процессы, необходимые для запуска и функционирования операционной системы клиентской рабочей станции.

3.11 Мандатное разграничение контроля доступа к ресурсам

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, 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).

Категория – это символьное значение, 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 ($УД_П=УД_Р$), то пользователь получает полный доступ к ресурсу;
- если уровень доступа пользователя меньше уровня доступа ресурса ($УД_П<УД_Р$), то пользователь получит доступ только на запись, но не получит доступ на чтение, в том числе и на просмотр содержимого ресурса;
- если уровень доступа пользователя выше уровня доступа ресурса ($УД_П>УД_Р$), то пользователь получит права чтения и просмотра 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 полный доступ 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 чтения и просмотра ресурса;
- если уровень доступа пользователя совпадает с уровнем доступа ресурса и категория, назначенная пользователю, включают в себя все категории ресурса, то пользователь получает полный доступ к ресурсу.

3.12 Механизм контроля целостности и гарантированного восстановления программных модулей СЗИ

Контроль целостности программных модулей СЗИ и их надежное восстановление осуществляются драйвером BhProt. Контроль целостности осуществляется при запуске программных модулей СЗИ (контролируются все файлы в директории C:\BLOCKHOST).

Расчет контрольных сумм программных модулей СЗИ выполняется с помощью механизма вычисления хэша SHA1. Хэш вычисляется в процессе сборки, сохраняется в дистрибутиве в специальном файле и записывается в защищенную ветку реестра.

При запуске СЗИ рассчитываются контрольные суммы программных модулей СЗИ по указанному выше алгоритму и сравниваются с эталонным значением в защищенной ветке реестра. В случае обнаружения несовпадения в контрольных суммах происходит восстановление программных модулей из резервных копий в каталоге C:\BLOCKHOST\BACKUP, в системный журнал пишется событие аудита об обнаружении нарушения контроля целостности и выполнении восстановления.

Если восстановление программного модуля СЗИ из резервной копии невозможно, рабочая станция блокируется, в системный журнал пишется событие аудита об обнаружении нарушения контроля целостности и невозможности восстановления из резервной копии.

3.13 Механизм управления идентификаторами

Механизм управления идентификаторами предназначен для управления персональными электронными идентификаторами (токенами): eToken, SafeNet eToken, JaCarta PRO, JaCarta PKI, JaCarta-2, ESMART Token и ruToken.

Механизм управления идентификаторами позволяет выполнять следующие действия:

- регистрировать и вести учет персональных электронных идентификаторов;

- осуществлять управление персональными электронными идентификаторами:
  - назначение токенов пользователям;
  - приостановка/возобновление использования токенов;
  - вывод токенов из использования (отзыв цифровых сертификатов на устройствах);
  - запись цифровых сертификатов на токен;
  - удаление токенов из системы;
- уведомлять пользователей и администраторов о состоянии цифровых сертификатов на токенах (действителен, отозван, истекает, отклонен, одобрен и т.д.);
- осуществлять поиск и фильтрацию информации о токенах и пользователях в базе данных;
- формировать акты и отслеживать историю актов по результатам операций выдачи токена пользователю, изъятия токена и удаления токена из системы.

3.14 Механизм администрирования СЗИ

Механизм администрирования позволяет с помощью консоли управления установить необходимые настройки безопасности с последующей передачей настроек безопасности по всей иерархии в БД настроек подчиненных серверов и клиентских рабочих станций.

Механизм администрирования доступен только пользователю с правами администратора безопасности.

