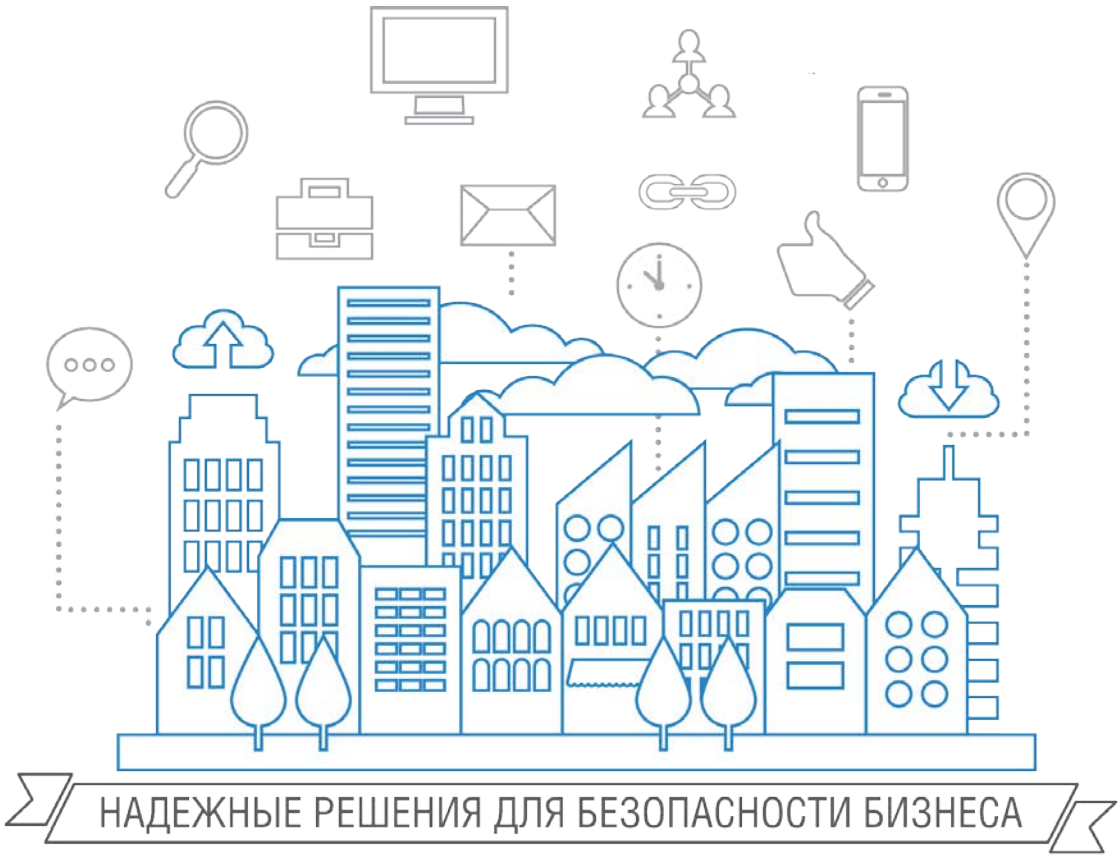
ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51
Почтовый адрес: 198096, г. Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт-Петербурге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»

Описание применения



Санкт-Петербург, 2017

Аннотация

Настоящий документ содержит описание применения средства защиты информации от несанкционированного доступа «Блокхост-сеть 2.0».

Содержание

1. Назначение средства защиты информации «Блокхост-сеть 2.0»

Средство защиты информации (СЗИ) «Блокхост-сеть 2.0» (в дальнейшем – СЗИ «Блокхост-сеть 2.0» или СЗИ) 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/Vista/7/8/8.1/2012/2012R2/10/2016.

СЗИ «Блокхост-сеть 2.0» обеспечивает:

- третий класс защищенности для 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;
- четвертый класс защищенности в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997).

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 средствах вычислительной техники (СВТ):

1) требования к разграничению доступа, предусматривающие то, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

2) требования к учету, предусматривающие то, 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 того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

Выполнение каждой группы требований обеспечивается соответствующими механизмами защиты, представленными на рисунке 1.

