ГАЗИНФОРМ СЕРВИС

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

Описание применения

Санкт-Петербург, 2019

Аннотация

Настоящий документ содержит описание применения средства защиты информации (СЗИ) от несанкционированного доступа «Блокхост-Сеть 3» (в дальнейшем – СЗИ «Блокхост-Сеть 3» или СЗИ).

В документе приведено назначение СЗИ и его основной функционал. В разделе «Описание задачи» описаны функции защиты, реализованные в СЗИ «Блокхост-Сеть 3», и разъясняется взаимодействие модулей программного обеспечения, для выполнения данного функционала.

Также документ содержит сведения об аппаратных и программных требованиях для установки клиентской и серверной части СЗИ на серверах и клиентских компьютерах, где предполагается использование СЗИ, и описываются входные и выходные данные СЗИ.

В конце документа приведен список использованных сокращений.

Содержание

1 Назначение средства защиты информации «Блокхост-Сеть 3»

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3» предназначено для защиты информационно-программных ресурсов от несанкционированного доступа в локальных вычислительных сетях (ЛВС) на базе персональных компьютеров (ПК), функционирующих под управлением операционных систем (ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

СЗИ «Блокхост-Сеть 3» обеспечивает:

- третий 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;
- второй уровень контроля отсутствия недекларированных возможностей в соответствии с руководящим документом «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Гостехкомиссия России, 1999.

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.

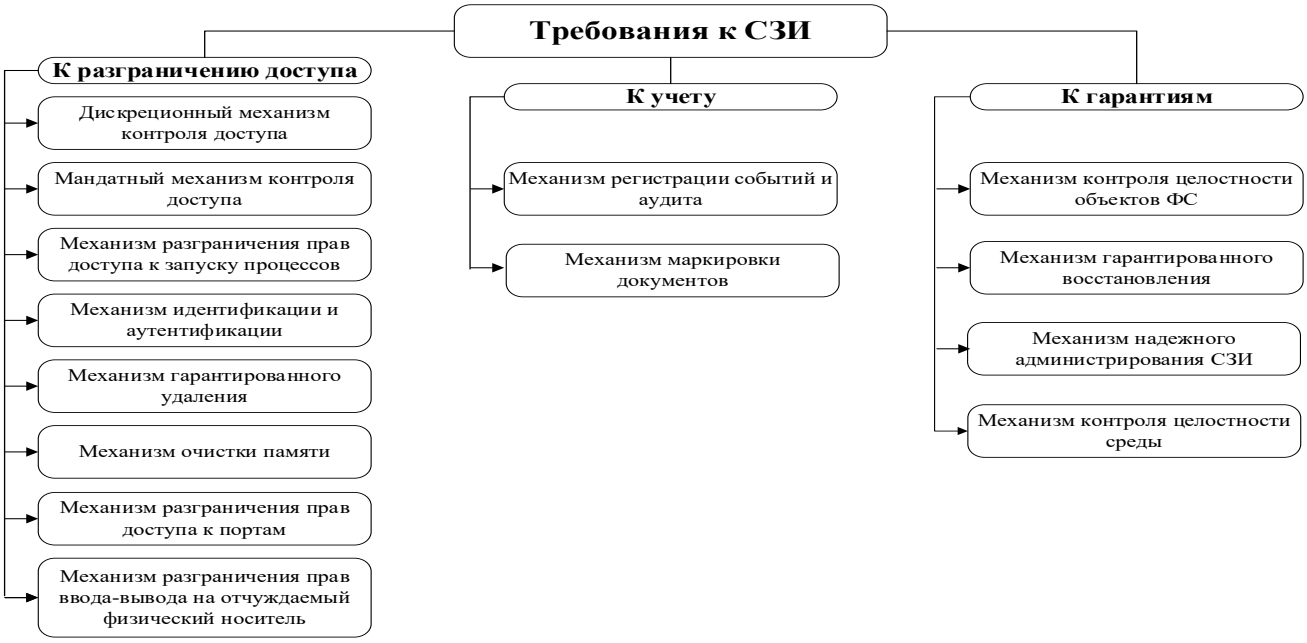

Рисунок 1 – Механизмы защиты, обеспечивающие выполнение требований к СЗИ

2 Условия применения

СЗИ «Блокхост-Сеть 3» устанавливается на ПК с процессорами, имеющими архитектуру x86 и AMD64, и функционирующие под управлением следующих ОС:

1) Клиентская часть СЗИ:

- 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 7 Home Basic SP1 (32-разрядная/64-разрядная);
- Windows 7 Home Premium SP1 (32-разрядная/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 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 10 Home (32-разрядная/64-разрядная);
- Windows 10 Pro (32-разрядная/64-разрядная);
- Windows 10 Enterprise (32-разрядная/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).

