|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Приложение №1**   |  |  | | --- | --- | |  |  |   **Техническое   задание** | | |
| **Наименование товара,**  **наименование услуг** | **Кол-во** | **Требования к оказываемым услугам, характеристики поставляемого товара** |
| Передача права на использование средства криптографической защиты информации ViPNetClient[[1]](#footnote-1)для Windows в сеть 14484 | 1 | **Требование к функциональности средства криптографической защиты информации (далее – СКЗИ):**  Клиентское программное обеспечение должно состоять из следующих модулей:  1) Модуль «Монитор» – отвечает за реализацию функций:   * Фильтрация защищенного и открытого трафиков по ряду параметров; * Реализуется режим «stealth» (режим инициативных соединений), позволяющий сделать невидимым компьютер защищенной сети из открытой сети; * Имеет встроенную систему обнаружения вторжений (IDS); * Обеспечивает мониторинг сетевой активности приложений, позволяющий обнаружить и блокировать несанкционированную активность программ-«троянцев». * Шифратора TCP/IP трафика — обеспечивает защиту (конфиденциальность, подлинность и целостность) любого вида трафика (приложений, систем управления и служебного трафика ОС), передаваемого между любыми объектами защищенной сети. * Чат-клиента – позволяет пользоваться услугами сервиса обмена защищенными сообщениями и организации чат-конференций между объектами защищенной сети, на которых установлено клиентское или серверное ПО для организации защищенной сети. * Клиента службы обмена файлами.   2) Модуль «Контроль приложений» – позволяет контролировать сетевую активность приложений и компонент операционной системы.  3) Почтовый модуль – выполняет функции почтового клиента защищенной почтовой службы, функционирующей в рамках защищенной сети и позволяет:   * Формировать и отсылать письма адресатам защищенной сети через простой графический интерфейс пользователя; * Использовать встроенные механизмы ЭЦП для подписи, в том числе множественной, текста письма и его вложений; * Контролировать все этапы «жизни» письма благодаря встроенному механизму обязательного квитирования писем; * Вести архивы писем; * Просматривать графическое отображение статусов электронных писем; * Имеет встроенную базу данных SQLite.   Клиентское программное обеспечение СКЗИ должно поддерживать ключи электронной подписи, созданные по алгоритму ГОСТ 34.10.2012  **Поддержка операционных систем:**   * Windows 8.1 (32/64-разрядная); * WindowsServer 2012 (64-разрядная); * WindowsServer 2012 R2 (64-разрядная); * Windows 10 (32/64-разрядная) следующих версий и сборок:   + версия 1709, сборка 16299,   + версия 1803, сборка 17134,   + версия 1809, сборка 17763,   + версия 1903, сборка 18362,   + версия 1909, сборка 18363;   + версия 2004, сборка 19041,   + версия 20H2, сборка 19042; * WindowsServer 2016 (64-разрядная), сборка 14393; * WindowsServer 2019 (64-разрядная), сборка 17763.   **Требования к сертификации СКЗИ:**   * Наличие сертификата ФСБ России по требованиям к межсетевым экранам по 4 классу; * Наличие сертификата ФСБ России к средствам криптографической защиты информации по классу не ниже КС2. |
| Установочный комплект средства криптографической защиты информации ViPNetClient для Windows | 1 | ***Установочный комплект СКЗИ должен включать:***   * Компакт-диск с дистрибутивов программного обеспечения и документацией на ПК ЭП в электронном виде * Формуляр на изделие; * Копии сертификатов соответствия по требованиям безопасности. |
| Сертификат активации сервиса прямой технической поддержки ПО ViPNetClientforWindows | 1 | * Приём обращений и консультирование по электронной почте в рабочие дни с 1:00 до 20:00 (по московскому времени); * Приём обращений и консультирование по телефону горячей линии в рабочие дни с 1:00 до 20:00 (по московскому времени); * Рекомендации по процессу установки продукта в объеме эксплуатационной документации; * Рекомендации по настройке продукта в объеме эксплуатационной документации; * Диагностику с целью установления факта ошибки в работе программного продукта. Выявленная ошибка, в зависимости от сложности, устраняется в процессе диагностики или в последующих обновлениях ПО; * Рекомендации по «тонкой» настройке продукта после знакомства с особенностями ИТКС Пользователя; * Предоставление обновлений (hotfix), устраняющих дефекты, выявленные в продукте; * Предоставление обновлений (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии ПРОДУКТА (servicepack); * Предоставлений новых версий (изменение мажорной (MAJOR) версии, поколения) ПРОДУКТА без взимания дополнительной платы (для ПАК — только программные компоненты). |