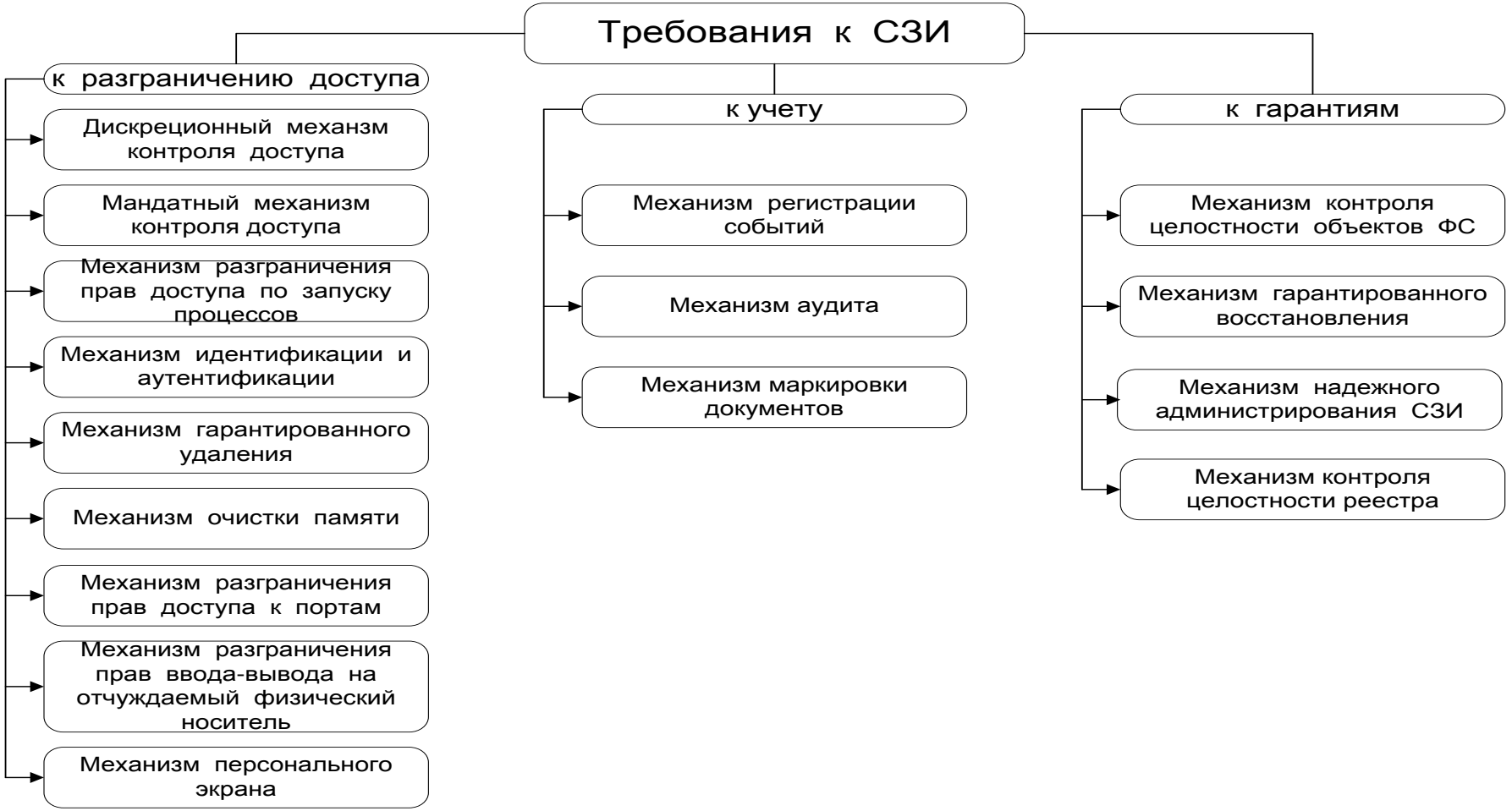


Рисунок 1. Механизмы защиты, обеспечивающие выполнение требований к СЗИ

2. Условия применения

СЗИ «Блокхост-сеть 2.0» устанавливается на ПК с процессорами, имеющими архитектуру x86 и AMD64, и функционирующие под управлением 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 Vista Business SP2 (32-разрядная);
- Windows Vista Business SP2 (64-разрядная);
- Windows 7 Home Basic SP1 (32-разрядная);
- Windows 7 Home Basic SP1 (64-разрядная);
- Windows 7 Home Premium SP1 (32-разрядная);
- Windows 7 Home Premium SP1 (64-разрядная);
- Windows 7 Professional SP1 (32-разрядная);
- Windows 7 Professional SP1 (64-разрядная);
- Windows 7 Enterprise SP1 (32-разрядная);
- Windows 7 Enterprise SP1 (64-разрядная);
- Windows 7 Ultimate SP1 (32-разрядная);
- Windows 7 Ultimate SP1 (64-разрядная);
- Windows 8/8.1 Core (32-разрядная);
- Windows 8/8.1 Core (64-разрядная);
- Windows 8/8.1 Professional (32-разрядная);
- Windows 8/8.1 Professional (64-разрядная);
- Windows 8/8.1 Enterprise (32-разрядная);
- Windows 8/8.1 Enterprise (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/Home N (32-разрядная);
- Windows 10 Home/Home N (64-разрядная);
- Windows 10 Pro/Pro N (32-разрядная);
- Windows 10 Pro/Pro N (64-разрядная);
- Windows 10 Enterprise/Enterprise N (32-разрядная);
- Windows 10 Enterprise/Enterprise N (64-разрядная);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (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).

Минимальные требования к производительности ПК обусловлены требованиями используемых ОС.

Требуется наличие дисковода 3,5"; COM-, USB- и LPT-портов; сетевой карты (при использовании сетевого варианта СЗИ «Блокхост-сеть 2.0»).

Дополнительно на компьютере должно быть установлено следующее программное обеспечение:

- .NET Framework 3.5 (для работы модуля контроля целостности реестра);
- .NET Framework 4.0 с обновлением NDP40-KB2468871 или выше (для работы консоли администрирования СЗИ);
- обновление системы безопасности KB3033929 (для ОС Windows Server 2008/2008R2);
- драйверы для устройств eToken и SafeNet eToken (любой из вариантов):
  - SafeNet Authentication Client 8.2. Подходит для всех поддерживаемых ОС, в комплект поставки СЗИ не входит.
  - eToken PKI Client 5.1 SP1 или eToken RTE 3.66 – при использовании персональных идентификаторов eToken PRO, eToken NG-FLASH, eToken NG-OTP;
  - eToken PKI Client 5.1 SP1 – при использовании персональных идентификаторов eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken PRO (Java), eToken GT (Java), eToken PRO (Java) SC, eToken PRO SC;
- драйверы для устройств ruToken, версия 4.2.4.0 и выше – при использовании персональных идентификаторов ruToken;
- драйверы «Единый клиент JaCarta» для устройств JaCarta PRO, JaCarta ГОСТ, JaCarta PKI – при использовании персональных идентификаторов JaCarta;
- драйверы «ESMART PKI Client» для устройств eSmart Token (при использовании (персональных идентификаторов eSmart Token USB 64K и eSmart Token SC 64K);
- драйверы AvBignDriver, устанавливаемые в составе пакета Avest CSP Bign, для поддержки персональных идентификаторов AvBign;
- СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2 – при организации входа пользователей в ОС с помощью сертификатов.

Для корректного отображения символов русского алфавита перед инсталляцией СЗИ на англоязычных ОС следует установить ***Русский язык*** в качестве ***Языка системы*** для программ, не поддерживающих Юникод

Перед началом установки СЗИ на ОС Windows 8/8.1/2012/2012R2 необходимо отключить встроенный антивирус ОС (Windows Defender).

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности и контролируемых рабочих станциях должны быть открыты 999 TCP порт и 5555 UDP порт.

СЗИ «Блокхост-сеть 2.0» 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.

СЗИ «Блокхост-сеть 2.0» имеет следующие ограничения:

- Установка СЗИ «Блокхост-сеть 2.0» должна выполняться на диск C:\.
- На жестком диске не должно быть других установленных операционных систем.
- На компьютере не должно быть динамических дисков, работу с ними «Блокхост-Сеть 2.0» не поддерживает. Также не поддерживается работа с твердотельными магнитными накопителями (SSD-дисками).
- 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 программам относятся:
  - средства защиты от несанкционированного доступа;
  - анализаторы файловой системы;
  - утилиты мониторинга файловой системы (ProcessMonitor и т.п.).
- 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 2.0» совместно с ОС семейства Windows допускается только в условиях выполненной активации операционной системы.
- Для эксплуатации и эффективного применения СЗИ «Блокхост-сеть 2.0» 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 2.0» является защита информации от несанкционированного доступа. Для выполнения этой задачи в СЗИ реализованы следующие функции защиты:

- дискреционный и мандатный механизмы контроля доступа к информационным ресурсам в соответствии с заданными параметрами контекста безопасности;
- идентификация и аутентификация;
- контроль целостности программ и данных;
- гарантированное восстановление функций СЗИ;
- аудит и регистрация доступа к информационным ресурсам;
- гарантированное удаление информационных ресурсов;
- контроль вывода документов на печать;
- защита ввода и вывода на отчуждаемый физический носитель информации;
- контроль запуска процессов;
- локальное и удаленное администрирование СЗИ.