2) Серверная часть СЗИ:

- 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).

Использовать СЗИ «Блокхост-Сеть 3» для защиты от НСД терминальных серверов не следует.

Минимальные требования к производительности ПК обусловлены требованиями используемых ОС.

Рекомендуется наличие дисковода 3,5"; COM-, USB- и LPT-портов; необходимо наличие сетевой карты (при использовании варианта с удаленным управлением СЗИ «Блокхост-Сеть 3»).

Дополнительно на ПК должно быть установлено следующее программное обеспечение (ПО):

- .NET Framework 4.5.2;
- распространяемый пакет Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015;
- обновление системы безопасности KB3033929 (для ОС Windows 7 и Windows Server 2008/2008R2).

При использовании персональных идентификаторов на ПК должно быть установлено следующее ПО:

- драйверы для устройств eToken и SafeNet eToken, ruToken, JaCarta, ESMART

Token, AvBign.

При входе в ОС Windows с использованием цифровых сертификатов пользователей необходимо:

- установить СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2;
- при использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

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.

СЗИ «Блокхост-Сеть 3» может работать в многопользовательском режиме использования ПК, когда на одном компьютере работают несколько пользователей, имеющих разные права доступа к информационным ресурсам, а обрабатываемая информация имеет разные уровни конфиденциальности.

Настройку параметров СЗИ должен выполнять только администратор безопасности (АБ).

СЗИ «Блокхост-Сеть 3» имеет следующие ограничения:

1) Установка СЗИ «Блокхост-Сеть 3» должна выполняться на диск C:\.

2) На жестком диске не должно быть других установленных операционных систем.

3) На компьютере не должно быть динамических дисков, работу с ними «Блокхост-Сеть 3» не поддерживает. Также не поддерживается гарантированное удаление на твердотельных магнитных накопителях (SSD-дисками).

4) 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.

Использование антивирусных программ допускается после проверки их совместимости с программным комплексом СЗИ.

Для корректной работы консолей администрирования СЗИ необходимо отключить параметр безопасности локальной политики ОС Windows **Системная криптография:**

использовать FIPS совместимые алгоритмы для шифрования, хеширования и подписывания.

Эксплуатация СЗИ «Блокхост-Сеть 3» совместно с ОС семейства Windows допускается только в условиях выполненной активации операционной системы.

Для эксплуатации и эффективного применения СЗИ «Блокхост-Сеть 3» необходимо использование лицензионного системного ПО.

Не рекомендуется ставить на контроль системные папки, так как это приводит к большому числу записей в журналы аудита и может повлиять на работоспособность СЗИ.

3 Описание задачи

Основной задачей СЗИ «Блокхост-Сеть 3» является защита информации от несанкционированного доступа и основана на перехвате обращений прикладных программ и/или системного ПО к ресурсам ПК и предоставлении доступа к этим ресурсам в соответствии с правилами разграничения доступа, установленными АБ.

Клиентская часть СЗИ «Блокхост-Сеть 3» выполняет следующие функции защиты:

- идентификация и аутентификация АБ и пользователей, работающих на ПК с СЗИ «Блокхост-Сеть 3», в том числе с применением персональных электронных идентификаторов (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 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205, SafeNet eToken 7200, SafeNet eToken 7300, SafeNet eToken 4100, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, JaCarta LT, 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, ESMART Token (USB-ключ и смарт-карта), Avest Token, ruToken, ruToken S, ruToken Lite, ruToken ЭЦП, USB-накопители, дискеты 3,5”), также возможно использование персонального идентификатора пользователя, хранящегося в области недоступной для непривилегированного пользователя (персональный идентификатор пользователя в реестре Windows);
- возможность двухфакторной аутентификации пользователей средствами СЗИ при входе в ОС Windows с использованием цифровых сертификатов пользователей. Сертификаты могут храниться на вышеуказанных персональных электронных идентификаторах eToken, SafeNet eToken, ruToken, JaCarta, ESMART Token и Avest Token;
- дискреционный и мандатный механизмы контроля доступа к информационным ресурсам ПК в соответствии с заданными параметрами безопасности;
- контроль целостности файловой системы;
- гарантированное восстановление функций безопасности СЗИ;
- аудит и регистрация доступа к информационным ресурсам;
- очистка памяти и гарантированное удаление информационных ресурсов;
- контроль вывода документов на печать, маркировка документов;
- защита ввода и вывода информации на отчуждаемые физические носители;
- контроль запуска процессов;
- управление идентификаторами входа;

- временное разграничение доступа пользователей к рабочей станции;
- администрирование СЗИ с помощью графического интерфейса АБ, который включает иерархию серверов, настройки групп пользователей и рабочих станций;
- контроль целостности программно-аппаратной среды.