В консоли управления администратору безопасности доступны следующие действия:

- управление сформированной сетевой структурой: основным и подчиненными серверами, клиентскими рабочими станции и группами, включающими подчиненные серверы и клиентские рабочие станции;
- управление клиентскими и серверными политиками (набором настроек механизмов безопасности и параметров работы серверов и клиентских рабочих станций);
- управление параметрами аутентификации пользователей при входе на клиентские рабочие станции;
- управление ограничениями при задании пароля и PIN-кода токена пользователя, настройка количества неправильных попыток входа;
- отслеживание изменений в списке установленных программ, служб, драйверов,

каталогах общего доступа, контроль аппаратной среды;

- отслеживание изменений в контрольных суммах заданных файлов;
- настройка гарантированного удаления объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления;
- регистрация событий аудита при печати документов для всех приложений;
- регистрация событий аудита при попытках доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям;
- регистрация событий аудита запуска и прекращения работы исполняемых файлов;
- управление очисткой всей свободной физической памяти поставленных на контроль приложений после их завершения;
- настройка возможности работы в мягком режиме, управление настройками журнала аудита;
- управление параметрами разграничения доступа к серверу;
- формирование списка собираемых событий и запуска цикла сбора событий с подчиненных серверов и клиентских рабочих станций;
- настройка параметров автоархивации событий, собранных с клиентских рабочих станций и подчиненных серверов;
- настройка параметров кэша событий для временного хранения событий подчиненных серверов/клиентских компьютеров;
- настройка присоединения сервера в иерархию в качестве головного или подчиненного сервера;
- настройка параметров экспорта событий в SIEM-систему;
- настройка доступа пользователей к объектам файловой системы: логическим дискам, каталогам и файлам;
- отслеживание изменений в перечне заданных файлов и восстановление их из резервных копий;
- настройка возможности входа пользователя в систему с использованием пароля;
- разграничение прав печати для указанных приложений, простановка специального колонтитула по шаблону печати для указанных приложений;
- формирование списка разрешенных для запуска процессов, доступных для выбранного пользователя на клиентской рабочей станции;

- формирование списка пользователей, которым будет предоставлена возможность входа на клиентскую рабочую станцию;
- настройка доступа пользователя к файловым ресурсам станции с помощью присвоения пользователям и ресурсам определенных меток;
- управление процессом установки или удаления программного обеспечения, в том числе клиентов Блокхост-Сеть на рабочие станции;
- формирование сводных данных о состоянии клиентов, подключенных к серверам иерархии;
- управление устройствами аутентификации пользователей на протяжении всего жизненного цикла (учет, назначение пользователям, приостановка использования, вывод из использования).

4 Входные и выходные данные

Входными данными для СЗИ от НСД «Блокхост-Сеть 4» являются:

- база данных настроек системы защиты;
- база данных настроек операционной системы.

Настройки системы защиты хранятся в клиентской и серверной базах данных и содержат информацию обо всех субъектах и объектах системы защиты, о настройках прав доступа по каждому механизму защиты и дополнительных параметрах.

Описание структуры клиентской и серверной базы данных представлено в Приложении 3 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Описание программы».

Выходными данными СЗИ от НСД «Блокхост-Сеть 4» являются файлы аудита, создаваемые в процессе работы СЗИ.

Промежуточными выходными данными считаются системные сообщения о недоступности тех или иных ресурсов для пользователя, защищенных СЗИ. Вид и содержание этих сообщений зависит от конкретной версии ОС.

В журнал аудита записываются все обращения к защищаемым ресурсам с указанием субъекта, защищаемого объекта, механизма, способа обращения, успешности попытки обращения и времени обращения.

Просмотр сообщений аудита и очистка журналов аудита осуществляются администратором безопасности с помощью консоли управления.

Полный перечень фиксируемых событий аудита приведен в Приложении 1 документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

5 Программные модули СЗИ

СЗИ от НСД «Блокхост-Сеть 4» включает подсистемы, содержащие программные модули, реализующие механизмы защиты в составе программного обеспечения СЗИ.