Данные функции в СЗИ «Блокхост-сеть 2.0» реализуются взаимодействием модулей программного обеспечения.

3.1. Механизм идентификации и аутентификации

В механизме идентификации и аутентификации реализованы следующие функции:

- идентификация и аутентификация пользователя при входе его в систему;
- сопоставление пользователя с электронным идентификатором;
- запись пароля на парольную дискету и считывание его с дискеты;
- блокирование и разблокирование системы;
- смена пароля пользователя.

Идентификация и аутентификация пользователя при входе в систему предназначена для защиты локального компьютера от загрузки ОС Windows незарегистрированным пользователем. Данный механизм предполагает наличие у пользователя его уникального регистрационного имени и пароля. В СЗИ ведется список разрешенных пользователей для входа в систему, который может быть изменен только администратором безопасности. Идентификация и аутентификация осуществляются на последнем этапе загрузки операционной системы. Поэтому невозможно загрузить ОС, не пройдя процедуры идентификации и аутентификации. Исключением является загрузка ОС в режиме «Защищенный режим», вход в котором доступен только администратору безопасности.

Для идентификации и аутентификации пользователя при его входе в систему реализованы следующие способы парольной защиты:

- вход в систему по паролю, вводимому пользователем с клавиатуры;
- вход в систему по ключевой дискете с паролем (пароль в зашифрованном виде предварительно записывается администратором безопасности на дискету, с которой он вводится в систему пользователем);
- вход в систему по электронному идентификатору;
- вход в систему с применением цифровых сертификатов пользователей, выработанных, в том числе с использованием российских криптографических алгоритмов (ГОСТ).

При входе в систему пользователь имеет возможность выбрать мандат входа, но не больше максимального, назначенного администратором безопасности.

Дополнительно в СЗИ предусмотрены ограничения на минимальную и максимальную длину пароля, а также на время доступа пользователя в систему.

При успешном доступе пользователя в систему его идентификационное имя фиксируется в БД настроек СЗИ, считывается модулем диспетчера доступа и используется для контроля всех последующих действий.

Сопоставление пользователя с электронным идентификатором, запись пароля на парольную дискету, возможность смены пароля пользователя, а также возможность блокирования системы осуществляется после входа пользователя в систему путем нажатия сочетания клавиш < Ctrl > + < Alt > + < Del > для вызова соответствующего меню.

Разблокирование системы происходит таким же образом, как и вход в нее.

Сетевой вход или запуск процесса от имени другого пользователя возможен только по паролю, вводимому пользователем с клавиатуры.

3.2. Дискреционный механизм контроля доступа к ресурсам

Субъектами доступа в СЗИ являются поименованные пользователи и процессы. Объектами доступа выступают следующие ресурсы:

- объекты файловой системы (логические диски, каталоги и файлы);
- порты (COM, LPT, USB) и подключаемые к ним устройства;
- процессы (файлы, запускаемые на исполнение).

Дискреционный механизм контроля доступа к ресурсам включает:

- механизм контроля доступа к объектам файловой системы;
- механизм разграничения прав доступа к портам;
- механизм разграничения прав доступа на запуск процессов.

СЗИ предоставляет право изменять правила разграничения доступа только администратору безопасности после его авторизации. При этом, администратор может изменять как списки пользователей и контролируемых объектов защиты, так и права доступа пользователей к этим объектам.

3.2.1. Механизм контроля доступа к объектам файловой системы

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

- только чтение,
- только запись,
- полный доступ.

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

При запрете файла на чтение его нельзя переименовать/переместить, запустить (если это исполняемый файл), но можно записать в него и удалить файл. При запрете каталога на чтение нельзя будет прочитать его содержимое (файлы и подкаталоги), при этом все его содержимое также имеет запрет по чтению.

При запрете файла на запись чтение его будет доступно, 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 прав доступа пользователя к объектам файловой структуры с учетом настроек СЗИ по доступу пользователя к каталогам и файлам, а так же процессов к ресурсам приводится в дискреционном механизме доступа.

3.2.2. Механизм разграничения прав доступа к портам

Разграничение прав доступа к портам (COM, LPT, USB) производится только для субъектов и подразумевает разрешение или запрет использования порта. Настройки данного механизма вступают в силу только после смены сеанса пользователя. Запрет/разрешение доступа к USB-портам производится для всех пользователей персонального компьютера одновременно.

3.2.3. Механизм разграничения прав доступа на запуск процессов

Механизм позволяет накладывать ограничения на запуск определенных процессов разным пользователям. Под запуском процесса понимается попытка открытия исполняемого файла потенциального процесса на исполнение. Возможны два варианта функционирования механизма:

- стандартный режим запуска всех процессов, кроме запрещенных;
- режим замкнутой программной среды.

При стандартном режиме (режиме по умолчанию) доступ на запуск процессов выполняется с учетом списка запрещенных процессов.

При режиме замкнутой программной среды создается список разрешенных к запуску процессов (программ) и разрешается запуск процессов только из данного списка. В состав списка разрешенных процессов помимо прикладных программ пользователя включаются необходимые системные процессы, без запуска которых ОС Windows и приложения не смогут функционировать.

3.2.4 Дискреционная модель разграничения прав доступа пользователя к объектам файловой системы ПК

В таблице 1 представлена дискреционная модель прав доступа пользователя к объектам файловой системы ПК.