Данные функции реализуются в СЗИ путем взаимодействия модулей специализированного программного обеспечения (СПО), входящих в состав СЗИ.

Серверная часть (сервер безопасности) СЗИ «Блокхост-Сеть 3» выполняет следующие функции:

- присоединение клиентских частей к сети СЗИ от несанкционированного доступа (НСД) «Блокхост-Сеть 3»;
- выполнение удаленной установки клиентских частей СЗИ «Блокхост-сеть 3» на рабочие станции из серверной консоли администрирования СЗИ;
- выполнение удаленной установки программного обеспечения на рабочие станции в сети из консоли системы развертывания и аудита Блокхост-сеть;
- удаленное управление настройками клиентов СЗИ от НСД «Блокхост-Сеть 3»;
- управление групповыми политиками безопасности;
- взаимная аутентификация клиент-сервер при сетевом взаимодействии;
- сетевое мандатное разграничение;
- централизованный сбор и просмотр данных аудита;
- присоединение и управление параметрами подчинённых серверов.

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.

В СЗИ ведется список разрешенных пользователей для входа в систему, который может быть изменен только АБ. 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 АБ.

В системе реализованы следующие способы идентификации и аутентификации пользователя:

- вход в систему по паролю, вводимому пользователем с клавиатуры;

- вход в систему по ключевому носителю с паролем (пароль в зашифрованном виде хранится на ключевом носителе);
- вход в систему с предъявлением цифрового сертификата, записанного на ключевом носителе.

Дополнительно в СЗИ предусмотрена возможность установки ограничения на минимальную длину пароля в настройках политик безопасности, а также на время доступа пользователя в систему.

Механизм аутентификации СЗИ «Блокхост-Сеть 3» можно полностью отключить, активировав ***Мягкий режим работы*** СЗИ (подробнее в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности»). При включенном мягком режиме вход в операционную систему может выполнить любой доменный или локальный пользователь рабочей станции, если это не противоречит установленным в домене политикам.

Мягкий режим работы, а также режим аутентификации ***Доверять аутентификации Windows*** (данный режим автоматически устанавливается при добавлении новых учетных записей в СЗИ) используются для первичной настройки средства защиты, до начала эксплуатации. В данных режимах средство защиты не обеспечивает выполнение заявленных функций безопасности. Эксплуатировать СЗИ в описанных режимах для защиты станции **запрещено**.

3.2 Дискреционный механизм контроля доступа к ресурсам

В качестве субъектов доступа в СЗИ рассматриваются поименованные пользователи, в т.ч. и администратор безопасности. Объектами доступа выступают объекты файловой системы (логические диски, каталоги и файлы).

Дискреционный механизм контроля доступа к ресурсам включает:

- контроль доступа к объектам файловой системы;
- разграничение прав доступа к запуску процессов.

СЗИ предоставляет право АБ после его авторизации изменять правила разграничения доступа. При этом может изменяться как список пользователей и контролируемых объектов защиты, так и права доступа к объектам защиты.

3.2.1 Контроль доступа к объектам файловой системы

Для каждой пары субъект-объект в явном виде можно задавать следующие типы доступа:

- только чтение,
- только запись,
- полный доступ (комбинация первых двух типов доступа).

При определении прав доступа конкретного пользователя к объектам файловой структуры учитывается иерархия объектов (логический диск, каталог, подкаталог, файл), а также дополнительные ограничения на доступ процессов к объектам файловой системы (ФС).

При запрете файла на чтение его нельзя переименовать/переместить, запустить (для исполняемых файлов), но можно записать в файл (при использовании приложений, поддерживающих такую возможность) и удалить файл. При запрете каталога на чтение все его содержимое также имеет запрет по чтению.

При запрете файла на запись будет доступно чтение файла или его запуск (для исполняемых файлов), а переименование/перенос, удаление и запись в него будут недоступны. При запрете каталога на запись нельзя будет каким-либо образом изменить его содержимое.

Полное описание процедур настроек СЗИ по разграничению прав доступа пользователя к каталогам и файлам, а также процессов к ресурсам приведено в описании дискреционного механизма доступа в эксплуатационной документации (ЭД) на средство.

