**Муниципальное образование городской округ – город Югорск**

**Администрация города Югорска**

**ПРОТОКОЛ**

**рассмотрения заявок на участие в аукционе в электронной форме**

«04» декабря 2014 г. № 0187300005814000697-1

ПРИСУТСТВОВАЛИ:

Заместитель председателя Единой комиссии по осуществлению закупок для обеспечения муниципальных нужд города Югорска (далее - комиссия):

1. Бандурин В.К. – заместитель председателя комиссии, директор департамента жилищно - коммунального и строительного комплекса;

Члены комиссии:

2. Климин В.А. – заместитель председателя Думы города;

3. Морозова Н.А. - советник главы города;

4. Долгодворова Т.И. – заместитель главы администрации города Югорска;

5. Резинкина Ж.В. – заместитель начальника управления экономической политики;

6. Абдуллаев А.Т. - начальник отдела по управлению муниципальным имуществом департамента муниципальной собственности и градостроительства;

7. Захарова Н.Б. - начальник отдела муниципальных закупок управления экономической политики.

Всего присутствовали 7 членов комиссии из 9.

Представитель заказчика: Виктор Юрьевич Овечкин, юрисконсульт муниципального казенного учреждения «Служба обеспечения органов местного самоуправления».

1. Наименование аукциона: аукцион в электронной форме № 0187300005814000697 на право заключения муниципального контракта на выполнение работ по проектированию, первичному оснащению и организации защищённого взаимодействия существующего сегмента системы видеонаблюдения, в том числе фото-видео фиксации нарушений ПДД ОМВД России по г. Югорску с сегментом интегрированной мультисервисной телекоммуникационной системы МВД России по ХМАО–Югре.

Номер извещения о проведении торгов на официальном сайте – <http://zakupki.gov.ru/>, код аукциона 0187300005814000697, дата публикации 24.11.2014.

2. Заказчик: муниципальное казенное учреждение «Служба обеспечения органов местного самоуправления». Почтовый адрес: 628260, Ханты - Мансийский автономный округ - Югра, Тюменская обл.,  г. Югорск, ул. 40 лет Победы, 11.

3. Процедура рассмотрения первых частей заявок на участие в аукционе была проведена комиссией в 10.00 часов 4 декабря 2014 года, по адресу: ул. 40 лет Победы, 11, г. Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область.

4. Количество поступивших заявок на участие в аукционе – 2.

5. Комиссия рассмотрела первые части заявок и приняла следующее решение:

|  |  |  |
| --- | --- | --- |
| Порядковый номер заявки | Решение о допуске или об отказе в допуске | Причина отказа в допуске |
| 2104784 | допустить к участию в аукционе и признать участником аукциона |  |
| 4388903 | допустить к участию в аукционе и признать участником аукциона |  |

6.Настоящий протокол подлежит размещению на сайте оператора электронной площадки [http://www.sberbank-ast.ru](http://www.sberbank-ast.ru/).

Сведения о решении

членов комиссии о допуске участника закупки к участию в аукционе

или об отказе их в допуске к участию в аукционе

|  |  |  |
| --- | --- | --- |
| Решение члена комиссии | Подпись члена комиссии | Состав комиссии |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | В.К. Бандурин |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | В.А. Климин |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | Н.А. Морозова |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | Т.И. Долгодворова |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | Ж.В. Резинкина |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | А.Т. Абдуллаев |
| Мое решение о допуске участника закупки к участию в аукционе или об отказе в допуске к участию в аукционе совпадает с решением, указанным в пункте 5 настоящего протокола |  | Н.Б. Захарова |