Таблица 1 – Дискреционная модель прав доступа к объектам файловой системы

Действующие права доступа пользователя	**Настройки СЗИ по доступу пользователя к ресурсам файловой системы**				**Дополнительные механизмы разграничения доступа процессов к ресурсам**
	Каталоги		**Файлы**		
	Запрет		**Запрет**		
	Чтение	**Запись**	**Чтение**	**Запись**	
Разрешения для каталогов					Нет запретов на доступ процессов к каталогу и нет запрета на запуск процессов из каталога
Полный доступ	-	-	-	-	
Исполнение файла из каталога	-	X	-	X	
Чтение каталогов и подкаталогов (без записи)	-	+	-	X	
Создание/удаление/ изменение каталогов и подкаталогов	-	-	X	X	
Разрешения для файлов					Нет запретов на доступ процессов к файлу и нет запрета на запуск

Действующие права доступа пользователя		Настройки СЗИ по доступу пользователя к ресурсам файловой системы				Дополнительные механизмы разграничения доступа процессов к ресурсам
		Каталоги		Файлы		
		Запрет		Запрет		
		Чтение	Запись	Чтение	Запись	
Полный доступ к файлу в каталоге		-	-	-	-	процесса из файла
Исполнение файла из каталога		-	X	-	X	
Чтение содержимого файла в каталоге (без записи):	1)	-	+	-	X	
	2)	-	-	-	+	
Создание/удаление файлов в каталоге и запись данных в файл	1)	-	-	-	-	(Примечание – при запрете на чтение запись возможна при использовании приложений, поддерживающих такую функцию)
	2)	-	-	+	-	
Запрещения для каталогов						
Запрет полного доступа:	1)	+	+	X	X	
	2)	X	X	X	X	Есть запрет на доступ процессов к каталогу
Запрет исполнения файла из каталога:	1)	+	X	X	X	
	2)	-	X	+	X	
	3)	X	X	X	X	Есть запрет на запуск процессов из каталога
Запрет чтения содержимого каталогов, подкаталогов и файлов		+	X	X	X	
Запрет создания/удаления/изменения каталогов и подкаталогов:	1)	+	X	X	X	
	2)	-	+	X	X	
Запрещения для файлов						
Запрет полного доступа:	1)	+	X	X	X	
	2)	-	X	+	X	
	3)	-	-	-	-	Есть запрет на доступ процессов к файлу
Запрет исполнения файла из каталога:	1)	+	X	X	X	
	2)	-	X	+	X	
	3)	-	-	-	-	Есть запрет на запуск данного файла как процесса
Запрет чтения и копирования	1)	+	X	X	X	

Действующие права доступа пользователя		Настройки СЗИ по доступу пользователя к ресурсам файловой системы				Дополнительные механизмы разграничения доступа процессов к ресурсам
		Каталоги		Файлы		
		Запрет		Запрет		
		Чтение	Запись	Чтение	Запись	
содержимого файлов в каталоге:	2)	-	X	+	X	
Запрет создания/удаления файлов в каталоге и записи данных в файл:	1)	+	X	X	X	
	2)	-	+	X	X	
	3)	-	-	-	+	
	4)	-	-	-	-	Есть запрет на доступ соответствующего процесса к файлу

Примечание:

1) Обозначение: «-» - отсутствие запрета, «+» - наличие запрета, «X» - любое значение.
2) Запрещения для каталогов автоматически распространяются на вложенные объекты.
3) Дискреционная модель разграничения доступа действует равно как на пользовательские файлы, так и на файлы операционной системы.
4) 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.
5) 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.
6) 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».
7) При установке дополнительных разграничений доступа для процессов отдельно от разграничений доступа для пользователя запреты для процессов перекрывают разрешения для пользователей.
8) При установке дополнительных разграничений доступа для процессов вместе с правами пользователя запреты для пользователя перекрывают разрешения для процессов и наоборот.
9) Доступ к каталогу, содержащему файлы СЗИ «Блокхост-сеть 2.0», запрещен для всех пользователей.
10) Для противостояния потенциальным уязвимостям среды функционирования СЗИ «Блокхост-сеть 2.0» (ОС Windows) администратор безопасности 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 2.0» (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. Мандатный механизм контроля доступа к ресурсам

Мандатный механизм контроля доступа обеспечивает разграничение доступа субъектов (пользователей, процессов) к объектам (дискам, папкам, файлам) с помощью классификационных меток (комбинации иерархических и неиерархических категорий), определяющих уровень допуска субъекта и уровень конфиденциальности объекта.

Классификационные метки (иерархическая категория) присваиваются субъектам/объектам из диапазона чисел 1-255 и соответствуют их месту (уровню) иерархии в пределах неиерархической 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. Назначать мандатные метки можно логическим дискам, каталогам и файлам. Назначение мандатной метки каталогу означает, что все содержимое этого каталога, а также содержимое вложенных папок будет иметь указанную мандатную метку. Это справедливо только в случае, если вложенным объектам дополнительно не назначена мандатная метка.

Общие правила разграничения доступа мандатного механизма СЗИ «Блокхост-сеть 2.0» состоят в следующем:

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

Для выполнения операции записи пользователю, имеющему большее значение иерархической мандатной метки, необходимо выполнить вход в систему с тем значением, которое соответствует значению ресурса, открываемого на запись.

Если пользователь вошел в систему со значением иерархической мандатной метки, меньше значения иерархической мандатной метки папки, запись в папку он осуществить не сможет.

Администратор безопасности при настройке мандатного механизма контроля доступа выполняет следующие действия:

- задает значения классификационных меток (иерархических и неиерархических категорий);
- в соответствии с политикой безопасности назначает каждому пользователю максимальный уровень допуска (комбинацию иерархических и неиерархических категорий);

- определяет защищаемые ресурсы и присваивает им уровень конфиденциальности (комбинацию иерархических и неиерархических категорий).

Реализация мандатного механизма предусматривает разграничение прав ввода-вывода на отчуждаемые физические носители (ОФН) так же, как и на обычные жесткие диски или другие объекты, имеющие свой уровень конфиденциальности. В качестве ОФН используются гибкие диски, флэш-диски и т.п. Ввод-вывод на отчуждаемые физические носители доступен для данного субъекта только в том случае, если уровень конфиденциальности ОФН не выше уровня конфиденциальности субъекта. Скопировать документ с отчуждаемого носителя разрешается только в папку с уровнем равным уровню конфиденциальности устройства.

Для работы сетевого мандатного режима требуется подключение к серверу СЗИ.

Мандат пользователя рабочей станции, с которым он входит на удаленную машину, равен мандату интерактивно вошедшего пользователя.

3.4. 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 8/8.1 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);
8) печать на принтерах общего доступа возможна только при включении режима маркировки документов.

3.5. Механизм гарантированного удаления

Механизм гарантированного удаления реализован в модуле диспетчера доступа. В случае если производится попытка удаления файла, поставленного на контроль по данному механизму, диспетчер доступа запрещает удаление стандартным способом. В область внешней памяти, где находились файлы, поставленные на контроль механизма гарантированного удаления, осуществляется трехкратная запись информации по специальному алгоритму, исключающему считывание остаточной информации на диске после удаления.

3.6. Механизм очистки памяти

Механизм очистки памяти осуществляет очистку (обнуление) освобождаемых СЗИ «Блокхост-сеть 2.0» областей оперативной памяти ЭВМ и удаляемых данных на локальных дисках. Очистка осуществляется записью нулей в освобождаемую область памяти.