Подсистема «Управление и администрирование» клиентской части содержит следующие логические модули:

- модуль «Диспетчер соединений клиента» является диспетчером запросов на получение настроек, которые поступают от других подсистем клиента СЗИ или от сервера СЗИ;
- модуль «Менеджер БД настроек клиента» предназначен для записи и чтения заданных настроек клиента, из/в БД настроек;
- модуль «Менеджер настроек клиента» предназначен для получения информация о ресурсах ПК из реестра ОС Windows, и выполняет запросы на получение данной информации от модуля «Диспетчер соединений клиента», а также удаленные запросы;
- модуль «Управление токенами на клиенте» предназначен для управления удаленной выдачей токенов, контроль и управление жизненным циклом токенов, осуществляет запись и синхронизацию цифровых сертификатов на токенах при удаленной выдаче токенов.

Подсистема «Управление и администрирование» серверной части содержит следующие логические модули:

- модуль «Консоль подсистемы управления» обеспечивает графический интерфейс для управления и администрирование режимами работы, настройками и политиками для удаленных клиентов СЗИ и сервера СЗИ, получает и сохраняет данные режимов работы и настроек из/в БД настроек;
- модуль «Служба соединения консоли с сервером» обеспечивает связь модуля «Консоль управления» с другими службами сервера и обмен данными между ними, осуществляет разграничение доступа к управлению СЗИ;
- модуль «Диспетчер соединений сервера» является диспетчером запросов на получение настроек, поступающих от других подсистем сервера СЗИ, осуществляет передачу настроек клиентов от сервера СЗИ через подсистему сетевого обмена;
- модуль «Менеджер политик и настроек клиентов» взаимодействует с БД настроек клиента и БД настроек сервера СЗИ, выполняя запись и чтение заданных настроек, из/в БД настроек, и передает их в подсистему «Сетевой обмен» для передачи клиентам СЗИ;
- модуль «Управление токенами на сервере» предназначен для управления выпуском токенов для пользователей, выполняет контроль и управление жизненным циклом токенов, осуществляет формирование, запись и синхронизацию цифровых

сертификатов на токенах, при подключении токенов на клиенте или на сервере.

Подсистема «Аудит» клиентской части содержит следующие логические модули:

- модуль «Диспетчер событий аудита» осуществляет сбор событий аудита, которые поступают от всех подсистем, формирует описание для события безопасности, и записывает сформированное сообщение аудита в журнал сообщений MS Windows данного ПК;
- модуль «Сигнализация (на клиенте)» осуществляет передачу сообщений аудита, относящихся к оповещениям «сигнализации» в подсистему сетевого обмена для дальнейшей передачи по сети на сервер;
- модуль «Сбор сообщений аудита» (на клиенте) осуществляет чтение записей аудита из «журнала аудита» и обеспечивает их передачу в подсистему сетевого обмена для дальнейшей передачи по сети на сервер.

Подсистема «Аудит» серверной части содержит следующие логические модули:

- модуль «Консоль подсистемы аудита» обеспечивает просмотр записей аудита из БД при помощи графического интерфейса;
- модуль «Служба соединения консоли с сервером» обеспечивает связь модуля «Консоль управления» с другими службами сервера и обмен данными между ними, осуществляет разграничение доступа к управлению СЗИ;
- модуль «Монитор сигнализации» (на сервере) выполняет чтение записей аудита из БД сервера, а также осуществляет запись сообщений аудита в БД, получает от подсистемы сетевого обмена данные аудита и осуществляет запись полученных сообщений аудита в БД;
- модуль «Сбор сообщений аудита» (на сервере) получает сообщения аудита, относящихся к оповещениям «сигнализации» от подсистемы сетевого обмена.