**Заместитель председателя комиссии: В.К. Бандурин**

Члены комиссии

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А. Климин

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.А. Морозова

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.И. Долгодворова

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ж.В. Резинкина

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Т. Абдуллаев

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.Б. Захарова

Представитель заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Ю. Овечкин

Приложение

к протоколу рассмотрения заявок

на участие в аукционе в электронной форме

от 04 декабря 2014 г. № 0187300005814000697-1

**Таблица рассмотрения заявок**

**на участие в аукционе в электронной форме на право заключения муниципального контракта на выполнение работ по проектированию, первичному оснащению и организации защищённого взаимодействия существующего сегмента системы видеонаблюдения, в том числе фото-видео фиксации нарушений ПДД ОМВД России**

**по г. Югорску с сегментом интегрированной мультисервисной телекоммуникационной системы МВД России по ХМАО–Югре**

Заказчик: Муниципальное казенное учреждение «Служба обеспечения органов местного самоуправления»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Обязательные требования | Наименование товара | Характеристика | Номер заявки | |
| 2104784 | 4388903 |
| Первая часть заявки на участие в электронном аукционе должна содержать следующие сведения:  конкретные показатели, соответствующие значениям, установленным в части II «ТЕХНИЧЕСКОЕ ЗАДАНИЕ» документации об аукционе, и товарный знак (его словесное обозначение) (при наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), наименование места происхождения товара или наименование производителя товара предлагаемого для поставки товара.  Первая часть заявки на участие в электронном аукционе может содержать эскиз, рисунок, чертеж, фотографию, иное изображение товара, на поставку которого заключается контракт | Программно-аппаратный комплекс ViPNet Coordinator HW1000 сети VipNet № 2957 (Использование эквивалента не допустимо во избежание несовместимости с программно-аппаратными комплексами, установленными для защиты каналов связи системы ведомственного электронного взаимодействия с УМВД России по Ханты-Мансийскому автономному округу – Югре) | Программно-аппаратный комплекс ViPNet Coordinator HW1000, должен отвечать следующим требованиям:   1. должен быть совместим (по ключевой системе и средствам управления сети) с программным обеспечением, реализующим функции управления защищённой сетью ViPNet N 2957 «УГИБДД ХМАО», действующей в УМВД России по Ханты-Мансийскому автономному округу – Югре:   - обновление программного обеспечения,  - обновление справочно-ключевой информацией,  - управлением политиками безопасности;   1. встроенная операционная система GNU/Linux; 2. встроенный жёсткий диск; 3. должен иметь не менее 4 сетевых интерфейсов 10/100/1000 Mbit/sec RJ45; 4. должен обеспечивать отказоустойчивость путём организации кластера на безе 2-х одинаковых ПАК в конфигурации «активный – пассивный»; 5. должно обеспечиваться предоставление функции туннелирующего сервера без ограничений на число лицензий для туннелируемых IP-адресов; 6. должно обеспечиваться предоставление функции сервера IP-адресов; 7. программное обеспечение, реализующее функции криптографического шлюза, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; 8. должен обеспечивать подключение VPN-клиентов, присутствующих в сети, без ограничений по числу лицензий для одного ПАК; 9. в состав и стоимость комплекса должна входить программа для удаленного управления и мониторинга настройками криптошлюза и встроенного межсетевого экрана; 10. должно обеспечиваться автоматическое дистанционное распределение симметричной ключевой информации при появлении в сети новых пользователей, добавлении новых связей или удалении существующих связей, компрометации ключей других комплексов или в ходе выполнения штатных процедур смены ключевой информации на ПАК; 11. возможность монтажа в стандартную 19-ти дюймовую монтажную стойку от 480 мм и более; 12. должен иметь действующий сертификат ФСБ России по требованиям к средствам криптографической защиты информации по классу не ниже КС3 для шифрования ip-трафика; 13. действующий сертификат ФСТЭК России, удостоверяющий соответствие требованиям руководящих документов к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню контроля, и возможностью использования в АС до класса 1В включительно; 14. действующий сертификат на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации; 15. гарантия производителя не менее 1 (одного) года. | соответствует | соответствует |