3.7. Механизм контроля целостности и гарантированного восстановления

Механизм контроля целостности выполняет проверку целостности контролируемых файлов по алгоритму CRC-32 и при обнаружении ошибки обеспечивает их восстановление.

Проверка целостности выполняется периодически.

Этот же механизм используется для контроля целостности и надежного восстановления свойств СЗИ после сбоев и отказов оборудования. При обнаружении ошибки выполняется восстановление контролируемых объектов из резервных копий, хранящихся в БД, после перезагрузки системы.

3.8. Механизм контроля целостности реестра

Механизм контроля целостности реестра выполняет проверку целостности разделов (ветвей), параметров (ключей) и значений параметров реестра ОС Windows путём их сравнения с эталоном и при обнаружении ошибки информирует об этом пользователя.

Проверка целостности выполняется по следующим типам событий:

- переименование/удаление контролируемого раздела;
- добавление подраздела в контролируемый раздел;
- удаление существующего подраздела из контролируемого раздела;
- изменение названия подраздела в контролируемом разделе;
- добавление нового параметра в контролируемый раздел;
- изменение названия параметра в контролируемом разделе;
- удаление параметра в контролируемом разделе;
- изменение значения параметра в контролируемом разделе.

Модуль контроля целостности реестра позволяет осуществлять восстановление поврежденного или несанкционированно измененного раздела/параметра/значения параметра реестра.

Модуль контроля целостности реестра позволяет включать/выключать автозапуск системных служб и драйверов рабочих станций через соответствующие ключи реестра, а также – редактировать список автозагрузки рабочей станции через соответствующие ключи реестра.

Модуль контроля целостности реестра осуществляет контроль целостности собственных программных компонентов по алгоритму CRC-32 и при обнаружении изменений в файле происходит предупреждение о нарушении целостности. Запуск измененных файлов невозможен. Этот механизм используется для контроля программного модуля после сбоев и отказов оборудования.

Модуль контроля целостности реестра реализован в виде отдельного программного приложения.

3.9. Механизм регистрации событий и аудита

Механизм регистрации событий выполняет прием сообщений аудита от модуля диспетчера доступа, модуля аутентификации, модуля контроля целостности и гарантированного восстановления, модуля контроля печати. Журналы формируются из сообщений, поступающих при обращении к защищаемым ресурсам, а также при срабатывании всех механизмов защиты, встроенных в операционную систему. Сообщения журнала аудита 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.

Информация о событиях, входящих в определенный администратором перечень, анализируется и отправляется сетевому монитору безопасности на сервер безопасности.

3.10. Механизм персонального экрана

Персональный экран реализует защиту ПК, подключенного к ЛВС, от НСД к его ресурсам из внешних источников, разграничение доступа пользователя ПК к ресурсам сети, а также – фильтрацию сетевого трафика. Реализованы следующие функциональные возможности фильтрации пакетов:

- фильтрация на сетевом уровне на основе сетевых адресов отправителя и получателя;
- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов.

Для пользователя создается один или несколько профилей персонального экрана, в котором выбирается тип политики: запретительная или разрешительная.

Для профиля пользователя задаются общие настройки, не зависящие от типа выбранной политики (фильтрация протоколов ICMP и IGMP, фильтрация по типам ICMP запросов, регистрация типов ICMP пакетов) и настройки политик. Политика разграничения доступа состоит из набора правил фильтрации.

Правила фильтрации используют IP-адрес и порт узла отправителя, IP-адрес и порт узла получателя, признаки активности используемого правила и регистрации в журнале аудита. При этом IP-адреса и порты узлов могут задаваться перечислением или диапазоном.

Также реализована возможность фильтрации по сетевым интерфейсам локальной машины, флагам TCP протокола и времени жизни пакета (TTL).

ПЭ стартует при загрузке ОС. Модуль загружается после драйвера NDIS, но до регистрации сетевых протоколов. Проверка старта ПЭ может быть выполнена с помощью модуля GIS.Client.FirewallIcon.exe, отображающего нотификатор в панели инструментов Windows или вручную с помощью команды sc query DrvFltIP. При входе пользователя в систему драйверу ПЭ от модуля идентификации и аутентификации приходит конфигурация настроек, согласно которой выполняется дальнейшая фильтрация сетевого трафика. Драйвер ПЭ на этапе инициализации регистрируется, как драйвер-фильтр интерфейса NDIS 6, настраиваются функции обратного вызова, которые гарантируют присоединение фильтра к любому существующему или вновь появляющемуся в системе сетевому адаптеру. В дальнейшем для каждого такого адаптера фильтром обрабатывается любая сетевая активность указанного устройства.

Регистрация траффика выполняется согласно опциям «Общих настроек» профиля ПЭ, а так же опции «Аудит» для каждого отдельно взятого правила. Аудит трафика может выполняться, как посредством записи соответствующих событий в системный журнал с помощью службы диспетчера аудита (LogDispatcher.exe), так и отправкой на Syslog-сервер.

Контроль целостности программной и информационной части персонального экрана выполняется модулем контроля целостности (IntegrityChecker.exe), а так же с помощью ЭЦП. Каждый драйвер ПЭ подписан доверенным сертификатом компании ООО «Газинформсервис», который включен в список доверенных распространителей системного ПО компании Verisign и Microsoft. Корректность проверки ЭЦП гарантирует целостность программной и информационной части ПЭ. Проверка ЭЦП осуществляется автоматически средствами ОС при запуске драйвера. Драйвер, подпись которого не была проверена или целостность исполняемого образа которого была нарушена, не будет загружен ОС. Резервная копия исполняемого образа создается в Backup при установке СЗИ «Блокхост-сеть 2.0». Процедура восстановления после сбоев и отказов оборудования, обеспечивающая восстановление свойств ПЭ гарантируется спецификацией интерфейса NDIS 6 и является архитектурной особенностью. При нарушении целостности драйвера персонального экрана администратор безопасности может восстановить его следующим образом:

- заново установить драйвер персонального экрана из папки `C:\BlockHost\Backup\BlockHost\bppfw`. Для этого необходимо сделать следующее:
  1) выбрать пункт ***Панель управления →Центр управления сетями и общим доступом*** и нажать на ссылку ***Подключение по локальной сети***;
  2) в появившемся окне **«Состояние-Подключение по локальной сети»** нажать кнопку ***Свойства***:

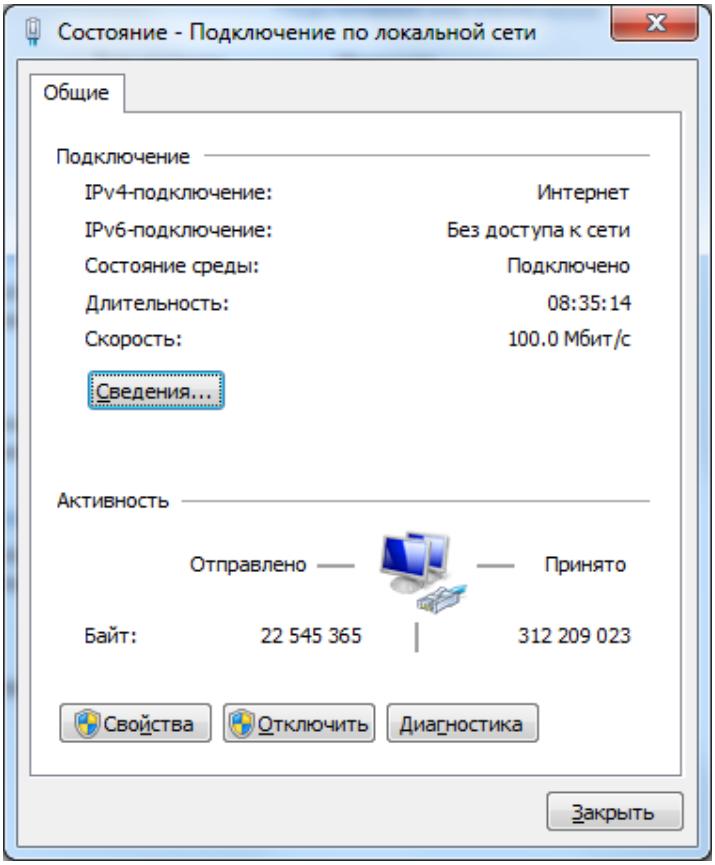


Рисунок 2. Окно «Состояние-Подключение по локальной сети»

3)в появившемся окне выбрать компонет ***Клиент для сетей Microsoft*** и нажать кнопку ***Установить*** (рис. 3);

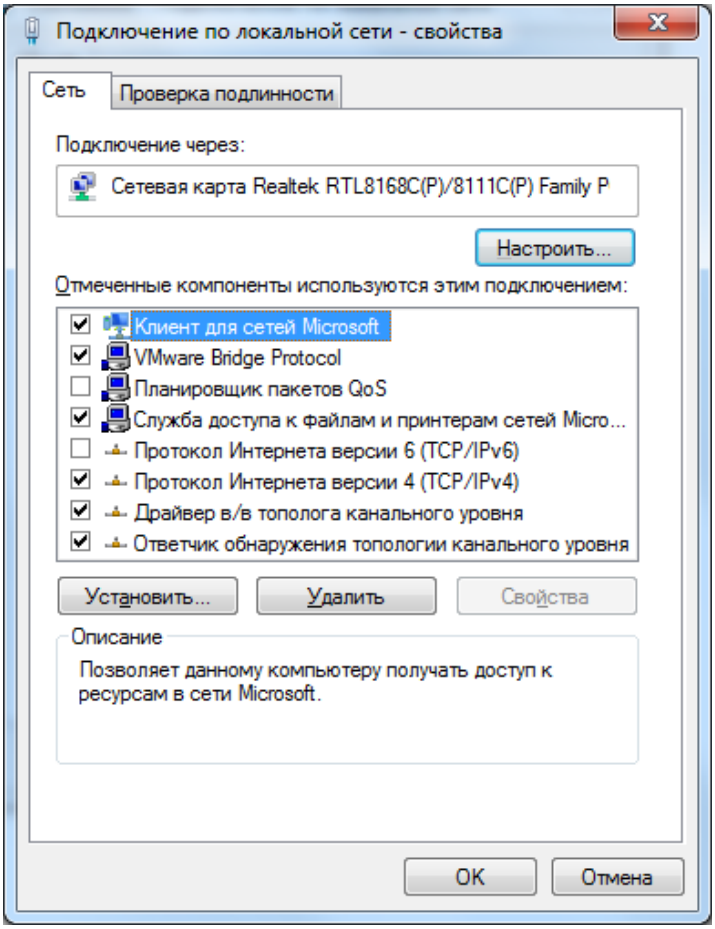


Рисунок 3. Выбор пункта «Установить»

4)выбрать сетевой компонент ***Служба*** и нажать ***Добавить***:

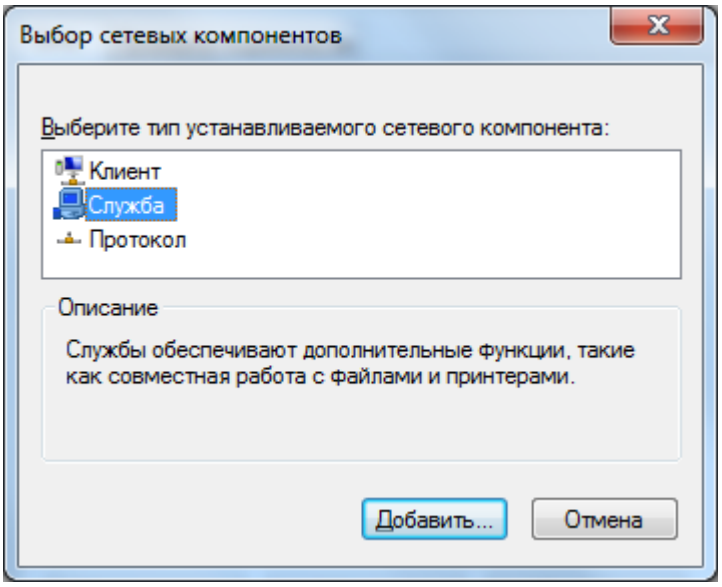


Рисунок 4. Выбор компонента «Служба»

5)в окне выбора сетевой службы нажать ***Установить с диска*** (рис. 5);