3.2.2 Разграничение прав доступа на запуск процессов

Механизм позволяет накладывать ограничения на запуск определенных процессов разным пользователям. Под запуском процесса понимается попытка открытия исполняемого файла. Механизм функционирует в режиме замкнутой программной среды. АБ создает список разрешенных к запуску процессов (программ). Пользователь может запускать процессы только из данного списка. В состав списка разрешенных процессов, помимо прикладных программ пользователя, включаются приложения, необходимые для начала сессии пользователя в ОС Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

3.2.3 Дискреционная модель разграничения прав доступа пользователя к объектам ФС

В дискреционной модели прав доступа пользователя к объектам файловой системы ПК необходимо учитывать:

1) Запрещения для каталогов автоматически распространяются на вложенные объекты.

2) Дискреционная модель разграничения доступа действует равно как на пользовательские файлы, так и на файлы операционной системы.

3) Приведенные выше правила действуют при отсутствии ограничений со стороны встроенных средств защиты ОС с файловой системой NTFS. Запрещения, установленные в рамках ОС, перекрывают разрешения СЗИ и наоборот.

4) Дискреционная модель разграничения доступа распространяется на все логические диски, в том числе служащие для отображения содержимого отчуждаемых физических носителей, которые можно рассматривать в данной модели как каталоги и применять к ним все правила, используемые для каталогов.

5) Механизм разграничения доступа к устройствам (логическим и съемным дискам) СЗИ для ОС перекрывает механизм разграничения доступа для каталогов и файлов. Для доступа к устройствам действует политика: «Что не разрешено - то запрещено».

6) При установке дополнительных разграничений доступа для процессов отдельно от разграничений доступа для пользователя запреты для процессов перекрывают разрешения для пользователей.

7) При установке дополнительных разграничений доступа для процессов вместе с правами пользователя запреты для пользователя перекрывают разрешения для процессов и наоборот.

8) Доступ к каталогу, содержащему файлы СЗИ «Блокхост-Сеть 3», запрещен для всех пользователей.

9) Для противостояния потенциальным уязвимостям среды функционирования СЗИ «Блокхост-Сеть 3» (ОС Windows) АБ должен для каждого пользователя средствами дискреционного механизма СЗИ запретить запись в следующие каталоги:

- корневой каталог ОС Windows, описанный переменной окружения *%WINDIR%*;
- каталог размещения СЗИ «Блокхост-Сеть 3» (по умолчанию это: *c:\blockhost*);
- каталог установки программ, описанный переменной окружения *%PROGRAMFILES%*;
- каталог установки программ, описанный переменной окружения *%PROGRAMFILES(x86)%* – для 64-битных ОС;
- директории, указанные в системной переменной *PATH*.

По умолчанию все процессы имеют права на полный доступ ко всем объектам.

3.3 Мандатное разграничение контроля доступа к ресурсам

Мандатное разграничение контроля доступа в СЗИ «Блокхост-Сеть 3» реализуется посредством классификационных уровней. Классификационный уровень является комбинацией иерархических и неиерархических категорий, назначаемых каждому объекту (диску, папке, файлу) и субъекту (пользователю, процессу) доступа.

Классификационные метки (иерархическая категория) присваиваются субъектам/объектам из диапазона чисел 1-255 и соответствуют их месту (уровню) иерархии в пределах иерархической категории. Иерархическая категория определяет уровень конфиденциальности защищаемой информации (чем метка больше, тем выше степень конфиденциальности). Иерархическая метка субъекта определяет права доступа к соответствующей иерархической категории. Неиерархические категории выступают в качестве ограничений по доступу субъектов к объектам, соответствующих неиерархических категорий.

Иерархические метки и неиерархические категории создаются и назначаются субъектам и объектам доступа администратором безопасности. Одному субъекту или объекту доступа может быть назначена только одна (максимальная) иерархическая метка. Одному объекту или субъекту доступа может быть назначено несколько неиерархических категорий.

Иерархические метки и неиерархические категории создаются и назначаются субъектам и объектам доступа администратором безопасности в соответствии с правилами:

1) Задаются значения иерархических меток и имена неиерархических категорий.

2) Каждому пользователю (субъекту) назначается метка и категория (или несколько категорий) – определяется уровень доступа.

3) Иерархические метки и неиерархические категории (соответствующие уровни конфиденциальности) присваиваются ресурсам (объектам доступа).

