**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на оказание комплекса услуг по защите информации и аттестации информационной системы персональных данных Бюджетного профессионального образовательного учреждения Вологодской области «Великоустюгский медицинский колледж  
имени Н. П. Бычихина»**

**ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ**

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ИС | Информационная система |
| ИСПДн | Информационная (-ых) система (-х) персональных данных |
| НСД | Несанкционированный доступ к информации |
| ПДн | Персональные данные |
| ПО | Программное обеспечение |
| РФ | Российская Федерация |
| СЗИ | Средство (-а) защиты информации |
| СКЗИ | Средство (-а) криптографической защиты информации |
| СЗПДн | Система защиты персональных данных |
| ФСБ России | Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |

**ОБЩИЕ СВЕДЕНИЯ**

Настоящий документ содержит техническое задание на оказание комплекса услуг по защите информации и аттестации информационной системы персональных данных Бюджетного профессионального образовательного учреждения Вологодской области «Великоустюгский медицинский колледж имени Н. П. Бычихина».

1. **ЗАКАЗЧИК УСЛУГ**

Заказчик – Бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский медицинский колледж имени Н. П. Бычихина» (далее – БПОУ ВО «Великоустюгский медицинский колледж имени Н. П. Бычихина»).

Юридический адрес: 162390, Вологодская область, Великоустюгский район,  
г. Великий Устюг, ул. Павла Покровского, д. 2А.

## ЦЕЛЬ И ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

* 1. Основной целью оказания услуг является обеспечение защиты ПДн от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных несанкционированных действий в отношении такой информации, обрабатываемой в информационной системе персональных данных БПОУ ВО «Великоустюгский медицинский колледж имени Н. П. Бычихина» (далее – ИСПДн).
  2. Оказываемые услуги должны включать в себя мероприятия по реализации организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения установленных требований к защите ПДн.
  3. Задачи, подлежащие решению при оказании услуг:
* уточнение исходных данных;
* поставка, установка и настройка СЗИ (согласно требованиям, приведенным в приложении № 1 к настоящему Техническому заданию);
* разработка необходимой организационно-распорядительной и технической документации;
* проведение приемо-сдаточных испытаний межсетевого взаимодействия ИСПДн;
* аттестационные испытания ИСПДн на соответствие требованиям безопасности информации.
  1. Срок оказания услуг: 180 календарных дней с даты подписания договора.

1. **ХАРАКТЕРИСТИКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ**
   1. Обработка ПДн осуществляется в рамках ИСПДн.
   2. Обработка, хранение и передача ПДн в ИСПДн происходит с использованием программных и технических средств.
   3. Аппаратной платформой для программных средств обработки ПДн является автоматизированное рабочее место пользователей ИСПДн.
   4. В состав ИСПДн входит 1 АРМ пользователей по адресу: 162390,  
      Вологодская область, Великоустюгский район, г. Великий Устюг, ул. Павла Покровского,  
      д. 2А.
2. **ТРЕБОВАНИЯ К ОБЪЕМУ ОКАЗЫВАЕМЫХ УСЛУГ**

Оказание комплекса услуг по защите информации и аттестации ИСПДн включает в себя следующие мероприятия:

* 1. Обновление СЗПДн.
     1. Исполнитель выполняет поставку, обновление, установку и настройку СЗИ и СКЗИ на АРМ Заказчика (согласно требованиям, приведенным в Приложении 1 к настоящему Техническому заданию).
     2. Установка и настройка СЗИ и СКЗИ осуществляется Исполнителем в соответствии с требованиями нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с эксплуатационной документацией на СЗИ и СКЗИ. Исполнитель предоставляет Заказчику акт установки СЗИ и СКЗИ.
     3. Заказчик предоставляет технические и программные средства для установки средств защиты информации. Состав программных и аппаратных средств, предоставляемых Заказчиком, должен соответствовать требованиям, указанным в формулярах на поставляемые СЗИ и СКЗИ.
     4. Проведение приемо-сдаточных испытаний схемы подключения ИСПДн к федеральной ИС (защищенная сеть).
  2. Проверка состояния технологического процесса автоматизированной обработки защищаемой информации, в том числе ПДн, включающая в себя:
* анализ обобщённой технологической схемы ИСПДн с существующими информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации, в том числе ПДн;
* проверку соответствия описания технологического процесса обработки, хранения и передачи информации ограниченного доступа реальной практике на объекте;
* определение субъектов и объектов доступа и средств обработки и передачи информации;
* проверку данных ИСПДн, представленных в техническом паспорте;
* проверку наличия оформленных разрешений на допуск персонала к конфиденциальной информации, меток конфиденциальности на информационных носителях, соответствия технологических инструкций пользователей и администратора безопасности установленным требованиям;
* установление опасных факторов и угроз, критических мест ИСПДн, снижающих уровень защиты.
  1. Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации, включающая в себя:
* проверку правильности классификации ИСПДн;
* проверку уровня подготовки кадров и распределения ответственности персонала;
* проверку комплектности и характеристик средств защиты, наличия сертификатов соответствия на средства вычислительной техники (СВТ) и средства защиты информации (СЗИ);
* проверку выполнения требований к помещениям, в которых производится обработка информации средствами ИСПДн.
  1. **Разработка (актуализация) организационно-распорядительной и технической документации, требуемой для аттестации ИСПДн.**

Все организационно-распорядительные и технические документы, разрабатываемые Исполнителем в процессе оказания услуг, должны быть загружены Исполнителем в базу данных ПО для автоматизации организационных мероприятий по обеспечению информационной безопасности (онлайн-сервиса), поставляемого в рамках данного ТЗ (в соответствии с Приложением 1 настоящего ТЗ). Исполнитель проводит инструктаж пользователей ИСПДн по использованию ПО для автоматизации организационных мероприятий по обеспечению информационной безопасности (онлайн-сервиса).

* 1. **Проведение аттестационных испытаний.**
     1. **Исполнителем проводятся испытания** ИСПДн на соответствие требованиям по безопасности информации. Испытания проводятся в соответствии с утвержденной Исполнителем и согласованной с Заказчиком «Программой и методиками аттестационных испытаний».
     2. По результатам испытаний ИСПДн **Исполнителем** оформляются Протокол аттестационных испытаний и Заключение с выводом о соответствии объекта информатизации требованиям по безопасности информации.

При выявлении несоответствия, в Заключении указываются выявленные недостатки с рекомендациями по их устранению.

# ТРЕБОВАНИЯ К ПОСТАВЛЯЕМЫМ СЗИ

* 1. Исполнитель должен обеспечить:
* предпродажную подготовку СЗИ в соответствии с требованиями (приложение № 1 к настоящему Техническому заданию);
* работоспособность поставляемых СЗИ.
  1. ПО поставляемых СЗИ должно иметь действующие сертификаты.
  2. При оказании услуг должны соблюдаться все авторские и смежные с ними права разработчика СЗИ.

# ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ ПРИ ОКАЗАНИИ УСЛУГ

* 1. **Исполнитель обязан использовать исправные и поверенные приборы, инструменты и средства измерений.**
  2. **Исполнитель обязан оказывать услуги в соответствии с требованиями эксплуатационной документации на приборы, инструменты и средства измерений с соблюдением норм и правил техники безопасности.**
  3. **Исполнитель** устанавливает и настраивает СЗИ в соответствии **с требованиями законодательства по защите информации,** а также в соответствии с эксплуатационной документацией на СЗИ.
  4. **Все** организационно-распорядительные документы, разрабатываемые Исполнителем в процессе оказания услуг, должны соответствовать технологии обработки информации в ИСПДн.
  5. Организационно-распорядительные документы должны создавать условия для обеспечения защиты ПДн от угроз несанкционированного доступа, инсайдерских угроз, угроз хищения носителей информации.