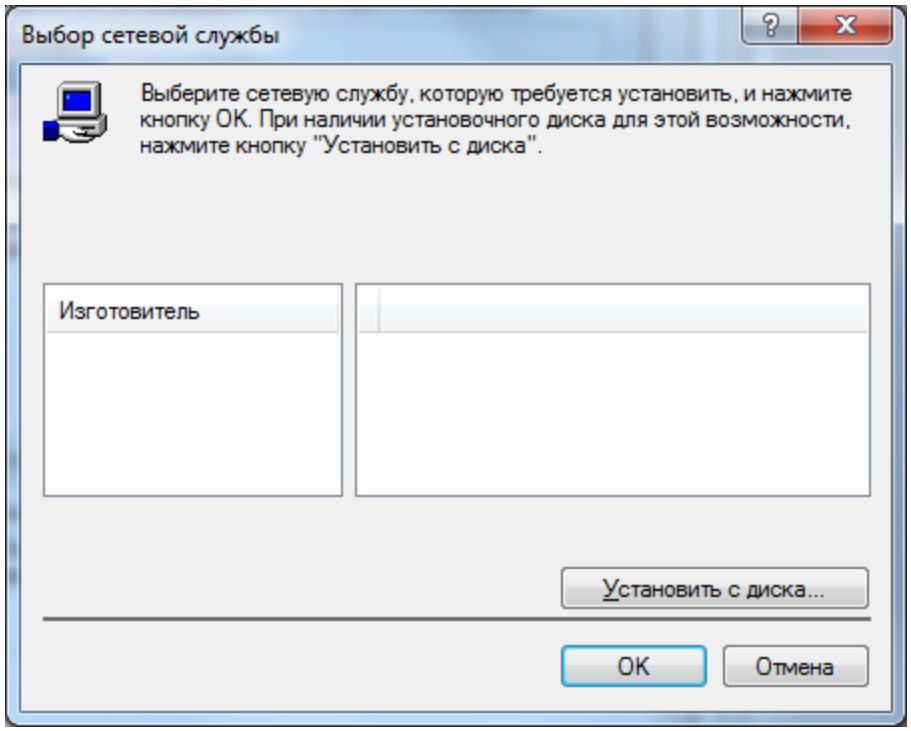


Рисунок 5. Установка драйвера

6)в появившемся окне **«Установка с диска»** нажать кнопку ***Обзор*** и в окне **«Поиск файла»** выбрать в папке `C:\BlockHost\Backup\BlockHost\bppfw` файл `DrvFltIP.inf`. Нажать кнопку ***OK***.

3.11. Механизм управления идентификаторами

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

3.12. 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 и запрещенных для запуска;
- формирование списка файлов, целостность которых требуется контролировать;
- делегирование прав доступа по администрированию СЗИ пользователям (такие пользователи должны быть включены в группу администраторов текущей рабочей станции);
- формирование списка процессов для контроля печати и настройка колонтитулов для выводимой информации;
- формирование режимов работы и набора правил доступа для персонального экрана.

4. Входные и выходные данные

Входными данными для СЗИ «Блокхост-сеть 2.0» являются:

- база данных настроек системы защиты;
- база данных настроек операционной системы;
- база данных шаблонов настроек системы защиты для пользователей;
- настройки реестра, влияющие на работу системы защиты;
- база данных настроек персонального экрана.

Настройки системы защиты хранятся в локальной базе данных, представленной 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.

Для удобства задания настроек системы защиты для пользователей используются шаблоны настроек, обеспечивающие типовые варианты применения системы защиты. Структура базы данных шаблонов настроек повторяет структуру базы данных настроек системы защиты в части прав доступа пользователей.

Настройки персонального экрана задаются в конфигурационном файле, который содержит следующие данные по каждому пользователю:

- режимы работы (включение при загрузке ОС или по требованию, запретительная или разрешительная политика доступа);
- наборы правил доступа для запретительной и разрешительной политик.

Выходными данными СЗИ «Блокхост-сеть 2.0» 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. На каждый день создается свой файл аудита. Просмотр сообщений аудита и очистка журналов аудита осуществляются администратором безопасности через интерфейс ОС: «Панель управления» → «Администрирование» → «Просмотр событий».

В таблице 2 представлены механизмы защиты и возможные сообщения, относящиеся к защите ресурсов каждым механизмом.

Таблица 2 – Механизмы защиты и возможные сообщения, относящиеся к защите ресурсов каждым механизмом

Механизм	Сообщение
Дискреционный механизм доступа	открытие файла для чтения
	открытие файла для записи
	открытие файла на исполнение
	удаление файла
	чтение директории
	запись в директорию
	обращение к директории

Механизм	Сообщение
	переименование директории
	удаление директории
Мандатный механизм доступа	открытие файла для чтения
	открытие файла для записи
	открытие файла для чтения и записи
	удаление файла
	чтение директории
	запись в директорию
	обращение к директории
	переименование директории
	удаление директории
Контроль запуска процессов	запуск процесса (полный путь к запускаемому процессу)
Очистка памяти	очистка памяти при завершении контролируемого процесса
Гарантированное удаление	гарантированное удаление файла
Вывод документа на печать	вывод конфиденциального документа на печать
Ввод-вывод на отчуждаемый физический носитель (ОФН)	ввод на ОФН
	вывод на ОФН
Аутентификация	аутентификация пользователя в СЗИ
Проверка целостности	проверка целостности контролируемых данных
Изменение настроек	изменение настроек СЗИ
Выключение компьютера	выключение/перезагрузка компьютера

5. Программные модули СЗИ «Блокхост-сеть 2.0»

СЗИ «Блокхост-сеть 2.0» включает следующие программные модули, реализующие механизмы защиты и их взаимодействие в составе программного обеспечения СЗИ (рисунок 6):

- модуль диспетчера доступа и гарантированного удаления;
- модуль интерфейса администратора;
- модуль определения информации о системе;
- модуль получения и установки локальных настроек;
- модуль контроля печати;
- модуль аутентификации;
- модуль контроля целостности и гарантированного восстановления;
- модуль контроля целостности реестра;
- модуль персонального экрана;
- модуль регистрации событий;
- модуль работы с локальной базой данных;
- модуль инсталляции/деинсталляции СЗИ;
- модуль запроса настроек пользователя для сетевых подключений;
- клиент сетевого взаимодействия;
- сервер сетевого взаимодействия;
- модуль монитора сетевого администратора;
- сервер сетевого мандатного режима;
- модуль интерфейса администратора;
- модуль получения информации об удаленной системе;
- серверный модуль получения и установки настроек;
- модуль работы с серверной базой данных.

Входными данными для работы модуля аутентификации являются списки зарегистрированных пользователей и их пароли, хранимые в БД настроек СЗИ, 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 в журнал аудита. При успешном доступе пользователя в систему его идентификационное имя фиксируется в БД настроек СЗИ, считывается модулем диспетчера доступа и используется для контроля всех последующих его действий.

Модуль диспетчера 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 настроек СЗИ. Все обращения к защищаемым ресурсам контролируются и фиксируются в БД журналов аудита модулем регистрации событий.

Модуль контроля целостности и гарантированного восстановления и модуль регистрации событий являются сервисами (службами) Windows, 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.