Подсистема «Контроль портов и съемных МНИ» клиентской части содержит следующие логические модули:

- модуль «Получение настроек» получает по запросу настройки для контроля портов и съемных МНИ (включая USB-носители) от подсистемы «Управление и администрирование»;
- модуль «Контроль портов съемных МНИ и прав доступа к съемным МНИ» осуществляет контроль установленного разрешения или запрета доступа пользователей к определенным типам портов съемных USB-устройств;
- модуль «Контроль подключения съемных USB-носителей» осуществляет идентификацию подключаемого USB-носителя или класса USB-носителей, контроль установленного разрешения или запрета на подключение и использование USB-носителя или класса USB-носителей, контроль установленной связи с пользователем

конкретного USB-носителя или класса USB-носителей, контроль установленной для конкретного USB-носителя опции «только чтение»;

Подсистема «Контроль целостности и надежное восстановление СЗИ» клиентской части содержит следующие логические модули:

- модуль «Контроль целостности запускаемых файлов СЗИ» осуществляет контроль целостности исполняемых файлов служб СЗИ при запуске клиента СЗИ, до запуска файлов СЗИ операционной системой по списку контроля целостности файлов СЗИ. Модуль выполняет расчет контрольных сумм файлов и сравнение их с эталонными контрольными суммами, которые содержатся в БД, и при необходимости, выполняет восстановление поврежденных файлов из БД;
- модуль «Контроль и восстановление служб СЗИ» осуществляет периодический контроль работы запущенных служб клиента СЗИ по списку контроля целостности файлов СЗИ. При аварийном завершении работы запущенных служб СЗИ, модуль осуществляет их повторный перезапуск;
- модуль «Контроль целостности и восстановление файлов СЗИ» осуществляет периодический контроль целостности исполняемых файлов и библиотек служб СЗИ. Модуль выполняет расчет контрольных сумм файлов и сравнение их с эталонными контрольными суммами файлов, которые записаны БД, при необходимости, модуль осуществляет восстановление поврежденных исполняемых файлов служб СЗИ используя эталонные копии файлов СЗИ, которые записаны в БД.

Подсистема «Идентификация и аутентификация пользователей» клиентской части содержит следующие логические модули:

- модуль «Идентификация и аутентификация» осуществляет идентификацию и аутентификацию пользователей при попытке входа на ПК, содержит библиотеки расчета хеш-функций;
- модуль «Интерфейс взаимодействия с графической подсистемой MS Windows» обеспечивает интерфейс взаимодействия пользователя с графической подсистемой аутентификации пользователей MS Windows;

Подсистема «Контроля прав доступа» клиентской части содержит следующие логические модули:

- модуль «Получение настроек» получает от подсистемы «Управление и администрирование» настройки контроля прав доступа пользователей к файловым объектам на жестких дисках и съемных МНИ (список прав дискреционного доступа, список прав мандатного доступа, список логических устройств, на которых должно выполняться гарантированное удаление файлов);
- модуль «Разграничение прав доступа и гарантированное удаление файлов» используя полученные настройки, осуществляет разграничение дискреционных и

мандатных прав доступа пользователей к файловым объектам, осуществляет гарантированное удаление файлов на указанных в настройках логических томах;

- модуль «Сетевой мандатный доступ (на клиенте)» получает сетевые права мандатного доступа всех пользователей, которые выполнили вход на своих удаленных ПК и пытаются выполнить сетевой удаленный вход на данный ПК;
- модуль «Гарантированное удаление файлов по требованию» предназначен для гарантированного удаления остаточной информации при удалении файлов;
- модуль «Сетевой мандатный доступ (на сервере)» осуществляет централизованный сбор данных о правах мандатного доступа пользователей, которые выполнили вход на своих ПК, подключенных к сети, передает полученные данные через подсистему «сетевого обмена» на все другие клиенты СЗИ, которые установлены на ПК и подключены к сети.

Подсистема «Контроль процессов» клиентской части содержит следующие логические модули:

- модуль «Получение настроек» получает настройки контроля запуска процессов («список разрешенных процессов») от подсистемы «Управление и администрирование»;
- модуль «Контроль запуска разрешенных процессов» осуществляет на ПК контроль запуска процессов, включенных в «список разрешенных процессов»;
- модуль «Очистка оперативной памяти» отслеживает завершение процессов в оперативной памяти, и после завершения процесса, осуществляет очистку свободного адресного пространства оперативной памяти.