# ПОРЯДОК ПРИЕМКИ РЕЗУЛЬТАТОВ РАБОТ

* 1. Исполнитель обязан своевременно предоставить отчетную документацию Заказчику в порядке, определенном Договором и в соответствии с разделом 4 [«](#_ПОРЯДОК_ОПЛАТЫ_ОКАЗАННЫХ)Требования к объему оказываемых услуг» настоящего ТЗ.
  2. Исполнитель должен уведомить Заказчика о готовности к сдаче-приемки работ в срок, не превышающий 5 (пять) дней до даты окончания работ.
  3. Документы должны быть представлены в бумажном виде, в 1 экземпляре, и в электронном виде в 1 экземпляре.
  4. Документы, передаваемые в электронном виде, должны быть представлены в форматах MS Office (в формате \*.doc/\*docx для текстовых документов, \*.xls/\*xlsx для таблиц и расчетов и \*.vsd/\*vsdx для схем и чертежей). Все комплекты документов, передаваемых в бумажном виде, должны предоставляться в адрес Заказчика с сопроводительным письмом.
  5. Экспертизу и приемку результатов работ осуществляет Заказчик. Заказчик имеет право для приемки работ привлекать внешнюю экспертизу.
  6. В случае отсутствия замечаний, Заказчик в течение 5 (пяти) рабочих дней с момента завершения приемки подписывает два экземпляра Акта сдачи-приемки выполненных работ и возвращает 1 (один) экземпляр Исполнителю. В случае наличия замечаний, Заказчик направляет Исполнителю мотивированный отказ от приемки работ с перечнем необходимых доработок и указанием сроков их выполнения. Исполнитель должен устранить недостатки в указанные сроки и предъявить результаты Заказчику. Повторная приемка работ должна осуществляться в порядке, определенном настоящим разделом.
  7. Оплата работ Заказчиком предусматривается в случае приемки работ на основании подписанного Исполнителем и Заказчиком Акта сдачи-приемки выполненных работ.

# ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

Исполнитель должен обеспечить гарантийное обслуживание поставленного (используемого) оборудования на следующих условиях:

* исполнитель гарантирует, что поставляемое (используемое) оборудование соответствует требованиям, приведенным в Приложении 1 настоящего Технического задания, а также свободно от дефектов материалов и изготовления;
* срок гарантии производителя на все поставленное оборудование должен составлять не менее 12 месяцев.

# ТРЕБОВАНИЯ К ЛИЦЕНЗИРОВАНИЮ ИСПОЛНИТЕЛЯ

В соответствии с подпунктом 5 пункта 1 статьи 12 Федерального закона № 99-ФЗ «О лицензировании отдельных видов деятельности» от 04 мая 2011 года Исполнитель обязуется предоставить документы, подтверждающие соответствие оказываемых услуг требованиям законодательства:

* копию действующей лицензии ФСБ России на осуществление деятельности 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;
* копию действующей лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

# ТРЕБОВАНИЯ К КАЧЕСТВУ УСЛУГ

Услуги должны оказываться с соблюдением требований Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и принятыми в соответствии с ним нормативно-методическими документами, устанавливающими требования к защите персональных данных.

Качество и комплектность СЗИ и ПО должны соответствовать требованиям, предъявляемым к техническим характеристикам товара в стране производителя, а также действующим в РФ стандартам и техническим условиям. Упаковка, в которой поставляется ПО, должна обеспечивать ее сохранность при транспортировке и хранении. Маркировка на упаковке должна соответствовать действующим стандартам.