| Передача права на использование ПО ViPNet Client 3.х (КС2) сети VipNet № 2957 (Использование эквивалента не допустимо во избежание несовместимости с программно-аппаратными комплексами, установленными для защиты каналов связи системы ведомственного электронного взаимодействия с УМВД по ХМАО-Югре) | Программное обеспечение ViPNet Client 3.х (КС2) должно отвечать следующим требованиям:   * совместимо (полностью) с ПАК ViPNet Coordinator HW1000 реализующим функции криптографического шлюза, представленным в настоящем ТЗ; * поддержка операционных систем: * Microsoft Windows XP Professional; * Microsoft Windows Vista (вся линейка); * Microsoft Windows 7 (вся линейка); * предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами; * предоставлять функции контроля запускаемых в операционной системе приложений; * предоставлять функции контентной фильтрации прикладных протоколов http, ftp; * программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; * взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза); * наличие сертификата ФСТЭК России на соответствие требованиям к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно;   наличие сертификата ФСБ России на соответствие требованиям к СКЗИ по классу КС2 и на соответствие требованиям к МЭ по 4-ому классу защищенности | соответствует | соответствует |
| Аппаратный модуль доверенной загрузки | Требования к аппаратному модулю доверенной загрузки:  – должен обеспечивать защиту от НСД к компьютеру;  – должен начинать работу до загрузки операционной системы;  – должен выполнять следующие основные функции:  • идентификация и аутентификация пользователей при их входе в систему с помощью персональных идентификаторов iButton, eToken PRO (Java), eToken PRO, iKey 2032, Rutoken, Rutoken RF  • защита от несанкционированной загрузки операционной системы со съемных носителей информации: дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.;  • контроль целостности программного и аппаратного обеспечения защищаемого компьютера до загрузки операционной системы:  • файлов и физических секторов жесткого диска;  • элементов системного реестра компьютера;  • журнала транзакций;  • PCI-устройств;  • структур SMBIOS;  • таблиц ACPI;  • конфигурации оперативной памяти;  • функционирование механизма сторожевого таймера;  • регистрация событий, связанных с безопасностью системы;  • поддержка следующих файловых систем для контроля целостности файлов: NTFS, FAT32  В качестве персональных идентификаторов должна быть реализована возможность использования идентификаторов следующих типов: DS1992; DS1993; DS1994; DS1995; DS1996; eToken PRO; eToken PRO (Java); Ru-token; Rutoken RF; iKey 2032; eToken PRO или эквивалентов.  В комплекте должны быть считыватель и не менее 2 идентификаторов любых из указанных типов.  Должна быть предоставлена возможность работы на нескольких компьютерах при предъявлении одного и того же персонального идентификатора.  Требования к реализации функции защиты от несанкционированной загрузки операционной системы со съемных носителей информации:  модуль доверенной загрузки должен обеспечивать невозможность загрузки пользователем нештатной копии ОС со съемных носителей информации (дискеты, оптические диски, магнитооптические диски, ZIP-устройства, USB-диски и др.);  администратору модуля доверенной загрузки должна быть предоставлена возможность выполнения загрузки ОС со съемных носителей информации;  для пользователя должен быть обеспечен доступ к информации на съемных носителях после загрузки ОС.  Контроль целостности программного и аппаратного обеспечения защищаемого компьютера должен базироваться на расчете текущих значений контрольных сумм объектов контроля и сравнении полученных значений с эталонными, вычисленными при установке или последующем администрировании модуля доверенной загрузки.  Должна быть обеспечена возможность анализа журнала транзакций файловых систем NTFS.  Блокировка доступа к компьютеру должна осуществляется двумя способами:  • путем принудительной автоматической перезагрузки компьютера с помощью стандартной процедуры Reset.  • принудительным автоматическим выключением питания (в случае отсутствия в защищаемом компьютере разъема Reset).  В модуле доверенной должен функционировать журнал регистрации событий, связанных с безопасностью системы.  Требования к сертификации:  Наличие действующего сертификата ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ класса 1Б. | соответствует | соответствует |