Устанавливаются следующие отношения между неиерархическими категориями субъектов и объектов:

- пользователь, отнесённый к соответствующей категории (субъект), имеет полный доступ (Чтение, Запись) к объекту, отнесенному к этой же категории;
- каждому пользователю, отнесённому к соответствующей категории (субъекту), запрещается какой-либо вид доступа (Чтение, Запись) к объектам отнесенным к другим категориям, не совпадающими с категорией этого пользователя;
- каждому пользователю, отнесённому к соответствующей категории (субъекту), устанавливается право доступа только «Чтение» ко всем остальным (не категорированным) ресурсам системы.

Общие правила разграничения доступа мандатного механизма состоят в следующем:

1) Субъект получает доступ к объекту по чтению, если его метка не меньше метки объекта и неиерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта.

2) Субъект получает доступ к объекту по записи, если его метка равна метке объекта и все неиерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

3.4 Защита ввода-вывода на отчуждаемый физический носитель

В СЗИ «Блокхост-Сеть 3» реализован механизм разграничения доступа пользователей к отчуждаемым носителям информации. Ввод-вывод на отчуждаемый носитель доступен для данного субъекта только в том случае, если уровень конфиденциальности носителя не выше уровня конфиденциальности субъекта.

Реализация механизма разграничения доступа к отчуждаемым носителям информации в СЗИ «Блокхост-Сеть 3» заключается в предоставлении АБ возможности санкционировать доступ каждого пользователя к следующим устройствам:

- съемные USB-накопители;
- CD/DVD- диски;
- дискеты 3,5”.

Разграничение прав доступа к портам (COM, LPT, USB) подразумевает разрешение или запрет на использование порта. Настройки данного механизма вступают в силу только после перезагрузки ОС. Для USB-портов допускается привязка к учетным записям пользователей, разрешенных для использования на ПК USB-устройств.

3.5 Механизм контроля печати

Механизм контроля печати осуществляет аудит процесса печати и маркировку конфиденциальных документов, выводимых на печать.

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

Маркировка включает в себя вывод настраиваемого штампа в колонтитулах страниц печатаемых документов.

Штамп может содержать следующие поля:

- дату/время распечатки;
- имя файла документа;

- уровень конфиденциальности документа;
- порядковый номер в формате «текущий номер страницы из общего числа листов»;
- имя пользователя, производившего печать документа;
- имя рабочей станции, с которой производилась печать документа;
- имя принтера, с которого производилась печать документа.

Механизм контроля печати имеет следующие ограничения:
1) 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;
2) 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;
3) механизмом контроля печати поддерживается работа с печатающими устройствами, для которых установлены драйвера поддержки PCL (работа механизма контроля печати с печатающими устройствами, для которых установлены драйвера поддержки PostScript не гарантируется – возможность печати на подобных устройствах может быть заблокирована);
4) в семействе Windows 8.1 не поддерживается работа с приложениями, использующими metro-интерфейс;
5) в режиме маркировки документов не поддерживается цветная печать – при печати цветного текста (изображения) вывод на печать происходит в черно-белом варианте;
6) блокируется возможность печати из браузера Mozilla Firefox;
7) блокируется возможность печати содержимого страницы браузера Internet Explorer (версия 11) при включенном контроле учетных записей (UAC).

3.6 Механизм очистки остаточной информации

Механизм очистки остаточной информации объединяет в себе механизм очистки памяти и механизм гарантированного удаления.

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

Модуль очистки памяти СЗИ контролирует завершение поставленных на контроль процессов и после их завершения производит очистку всей свободной физической памяти путем записи в нее маскирующей информации.

Гарантированное удаление выполняется модулем диспетчера доступа СЗИ. При

попытке удаления поставленного на контроль файла диспетчер доступа запрещает удаление средствами ОС и запускает модуль гарантированного удаления. Поставленные на контроль файлы удаляются путем трехкратного затирания их содержимого по специальному алгоритму, который исключает считывание остаточной информации на диске после удаления.

3.7 Механизм контроля целостности и гарантированного восстановления

Расчет контрольных сумм, установленных на контроль целостности файлов, должен осуществляться по алгоритму CRC-32 и при обнаружении СЗИ нарушений контрольных сумм (КС) должно происходить его надежное восстановление без привлечения АБ.

Подобный механизм используется для контроля целостности и надежного восстановления программных модулей СЗИ после сбоев. При запуске средства защиты автоматически создаются резервные копии всех программных модулей СЗИ и рассчитываются контрольные суммы файлов резервных копий программных модулей СЗИ по указанному выше алгоритму. Проверка целостности осуществляется по заданному АБ временному интервалу в процессе работы СЗИ. При обнаружении нарушений выполняется перезагрузка ОС с восстановлением модулей из резервных копий.