Модуль персонального экрана стартует при загрузке ОС. Модуль загружается после драйвера NDIS, но до регистрации сетевых протоколов. При входе пользователя в систему драйверу ПЭ от модуля идентификации и аутентификации приходит конфигурация настроек, согласно которой выполняется дальнейшая фильтрация сетевого трафика. Драйвер ПЭ на этапе инициализации регистрируется, как драйвер-фильтр интерфейса NDIS 6, настраиваются функции обратного вызова, которые гарантируют присоединение фильтра к

любому существующему или вновь появляющемуся в системе сетевому адаптеру. В дальнейшем для каждого такого адаптера фильтром обрабатывается любая сетевая активность указанного устройства.

С помощью модуля интерфейса администратора (локального и серверного) производится настройка параметров системы защиты и сохранение их в БД настроек. Для того чтобы новые параметры вступили в силу, необходимо сменить сеанс пользователя. Действия по изменению настроек фиксируются в журналах аудита.

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

Модуль получения информации об удаленной системе перенаправляет запросы о доступных ресурсах локальной машины модулю определения информации о системе данной локальной станции. Так же он обрабатывает информацию о подключении и отключении клиентских станций, информируя об этом модуль интерфейса администратора для разрешения или блокирования возможности их администрирования.

Модуль запроса настроек пользователя для сетевых подключений обрабатывает запросы модуля диспетчера 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.

Модуль получения и установки настроек (локальный и серверный) является диспетчером, которому направляются запросы на получение рабочих параметров при загрузке системы, входе нового пользователя или перезапуске модулей.

Модуль работы с базой данных (локальный и серверный) обрабатывает запросы на получение и сохранение настроек, кодирование и раскодирование файла конфигурации с параметрами работы системы и разграничениями для пользователей.

В модуле регистрации событий собираются все события аудита от модулей СЗИ, которые сохраняются в базе данных журналов аудита. Кроме того, производится фильтрация записей аудита для выявления событий из определенного перечня, которые отправляются модулю монитора 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 переправляется 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 локальной станции и сервера удаленного управления СЗИ, осуществляют обмен конфиденциальными данными по защищенному каналу, управляют потоками данных для различных модулей СЗИ.

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

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

Модуль контроля целостности реестра реализован в виде отдельного программного приложения. Описание модуля контроля целостности реестра приведено в документах «СЗИ «Блокхост-сеть 2.0». Контроль целостности реестра. Руководство администратора безопасности» и «СЗИ «Блокхост-сеть 2.0». Контроль целостности реестра. Описание программы».

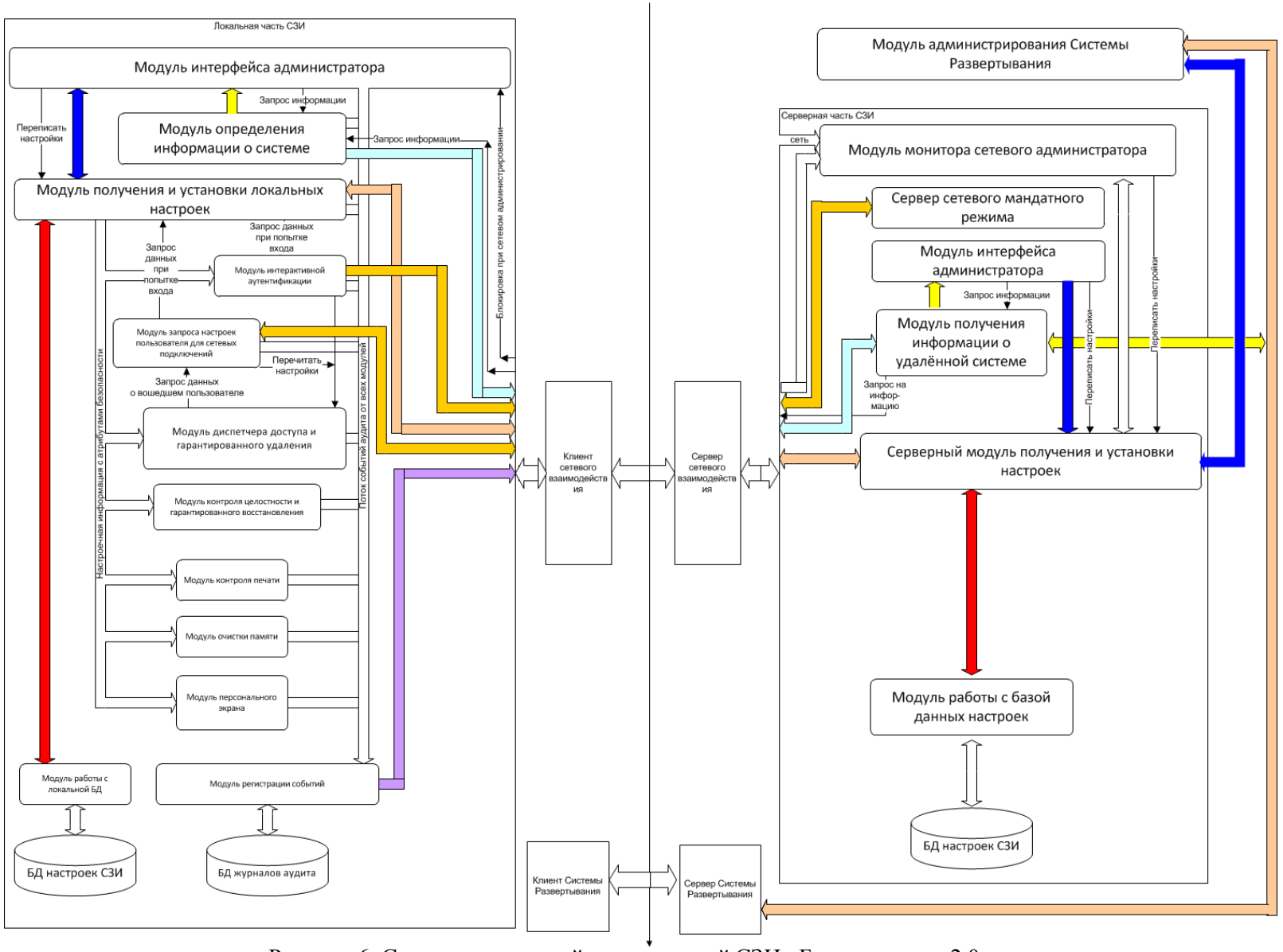


Рисунок 6. Состав и взаимодействие модулей СЗИ «Блокхост-сеть 2.0»