| Право на использование СЗИ от НСД | 1. СЗИ от НСД должна представлять собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.  2. СЗИ от НСД должна быть предназначена для ПЭВМ типа IBM PC, под управлением операционных систем Windows XP, Windows Server 2003, Windows Server 2003 R2, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 (в связи с их эксплуатацией у Заказчика).  3. СЗИ от НСД должна поддерживать 32-х и 64-х битные версии операционных систем.  4. Система предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.  5. СЗИ от НСД должна быть сертифицирована по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по 5-му классу защиты от НСД для СВТ и 4 уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.  6. Сертификат соответствия должен позволять использовать СЗИ от НСД при создании защищенных автоматизированных систем до класса защищенности 1Г включительно и ИСПДн до уровня 1 включительно.  7. СЗИ от НСД должна обеспечивать:  7.1. Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя.  7.2. Идентификацию и проверку подлинности пользователей при входе в операционную систему, а также аутентификация при входе на ПЭВМ до начала загрузки ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор.  7.3. Реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам.  7.4. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных.  7.5. Для предотвращения утечки информации с использованием сменных накопителей СЗИ от НСД должна позволять разграничивать доступ, как к отдельным типам накопителей, так и к конкретным экземплярам.  7.6. В соответствии с требованиями к СЗИ от НСД должен использоваться дискреционный принцип контроля доступа, который обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).  7.7. Возможность ограничивать средствами СЗИ от НСД, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа).  7.8. Регистрация и учет (аудит) действий пользователей, независимыми от ОС средствами (вход/выход пользователей, доступ к ресурсам, печать документов с возможностью добавления штампов и сохранение теневых копий распечатываемых документов, запуск \остановка процессов, администрирование). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей.  7.9. Возможность организации замкнутой программной среды (ЗПС) и различные способы её организации.  7.10. Возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом, просмотр журналов).  7.11. Возможность контроля целостности программно-аппаратной среды при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений.  7.12. Очистку остаточной информации (освобождаемого дискового пространства, зачистку определённых файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки.  7.13. Возможность самодиагностики основного функционала СЗИ от НСД с формированием отчета.  7.14. Возможность сохранения теневых копий распечатываемых документов.  7.15. Возможность сохранения конфигурации для последующего восстановления СЗИ от НСД.  7.16. Ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию.  7.17. Централизованное управление защищёнными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учётными записями пользователей, политиками, правами пользователей. Также этим модулем должен осуществляться периодический сбор журналов со всех защищённых рабочих станций.  7.18. Блокировка доступа к файлам по расширению.  7.19. Возможность настройки всех параметров СЗИ от НСД из единой консоли администрирования.  7.20. Возможность создания отчета по назначенным правам и формирование паспорта программного обеспечения, установленного на ПЭВМ.  7.21. Преобразование данных в файл-контейнер для хранения их на внешних носителях либо для передачи по различным каналам связи. Возможность использования встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, в том числе сертифицированного.  7.22. Возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованного управления.  7.23. Возможность использования механизма удаленной установки СЗИ от НСД средствами модуля централизованного управления самой СЗИ и средствами групповых политик Active Directory. | соответствует | соответствует |