3.8 Механизм регистрации событий и аудита

Механизм регистрации событий и аудита предназначен для отслеживания событий и регистрации обращения к защищаемым ресурсам. а также при срабатывании всех механизмов защиты. Централизованный сбор и просмотр данных аудита, из настроенного АБ перечня, осуществляется в консоли системы развертывания и аудита Блокхост-сеть. 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 консоли системы развертывания и аудита Блокхост-сеть АБ доступен следующий функционал для работы с событиями аудита:

- 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.

Информация анализируется и события, входящие в перечень, определенный администратором безопасности, отправляются сетевому монитору безопасности на сервер безопасности.

3.9 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.

Механизм контроль целостности среды включает в себя:

- 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).

Контроль параметров устройства осуществляется в момент запуска соответствующей службы. Получение информации о перечисленных устройствах осуществляется через интерфейс WMI. Соответствие контролируемых устройств классам WMI и поля, по которым осуществляется контроль изменения конфигурации, описаны в таблице 2.

Таблица 2 – Соответствие устройств классам WMI

Контролируемое устройство	**Класс WMI**	**Контроль изменения конфигурации осуществляется по следующим полям**
Процессор	Win32_Processor	• Name (модель процессора; например «Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz»); • DeviceID (ИД в компьютере).
Жесткий диск	Win32_DiskDrive	• 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	Win32_CDROMDrive	• SerialNumber (серийный номер); • Manufacturer (производитель устройства)MediaType (тип поддерживаемых носителей; например «DVD Writer»); • DeviceID (ИД в компьютере).
Сетевой адаптер	Win32_NetworkAdapter	• 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	Win32_BaseBoard	• 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).
Видео-карта	Win32_VideoController	• 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	Win32_PhysicalMemory	• BankLabel (метка банка, в котором находится память;

оперативной памяти		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).

3.10 Механизм управления идентификаторами

Механизм управления идентификаторами предназначен для управления ключевыми носителями. Под ключевым носителем подразумевается: eToken, SafeNet eToken, JaCarta PRO, JaCarta ГОСТ, JaCarta PKI, JaCarta-2, JaCarta LT, AvBign, ESMART Token и ruToken, USB-накопитель, дискета. В качестве ключевого носителя пользователя также может применяться персональный идентификатор пользователя в реестре Windows.

Механизм управления идентификаторами позволяет выполнять следующие действия:

- менять PIN-код ключевого носителя;
- получать информацию по носителю;
- менять имя зарегистрированного носителя (для ruToken);
- отвязывать пользователей от носителя;
- отвязать носитель от рабочей станции;
- редактировать сгенерированные станции;
- задать время жизни носителя.

Данные по каждому носителю отображаются в консоли на одном уровне с настройками пользователя (дополнительный узел в дереве «идентификаторы входа»).

Каждому пользователю соответствует один или более носитель, идентификация пользователя будет осуществляться по SID (данные о привязке пользователя, носителя и рабочей станции хранится на носителе и в базе настроек рабочей станции).

Администратор имеет возможность редактировать любой носитель, даже если он не присвоен пользователям на данной машине, в специальном разделе, где будут отображаться пользователи, ассоциированные с данным идентификатором, и машины, с которыми ассоциируется носитель.

3.11 Механизм администрирования СЗИ

Доступ к этому модулю предусматривает наличие у пользователя прав администратора безопасности.

Механизм администрирования обеспечивает настройку параметров работы СЗИ. Параметры СЗИ делятся на системные, которые задают правила доступа всех пользователей и индивидуальные, которые относятся к правилам доступа конкретных пользователей. Для удобства работы предусмотрен режим ввода настроек с использованием шаблонов.

После запуска СЗИ администратор безопасности может выполнять следующие действия:

- создание, изменение, удаление субъектов (пользователей и процессов), их уровней доступа, паролей пользователей с возможностью установки для пользователей различных шаблонов настроек доступа;
- назначение объектам уровней конфиденциальности;
- установка контролируемых объектов (файлы, папки, диски, USB-, COM-, LPT-порты) для конкретных субъектов с указанием атрибутов доступа;
- установка замкнутой программной среды;
- формирование списков процессов, разрешенных для запуска;
- формирование списка файлов, целостность которых требуется контролировать;
- формирование списка процессов, по завершению работы которых требуется очистка памяти;
- делегирование прав доступа по администрированию СЗИ пользователям (такие пользователи должны быть включены в группу администраторов текущей рабочей станции);
- управление аппаратными идентификаторами входа (изменение PIN-кода, задание времени жизни носителя, редактирование параметров станций и др.);
- управление групповыми политиками безопасности;
- формирование списка процессов для контроля печати и настройка колонтитулов для выводимой информации;
- формирование списка объектов контроля целостности среды;
- просмотр и анализ данных аудита в консоли системы развертывания и аудита Блокхост-сеть, настройка перечня регистрируемых событий;
- выполнение удаленной установки клиентских частей СЗИ «Блокхост-сеть 3» на рабочие станции, а также программного обеспечения на рабочие станции в сети из консоли системы развертывания и аудита Блокхост-сеть.