Подсистема «Контроль целостности файлов» клиентской части содержит следующие логические модули:

- модуль «Расчет контрольных сумм» осуществляет расчет эталонных контрольных сумм файлов, которые затем используются при контроле целостности файлов;
- модуль «Контроль целостности и восстановление файлов» осуществляет контроль целостности файлов при помощи расчета контрольных сумм файлов, и сравнения с эталонными контрольными суммами, при необходимости, осуществляет восстановление поврежденных файлов из эталонных копий файлов.

Подсистема «Контроль аппаратно-программной среды» клиентской части содержит следующие логические модули:

- модуль «Запуск контроля целостности среды» получает настройки от подсистемы «Управление и администрирование» и передает их модулю «Запуск контроля целостности среды», который собирает данные о составе начальной конфигурации аппаратных и программных средств, установленных на ПК, и записывает их в БД;
- модуль «Контроль целостности среды» записывает и получает данные о

конфигурации аппаратных и программных средств ПК, хранящихся в БД.

Подсистема «Контроль печати» клиентской части содержит следующие логические модули:

- модуль «Контроль операций печати» осуществляет контроль заданных разрешений для приложений печати, запускаемых от имени пользователей на распечатку файлов на принтере;
- модуль «Принтпроцессор печати» осуществляет маркировку страниц документов, направленных на печать, осуществляет управление виртуальным принтером и процессом печати файлов.

Подсистема «Сетевой обмен» клиентской и серверной частей содержит следующие логические модули:

- модуль «Сервер сетевого обмена» осуществляет обмен данными по сети Ethernet между сервером СЗИ и клиентами СЗИ, установленными на защищаемых ПК. Модуль осуществляет прием и передачу данных по сети по протоколам TCP/IP и OpenSSL;
- модуль «Клиент сетевого обмена» осуществляет обмен данными по сети Ethernet между клиентами СЗИ. Модуль осуществляет прием и передачу данных по сети по протоколам TCP/IP и OpenSSL;
- модуль «Контроль сетевого мандатного доступа» осуществляет контроль сетевого доступа пользователей, которые подключаются по сети. Контроль сетевого мандатного доступа пользователей осуществляется по списку IP-адресов ПК (хостов), подключенных к сети.

Подсистема «Развертывание» функционирует на клиентской и серверной частях СЗИ и осуществляет сетевую инсталляцию и развертывание клиентов СЗИ. Подсистема содержит следующие логические модули:

- модуль «Консоль подсистемы развертывания» предназначен для управления процессом удаленного сетевого развертывания клиентов СЗИ;
- модуль «Служба соединения консоли с сервером» обеспечивает связь модуля «Консоль подсистемы развертывания» с другими службами сервера и обмен данными между ними, осуществляет разграничение доступа к управлению СЗИ;
- модуль «Сервер развертывания» осуществляет процесс развертывания клиентов СЗИ, передает необходимые инсталляционные файлы клиентов СЗИ по сети;
- модуль «Лицензирование» предназначен для установки серверных лицензий для клиентов СЗИ;
- модуль «Агент развертывания» запускается на удаленных ПК и выполняет процесс инсталляции файлов клиентов СЗИ.

Модули используют внешние программные компоненты, не входящие в состав СЗИ,

обеспечивающие работу графического пользовательского интерфейса (библиотека «Qt») с различными БД и сетевым протоколом SSL.

Перечень сокращений

БД	-	База данных
ЗПС	-	Замкнутая программная среда
НСД	-	Несанкционированный доступ
ОС	-	Операционная система
ПО	-	Программное обеспечение
ПК	-	Персональный компьютер
СВТ	-	Средства вычислительной техники
СЗИ	-	Средство защиты информации
СКЗИ	-	Средство криптографической защиты информации