| Передача неисключительного права на использование СЗИ НСД | 1 | 1. СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов. 2. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, WindowsVista, Windows 7, Windows 8, Windows 8.1, Windows 10, WindowsServer 2003, WindowsServer 2003 R2, WindowsServer 2008, WindowsServer 2008 R2, WindowsServer 2012, WindowsServer 2012 R2, в многопользовательском режиме их эксплуатации. 3. СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем. 4. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go. 5. СЗИ НСД должна быть сертифицирована на соответствие требованиям Руководящих документов (РД СВТ, Гостехкомиссия России, 1992 г.) к 5-му классу защищенности от НСД для СВТ и 4-му уровню контроля отсутствия НДВ (РД НДВ, Гостехкомиссия России, 1999 г.), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. 6. Модуль СКН должен быть сертифицирован на соответствие требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации по 4-му классу защиты в соответствии с профилем защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ). 7. СЗИ НСД может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно. 8. СЗИ НСД должна обеспечивать:    1. регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере;    2. идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows;    3. реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;    4. возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в операционную систему;    5. возможность настройки принудительной двухфакторной аутентификации для учётной записи с правами администратора и/или пользователя;    6. возможность средствами СЗИ НСД выполнить настройку периода действия учётной записи;    7. возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;    8. возможность при создании учётной записи выбрать тип учётной записи (внутренний, внешний, системный, приложение, гостевой, временный);    9. 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), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;    10. контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:    * Android-устройств;    * iOS-устройств;    * Bluetooth-устройств;    * DVD- и CD-ROM-дисководов;    * устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;    * USB-контроллеров;    * беспроводныхустройств (Wireless Communication Devices);    * биометрических устройств;    * дисководов магнитных дисков;    * звуковых, видео- и игровых устройств;    * инфракрасных устройств (IrDA);    * контроллеров магнитных дисков;    * ленточных накопителей;    * модемов;    * переносных устройств;    * портов (COM и LPT);    * сенсоров;    * сетевых адаптеров;    * сканеров и цифровых фотоаппаратов;    * принтеров;    * съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).    1. предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;    2. преобразование информации:    * на съемных носителях информации для создания доверенной среды при работе со съемными носителями;    * при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);    * при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.    1. блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;    2. возможность работы с преобразованными файлами-контейнерами на компьютерах, где программное обеспечение СЗИ НСД не установлено;    3. сохранение теневых копий файлов, записываемых на съемные носители;    4. использование дискреционного принципа контроля доступа:    * обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).    1. возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);    2. регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей;    3. расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;    4. возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;    5. возможность разграничения доступа к буферу обмена;    6. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);    7. возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;    8. очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Запрет смены пользователей без перезагрузки;    9. выполнение регистрации действий по зачистке остаточной информации;    10. возможность самодиагностики основного функционала СЗИ НСД с возможностью сохранения отчета;    11. возможность сохранения конфигурации для последующего восстановления СЗИ НСД;    12. ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;    13. возможность настройки репликации серверов безопасности;    14. централизованное управление лицензиями на терминальные подключения и на клиентов в нескольких доменах безопасности при использовании отдельного модуля «Сервер лицензий»;    15. централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора;    16. возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании-разработчика СЗИ НСД;    17. возможность использования SQL базы данных для централизованного хранения событий аудита;    18. возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:    * нарушение контроля целостности объекта;    * попытка работы после блокировки при нарушении целостности;    * попытка входа на клиентскую рабочую станцию с неправильным паролем;    * блокировка пользователя после многократного ввода неправильного пароля;    * СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);    * клиент недоступен долгое время (с возможностью задания периода времени);    * попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.    1. блокировку доступа к файлам по расширению;    2. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;    3. возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;    4. возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления;    5. возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик ActiveDirectory. Проверка подписи файлов при обновлении СЗИ НСД;    6. возможность визуализации сети защищаемых компьютеров;    7. возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования);    8. возможность выполнять синхронизацию времени между сервером безопасности и клиентами;    9. возможность интеграции с SIEM-системами. 9. Должен быть реализован модуль межсетевого экрана. Данный модуль должен обеспечивать защиту рабочих станций и серверов от НСД посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы рабочих станций сетевых пакетов в соответствии с заданными администратором правилами.   Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы: USB-Flash-накопители, TouchMemory (iButton), eTokenPro/Java (USB-ключи и смарт-карты), USB-ключи Rutoken, JaCarta ГОСТ/PKI (USB-ключи и смарт-карты), карты HID Proximity. |
| Установочный комплект СЗИ от НСД | 1 | Установочный комплект СЗИ от НСД должен включать:   * Верифицированный дистрибутив; * Паспорт изделия (формуляр); * Копию сертификата соответствия по требованиям безопасности информации. |
| Средство антивирусной защиты | 1 | Срок действия лицензии не менее 36 мес.;  Количество клиентских лицензий – 5шт;  Наличие единого центра управления и сбора информации;  Все компоненты программного обеспечения должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем продлеваемого программного обеспечения;  При оказании услуг должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие персональные компьютеры, не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным обеспечением, включающим в себя защиту от проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты;  Предоставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика;  Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке;  Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке;  Предоставляемый серийный номер должен иметь возможность отложенной активации.  Срок действия лицензионных ключевых файлов на все программные продукты должен начинаться с момента активации серийного номера;  Антивирусные средства должны включать:   * программные средства защиты рабочих станций; * программные средства защиты серверов; * программные средства централизованного управления, мониторинга и обновления; * обновляемые базы данных сигнатур вредоносных программ всех типов и атак; * эксплуатационную документацию на русском языке.   Программное обеспечение (в том числе с помощью системы централизованного управления), используя актуальную версию, должно обеспечивать защиту рабочих станций под управлением операционных систем:   * Windows XP Professional (такжес SP1 ивыше); * WindowsServer 2003 (также с SP1 и выше); * WindowsServer 2008 (также с SP1 и выше); * WindowsServer 2012 * Windows 7; * Windows 10; * ОС из реестра отечественного ПО, в т.ч ОС ALT Linux |
| Установочный комплект средства антивирусной защиты информации | 1 | Установочный комплект средства антивируснойзащиты должен включать:   * Верифицированный дистрибутив; * Паспорт изделия (формуляр); * Копию сертификата соответствия по требованиям безопасности информации. |
| Внедрение средств защиты информации | 1 | Требования к установке и настройке средств защиты информации:   * Должна быть произведена тестовая инсталляция и настройка программных средств защиты информации с целью проведения тестовой эксплуатации работы программных средств защиты информации; * После проведения тестовой эксплуатации должна быть проведена установка и настройка программных средств защиты информации на все рабочие места операторов; * Настройка программных средств защиты информации производится в соответствии с требованиями руководящих документов ФСТЭК по защите информации и должна учитывать существующий технологический процесс обработки информации; * По результатам установки и настройки, должен быть подготовлен отчет, включающий детальное описание настроек подсистем системы защиты информации; * По окончании установки и настройки программных средств защиты информации составляются акты установки и готовности средств защиты информации; * Установка и настройка программных средств защиты информации не должна существенно нарушать рабочий процесс Учреждения. Время прекращения функционирования не должно превышать: 1,5 часа для рабочих станций |

***Требования к Исполнителю:***

*Наличие лицензии ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) со следующими видами работ:*

* *Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств*
* *Передача шифровальных (криптографических) средств.*

*Наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации со следующими видами работ:*

* *Услуги по установке, монтажу, испытаниям, ремонту средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).*

1. Поставка эквивалента недопустима в связи с необходимостью обеспечить совместимость с уже существующей защищённой сетью, построенной по технологии ViPNet [↑](#footnote-ref-1)