4 Входные и выходные данные

Входными данными для СЗИ «Блокхост-Сеть 3» являются:

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

Настройки системы защиты хранятся в клиентской и серверной базах данных, представленных в виде текстового файла определенной структуры. Данный файл содержит 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 3». Описание программы».

Выходными данными СЗИ «Блокхост-Сеть 3» 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 системы развертывания и аудита (СРиА). Полный перечень событий, фиксируемых в консоли СРиА приведен в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности. Приложение 5».

5 Программные модули СЗИ «Блокхост-Сеть 3»

СЗИ «Блокхост-Сеть 3» включает следующие программные модули, реализующие механизмы защиты и их взаимодействие в составе программного обеспечения СЗИ:

- модуль разграничения прав пользователей на доступ к ресурсам файловой системы и модуль гарантированного удаления;
- модуль графического интерфейса клиента безопасности;
- модуль графического интерфейса администратора;
- модуль определения информации о ресурсах ПК;
- модуль получения и установки настроек для сетевых подключений;
- модуль контроля печати;
- модуль подсистемы аутентификации;
- модуль контроля целостности среды;
- модуль контроля целостности файловой системы;
- модуль запуска и контроля состояния СЗИ;
- модуль работы с клиентской базой данных СЗИ;
- модуль сбора событий аудита клиента безопасности;
- модуль сбора событий аудита сервера безопасности;
- модуль развертывания клиентов безопасности;
- модуль агента развертывания;
- модуль диспетчера соединений клиента безопасности;
- модуль диспетчера соединений сервера безопасности;
- модуль клиента сетевого взаимодействия;
- модуль сервера сетевого взаимодействия;
- модуль монитора безопасности сетевого администратора;
- модуль настроек удаленных клиентов безопасности;
- модуль работы с серверной базой данных СЗИ;
- модуль сетевого мандатного режима;
- модуль очистки памяти;
- модуль контроля классификационного уровня в сети.

Описание логической структуры исполняемых модулей серверной и клиентской частей СЗИ «Блокхост-Сеть 3» и связи между ними приведены в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Описание

программы».

Входными данными для работы модуля подсистемы аутентификации являются списки зарегистрированных пользователей и их пароли, хранимые в базе данных (БД), синхронизированные с БД пользователей, зарегистрированных в операционной системе Windows. При включении компьютера этот модуль начинает работать на последнем этапе загрузки операционной системы. Все попытки пройти аутентификацию записываются считываются модулем сбора событий аудита. При успешном доступе пользователя в систему его идентификационное имя фиксируется в БД, считывается модулем разграничения прав доступа и используется для контроля всех последующих его действий.

Модуль разграничения прав доступа является драйвером файловой системы и загружается до запуска графической оболочки ОС. Драйвер запускается после прохождения пользователем аутентификации и начинает контролировать доступ к защищаемым объектам на основе информации из БД. Все обращения к защищаемым ресурсам контролируются и фиксируются в БД журналов аудита модулем сбора событий аудита.

Модуль контроля целостности и гарантированного восстановления и модуль регистрации событий являются собственными сервисами (службами), запускаемыми при загрузке системы и постоянно находятся в памяти до перезагрузки компьютера. Модули используют для своей работы настройки СЗИ и фиксируют в журналах аудита нарушение целостности поставленных на контроль файлов.

С помощью модуля графического интерфейса клиента безопасности и администратора производится настройка параметров системы защиты и сохранение их в БД настроек. Для того чтобы новые параметры вступили в силу, необходимо сменить сеанс пользователя. Действия администратора безопасности по изменению настроек СЗИ фиксируются модулем сбора событий аудита.

Модуль определения информации о ресурсах ПК получает данные о ресурсах ПК, списках пользователей, запущенных процессах и обслуживает запросы на получение данной информации как от локального модуля администратора, так и удаленные запросы.

Диспетчер настроек удаленных клиентов безопасности перенаправляет запросы о доступных ресурсах клиента безопасности модулю определения информации о ресурсах ПК данного клиента безопасности. Так же он обрабатывает информацию о подключении и отключении клиентов безопасности, информируя об этом модуль графического интерфейса администратора для разрешения или блокирования возможности их администрирования.