| Право на средство для контроля (анализа) защищённости информационных систем | Технические характеристики:  Обеспечение загрузки доверенной среды с любого компьютера (по технологии Live- CD/Live-flash) с автоматическим определением сетевого оборудования, подключенного к вычислительной сети;  Поиск остаточной информации на накопителях, подключенных к узлам сети (поддерживаются различные кодировки);  Локальный (на любом ПК) и сетевой аудит парольной защиты;  Инвентаризация (фиксация) ресурсов компьютерной сети (узлов, портов, сервисов);  Выявление (сканирование) уязвимостей сетевых сервисов;  Проверка возможности осуществления атак на отказ в обслуживании и подмены адреса;  Анализ сетевого трафика (в т.ч. в коммутируемых сетях, физически разделенных)  Аудит парольной информации для множества протоколов;  Гарантированная очистка информации на носителях;  Контрольное суммирование файлов, папок, а также посекторное суммирование для машинных носителей информации;  Аудит установленных обновлений ОС Windows;  Анализа защищенности беспроводных (Wi-Fi) сетей.  Требования по сертификации:  Должен быть сертифицирован в системе ФСТЭК России и Министерства обороны Российской Федерации:  1. Сертификат Минобороны России на соответствие:  требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 г. - по второму уровню контроля;  требованиям по соответствию реальных и декларируемых в документации функциональных возможностей.  2. Сертификат соответствия Федеральной службы по техническому и экспортному контролю на соответствие:  требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Классификация по уровню контроля отсутствия недекларированных возможностей» – по четвертому уровню контроля; | соответствует | соответствует |
| Установочный комплект для средства контроля (анализа) защищённости информационных систем | Установочный комплект с документацией (Live-CD). | соответствует | соответствует |
| Сертифицированный дистрибутив антивирусного средства к антивирусному средству п.8 настоящей спецификации | Требования к комплектности:  - CD в конверте с записанными сертифицированными приложениями;  - формуляр;  - заверенная копия сертификата ФСТЭК России, удостоверяющий, что антивирус соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей." (Гостехкомиссия России, 1999) –по 2 уровню контроля. | соответствует | соответствует |
| Средство антивирусной защиты | Средство антивирусной защиты должно удовлетворять следующим требованиям:  - Защита от вредоносных программ.  - Наличие регулярных обновлений баз.  - Наличие системы быстрого обнаружения.  - Анализ каждой запущенной программы на вредоносную активность.  - Откат к состоянию, предшествующему появлению вредоносной активности.  - Наличие механизма нейтрализации вредоносных объектов.  - Наличие системы предотвращения вторжений.  - Наличие сетевого экрана.  - Наличие функции блокирования сетевых атак.  - Поддержка русского языка в меню.  - Создание и применение политик доступа к программам и веб-страницам.  -Защита на основе программных агентов для устройств под управлением мобильных операционных систем.  -Проверка операционной системы и используемых программ на наличие уязвимостей.  - Обнаружение вредоносного программного обеспечения, основанного на использовании сигнатур.  - Защита от угроз, для которых еще не созданы сигнатуры.  - Функция персонального сетевого экрана.  - Контроль программ на основе политик.  - Контроль использования веб-ресурсов.  - Репутационная проверка файлов в режиме реального времени. | соответствует | соответствует |
| Средство защиты данных «Защищенный специальный носитель информации» | специальный носитель (СН) должен обеспечивать:  программное обеспечение (ПО) рабочей станции (РС), должно содержаться на открытом разделе флеш-диска СН:  драйвер USB-устройства для работы в составе операционной системы (ОС);  приложения для управления доступом к данным (СН).  СН должен представлять собой аппаратный модуль, выполненный по технологии флеш-диска с интерфейсом USB, предназначенный для хранения пользовательской информации (включая информацию конфиденциального  характера). Основными элементами данного аппаратного модуля должны являться:  1) микроконтроллер с внутренней памятью, используемой для хранения внутреннего ПО СН и служебной информации;  2) физический датчик случайных чисел (ДСЧ);  3) энергонезависимая флеш-память, используемая для хранения пользовательской информации, а также журнала событий и ПО РС.  ПАК должен иметь возможность использоваться на рабочих станциях типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64).  ПАК должен быть предназначен для защищенного хранения корпоративной или личной информации конфиденциального  характера и обеспечивает контролируемый доступ к защищаемой информации со стороны авторизованного пользователя в соответствии с  политиками доступа, установленными администратором.  ПО РС должно размещается на открытом диске СН и исполняется без установки на жесткий диск РС;  -должна быть предусмотрена возможность задания правил доступа к защищаемой информации посредством настройки политик;  -должен вестись журнал работы СН, содержащийся на закрытом разделе флеш-диска СН. | соответствует | соответствует |