Модуль получения настроек для сетевых подключений обрабатывает запросы модуля

разграничения прав доступа на загрузку настроек вошедших сетевых пользователей или запуска процессов от имени пользователя, не вошедшего интерактивно. Модуль обрабатывает запрос о текущем мандате работы пользователей на рабочей станции, что необходимо для организации сетевого мандатного режима.

Модуль очистки памяти контролирует работающие процессы и очищает память, при завершении процесса, поставленного на контроль.

Диспетчеры соединений клиента и сервера безопасности является диспетчерами, которым направляются запросы на получение рабочих параметров при загрузке системы, входе нового пользователя или перезапуске модулей.

Модули работы с клиентской и серверной базой данных СЗИ обрабатывают запросы на получение и сохранение настроек, кодирование и раскодирование файлов конфигурации с параметрами работы системы и разграничениями для пользователей.

В модуле аудита фиксируются все события аудита от модулей СЗИ, которые сохраняются в БД аудита. Кроме того, производится фильтрация записей аудита для выявления событий из определенного перечня, которые отправляются модулю монитора безопасности сетевого администратора для сигнализации о нарушениях безопасности.

Модуль контроля печати блокирует возможность печати на установленный виртуальный принтер и отслеживает отправку пользователем документа на другие установленные принтеры. Когда пользователь отправляет какой-либо документ на принтер, определяется имя пользователя, домен (если есть), к которому принадлежит пользователь, процесс, который производит печать, и принтер, на который производится печать. После этого задание перенаправляется на виртуальный принтер, на котором производится проверка полномочий печати и добавление колонтитулов на выводимые страницы.

Модули клиента и сервера сетевого взаимодействия предназначены для защищенного удаленного управления разграничениями полномочий пользователей на удаленной рабочей станции. Они осуществляют передачу данных по протоколу TCP/IP, взаимную аутентификацию клиента безопасности и сервера удаленного управления СЗИ, осуществляют обмен конфиденциальными данными по защищенному каналу, управляют потоками данных для различных модулей СЗИ.

Модуль монитора безопасности сетевого администратора выдает сетевому администратору информацию о попытках нарушения безопасности, о подключении рабочих станций к сети, о входе пользователей на локальные станции.

Модуль сетевого мандатного режима хранит список работающих машин и мандаты вошедших пользователей, что необходимо для осуществления сетевого мандатного

режима.

Модуль 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. При выявлении нарушения он передает событие об инциденте модулю аудита. Модуль контроля целостности среды взаимодействует с клиентской БД, в которой хранится эталонная программно-аппаратная конфигурация компьютера для выявления изменений в ресурсах.

Модуль контроля классификационного уровня в сети контролирует классификационные уровни объектов и субъектов, определяющие уровень конфиденциальности защищаемой информации. Информацию о классификационных уровнях объектов и субъектов модуль контроля классификационного уровня в сети получает от модуля клиента сетевого взаимодействия.

Модуль развертывания клиентов безопасности предназначен для установки программного обеспечения, в том числе клиентской части СЗИ «Блокхост-Сеть 3» на рабочие станции. Модуль развертывания клиентов безопасности отправляет модулю агента развертывания задания на установку программного обеспечения.

Модуль агента развертывания осуществляет взаимодействие с модулем развертывания клиентов безопасности и устанавливается на рабочих станциях в сети, на которые планируется установить программное обеспечение, в том числе клиентской части СЗИ «Блокхост-Сеть 3», с сервера безопасности с использованием модуля развертывания клиентов безопасности или вручную на клиенте.

Модуль запуска и контроля состояния СЗИ получает команды от модуля аутентификации и предоставляет АБ возможность санкционировать доступ каждого пользователя к устройствам. Ввод-вывод на устройства доступен для пользователя только в том случае, если уровень конфиденциальности носителя не выше уровня конфиденциальности пользователя. Модуль запуска контроля состояния СЗИ включает драйвер разграничения прав доступа к портам. Для USB-портов допускается привязка к учетным записям пользователей, разрешенных для использования на ПК USB-устройств.

Перечень сокращений

АБ	-	Администратор безопасности
АРМ	-	Автоматизированное рабочее место
БД	-	База данных
КС	-	Контрольная сумма
ЛВС	-	Локальные вычислительные сети
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
СПО	-	Специализированное программное обеспечение
ФС	-	Файловая система
ЭД	-	Эксплуатационная документация