# ИСТОЧНИКИ РАЗРАБОТКИ

Исполнитель при оказании услуг должен обеспечивать соблюдение следующих федеральных законов, постановлений Правительства Российской Федерации и нормативных актов:

* Федеральный закон от 27 июля 2006 года № 152***-***ФЗ «О персональных данных»;
* Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432).
* Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

# ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

Приложение 1 к Техническому заданию

**Перечень поставляемых средств защиты информации**

| **№ п/п** | **Наименование средств защиты информации** | **Функциональные характеристики средств защиты информации** | **Количество,**  **шт.** |
| --- | --- | --- | --- |
|  | Сертификат активации технической поддержки средства криптографической защиты информации, реализующего функции клиента | Комплект поставки сертификата активации технической поддержки средства криптографической защиты информации, реализующего функции клиента, должен включать в себя:   * сертификат прямой расширенной технической поддержки на срок не менее 1 (одного) года. | 1 |
|  | Средство защиты информации от несанкционированного доступа с модулями  защиты от НСД, контроля устройств, защиты диска и шифрования контейнеров, персонального межсетевого экрана, антивируса, обнаружения вторжений | Средство защиты информации от несанкционированного доступа (далее – НСД) должно осуществлять:   * + защиту серверов и рабочих станций от НСД;   + контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;   + разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;   + разграничение доступа пользователей к информации;   + контроль утечек информации;   + антивирусную защиту от вредоносного программного обеспечения;   + обнаружение и предотвращение вторжений;   + аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети;   + фильтрацию сетевых пакетов;   + защиту установленных сетевых соединений;   + шифрование данных, хранящихся в криптоконтейнерах;   + регистрацию событий безопасности и аудит;   + паспортизацию используемого программного обеспечения.   ***Требования к сертификации и применению в информационных системах:***  СЗИ должно соответствовать требованиям документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, «Требования к межсетевым экранам» (ФСТЭК России, 2016) не ниже 4 класса защиты, «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)» не ниже 4 класса защиты, «Профиль защиты средств антивирусной защиты типа «А» четвертого класса защиты» ИТ.САВЗ.А4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «Б» четвертого класса защиты» ИТ.САВЗ.Б4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «В» четвертого класса защиты» ИТ.САВЗ.В4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «Г» четвертого класса защиты» ИТ.САВЗ.Г4.ПЗ (ФСТЭК России, 2012), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) не ниже 4 класса защиты, «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2011), «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) не ниже 4 класса защиты, «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014).  СЗИ должно допускать использование в следующих информационных системах:   * + автоматизированные системы - до класса 1Г (включительно);   + государственные информационные системы – до 1 класса защищенности (включительно);   + информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно);   + автоматизированные системы управления производственными и технологическими процессами до 1 класса защищенности (включительно).   СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин.  ***Требования к операционной платформе и аппаратной части:***  СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):   * + Windows 10;   + Windows 8.1;   + Windows 7 SP1;   + Windows Server 2019;   + Windows Server 2016   + Windows Server 2012/2012 R2;   + Windows Server 2008 R2 SP1.   Должна быть возможность установки СЗИ по произвольному пути.  СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix.  СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMware ESX(i) и Microsoft Hyper-V.  СЗИ должно поддерживать работу с технологией Personal vDisk Citrix XenDesktop.  СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory.  СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ.  СЗИ не должно требовать при развертывании модификации топологии локальной вычислительной сети.  СЗИ должно иметь в составе дистрибутива драйвера для поддержки аппаратных идентификаторов.  В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе).  ***Требования к функциональности СЗИ:***  СЗИ должно выполнять следующие функции по защите информации:   1. Контроль входа пользователей в систему и работа пользователей в системе:    * проверка пароля пользователя при входе в систему;    * поддержка аппаратных средств аутентификации:    * идентификаторы iButton (типы DS1992 — DS1996);    * USB-ключи eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta ГОСТ Flash, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ, JaCarta PRO, JaCarta-2 PRO/ГОСТ, JaCarta WebPass, JaCarta-2 SE, JaCarta U2F, JaCarta LT, Rutoken S, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken ЭЦП Touch, Rutoken ЭЦП PKI, Rutoken ЭЦП Flash 2.0, Rutoken ЭЦП Bluetooth, Rutoken Lite, ESMART Token, ESMART Token ГОСТ, ESMART Token D.    * смарт-карты eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PRO, JaCarta-2 PRO/ГОСТ, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken Lite, ESMART Token, ESMART Token ГОСТ, ESMART Token D, с любыми совместимыми USB-считывателями;    * возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;    * возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);    * однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);    * возможность блокирования входа в систему локальных пользователей;    * возможность блокирования операций вторичного входа в систему в процессе работы пользователей;    * возможность блокировки сеанса работы пользователя по истечении интервала неактивности;    * возможность управления политикой сложности паролей;    * поддержка возможности входа в систему по сертификатам;    * возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.    * возможность оповещения пользователя о последнем успешном входе в систему;    * возможность выдачи пользователю предупреждения в виде сообщения о том, что в информационной системе реализованы меры защиты информации. 2. Избирательное (дискреционное) управление доступом:    * возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;    * возможность наследования прав доступа для файлов, каталогов и устройств;    * возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту. 3. Полномочное (мандатное) управление доступом:    * возможность заведения в системе не менее 10 уровней конфиденциальности;    * возможность выбора уровня конфиденциальности сессии для пользователя;    * возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;    * возможность изменения количества мандатных меток в системе и их названий;    * контроль потоков конфиденциальной информации в системе;    * возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP. 4. Контроль вывода конфиденциальных данных на печать:    * возможность ограничить перечень мандатных меток информации для печати на заданном принтере;    * теневое копирование информации, выводимой на печать:    * должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;    * должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом Windows Search.    * автоматическая маркировка документов, выводимых на печать;    * управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать:    * отдельный вид грифа для каждой мандатной метки;    * отдельный вид маркировки для первой страницы документа;    * отдельный вид маркировки для последней страницы документа;    * вид маркировки для оборота последнего листа;    * поддержка функции печати в файл;    * поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях. 5. Контроль аппаратной конфигурации компьютера и подключаемых устройств.  * Должны контролироваться следующие устройства:   + последовательные и параллельные порты;   + локальные устройства;   + сменные, физические и оптические диски;   + программно реализованные диски;   + USB-устройства;   + PCMCIA-устройства;   + IEEE1394 (FireWire)-устройства;   + устройства, подключаемые по шине Secure Digital. * Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства. * Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации. * Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться. * Должна быть возможность группового добавления устройств в подсистему контроля устройств без подключения устройства к компьютеру. * Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации:   + должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;   + должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом Windows Search. * В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя. * При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств. * Контроль сетевых интерфейсов:   + Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).   + Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя.   + Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии Active Scripts.   + Список модулей, разрешенных для запуска, должен строиться:   + с помощью явного указания модулей;   + по информации об установленных на компьютере программах;   + по зависимостям исполняемых модулей;   + по ярлыкам в главном меню;   + по событиям журнала безопасности. * Контроль целостности файлов, каталогов, элементов системного реестра:   + Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя.   + Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.   + Должна быть возможность восстановления исходного состояния контролируемого объекта.   + Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.   + При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.   + Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей.   + Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации.   + Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации.   + Затирание информации на локальных и сменных дисках по команде пользователя.   + Возможность настройки количества проходов затирания информации отдельно для локальных дисков, съемных носителей, оперативной памяти.   + Затирание данных и имен файлов, каталогов при удалении информации.   + Возможность добавления объектов файловой системы в исключения подсистемы затирания данных.   + Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. * Шифрование контейнеров:   + Должна обеспечиваться возможность создания зашифрованных контейнеров (криптоконтейнеров) с возможностью подключения их к системе как виртуальных дисков.   + Вся информация, размещаемая в контейнере, должна шифроваться по алгоритму ГОСТ 28147-89.   + Ключевая информация для обеспечения шифрования и расшифровки данных в криптоконтейнерах должна размещаться в аппаратных идентификаторах или на съемном USB-носителе.   + Должна быть возможность выбора размера криптоконтейнера при его создании.   + Должна поддерживаться возможность автоматического и ручного подключения криптоконтейнера по команде пользователя.   + Доступ к криптоконтейнерам должен регулироваться дискреционными правилами разграничения доступа. * Защита сетевого взаимодействия и фильтрация трафика:   + Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.   + Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры).   + Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов.   + Должны быть предусмотрены механизмы защиты установленных сетевых соединений между субъектами доступа (пользователями и компьютерами) и защищаемыми объектами (серверами и информационными системами) на основе открытых стандартов протоколов семейства IPsec, которые позволяют контролировать аутентичность и целостность передаваемых данных.   + Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты:   + соединение без защиты;   + маркируется каждый пакет;   + подписывается заголовок каждого пакета;   + подписывается каждый пакет целиком.   + Должна быть возможность ограничивать сетевые соединения по правилам фильтрации:   + на уровне отдельных протоколов из стека TCP/IP;   + на уровне параметров протоколов стека TCP/IP;   + на уровне параметров служебных протоколов стека TCP/IP;   + на уровне периодов времени;   + на уровне пользователей или групп пользователей;   + на уровне параметров прикладных протоколов;   + на уровне исполняемого файла/процесса;   + на уровне сетевого адаптера.   + Должна быть возможность осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода.   + Должна быть возможность маркировки сетевого трафика метками конфиденциальности.   + Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации:   + регистрация информации в журнале;   + звуковая сигнализация;   + запуск программы или сценария.   **Обнаружение и предотвращение вторжений:**   * + Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов.   + Должна быть возможность блокировки вредоносных сетевых адресов (IP, URL).   + Сигнатурные механизмы должны обеспечивать проверку HTTP-трафика на наличие заданных конструкций как для входящего, так и для исходящего сетевого трафика. При обнаружении признаков атаки прохождение подозрительных сетевых пакетов должно быть заблокировано.   + Эвристические механизмы должны распознавать и фиксировать следующие типы атак:   + сканирование портов;   + подделка ARP (ARP-spoofing);   + SYN-флуд;   + атаки, направленные на отказ в обслуживании (DoS);   + распределенные атаки, направленные на отказ в обслуживании (DDoS).   + При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера.   + Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов.   **Антивирусная защита:**   * + Должна обеспечиваться автоматическая проверка наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа.   + Должно обеспечиваться сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию.   + Должна быть возможность указать расписание запуска антивирусных проверок с возможностью выбора ежечасного запуска, запуска в заданное время ежедневно, запуска в заданный день недели и время еженедельно или по событиям запуска СЗИ и событию успешного обновления баз.   + Профили антивирусного сканирования должны поддерживать настройку следующих параметров:   + название и описание;   + уровень эвристического анализа;   + проверка или пропуск архивов;   + пропуск файлов больше заданного размера;   + проверка файлов только с заданным перечнем расширений;   + действия с обнаруженными вредоносными объектами – лечение, удаление, помещение в карантин;   + объекты сканирования, включая возможность указать проверку исполняемых процессов в оперативной памяти, проверку загрузочных секторов, проверку локальных, съемных и сетевых дисков и перечень проверяемых директорий.   + Должно обеспечиваться удаление вредоносного программного обеспечения и его блокировка (перемещение в карантин).   + Должно обеспечиваться восстановление файлов из карантина по команде администратора.   + Должен поддерживаться список файлов и директорий, исключаемых из проверки (белый список).   + Должна обеспечиваться возможность обновления баз данных признаков компьютерных вирусов (антивирусных баз), в том числе с доступом к серверу обновлений через прокси-сервер.   + Должен обеспечиваться контроль целостности антивирусных баз и защита от их подмены при загрузке с сервера обновлений.   + Должна обеспечиваться возможность развертывания зеркала сервера обновлений в локальной сети.   + Должна быть реализована возможность обновления антивирусных баз со съемных носителей и по локальной сети, без доступа к серверу обновлений.   Функциональный контроль ключевых компонентов системы.   * + Регистрация событий безопасности в журнале.   + Должна быть возможность формирования отчетов по результатам аудита.   + Должна быть возможность поиска и фильтрации при работе с данными аудита.   ***Требования к централизованному управлению в доменной сети:***   * + СЗИ должно предоставлять следующие возможности по управлению системой:   + Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров.   + Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты.   + Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности.   + Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров.   + Возможность настройки отображения диаграмм (детализации, цветовой гаммы), добавления, удаления, перемещения диаграмм на панели мониторинга.   + Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер).   + Выполнение команд, специфичных для защитных подсистем – удаленный запуск антивирусной проверки и обновления базы данных признаков компьютерных вирусов, включение и отключение режима обучения сетевой фильтрации и т.д.   + Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера.   + Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров.   + Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования.   + Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз.   + Возможность инвентаризации объектов файловой системы компьютера с последующим сохранением отчета в виде эталонного паспорта. Возможность сравнения нового паспорта с эталонным, возможность переопределения эталона.   + Возможность создания отчетов о настройках системы, установленных программах, зарегистрированных аппаратных средствах аутентификации.   + Возможность создания шаблонов политик:   + возможность создания шаблона по настроенным политикам СЗИ на компьютере;   + возможность проверки соответствия настроенных политик СЗИ на компьютере с выбранным шаблоном;   + возможность распространения (применения) шаблонов политик на компьютер или группу компьютеров.   + Централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу, при этом система должна позволять:   + распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов);   + посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов);   + создавать иерархию серверов безопасности с не менее чем 3 уровнями вложенности.   + Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности).   **Комплект поставки должен содержать:**  Неисключительное право на программное обеспечение средство защиты информации от несанкционированного доступа с модулями защиты от НСД, контроля устройств, защиты диска и шифрования контейнеров, персонального межсетевого экрана, антивируса, обнаружения вторжений, на срок не менее 1 года. | 1 |
|  | Дистрибутив средства защиты информации от несанкционированного доступа | Комплект поставки дистрибутива средства защиты информации от несанкционированного доступа должен включать в себя:   * CD в конверте с записанными сертифицированными приложениями; * формуляр; * заверенная копия сертификата ФСТЭК России. | 1 |
|  | Программное обеспечение для автоматизации организационных мероприятий по обеспечению информационной безопасности | ПО должно представлять собой онлайн-сервис и позволять автоматизировать разработку и ведение организационно-распорядительной документации в сфере информационной безопасности.  ПО должно обеспечивать работу с неограниченным числом организаций.  Создание внутренней документации каждой организации должно быть доступно как вручную, так и с использованием готовых шаблонов.  ПО должно обеспечивать выполнение следующих основных функций:   * автоматизация и систематизация разработки и ведения организационно-распорядительной документации в области информационной безопасности:   + создание внутренней документации организации в области информационной безопасности как вручную, так и с использованием готовых шаблонов;   + поддержание созданной документации в актуальном состоянии; * выполнение требований надзорных органов в области использования средств криптографической защиты информации и средств защиты информации; * инвентаризационный учёт активов, обеспечивающих информационную безопасность организации; возможность автоматического учета технических средств на основе отчетов из сканера уязвимостей RedCheck; * организация проведения совместных закупок в области информационной безопасности и информационных технологий; * учёт и обработка инцидентов в области информационной безопасности, назначение ответственных и задач для обработки инцидентов; возможность автоматического учета инцидентов на основе отчетов из сканера уязвимостей RedCheck; * учет и контроль проведения мероприятий для подготовки организации к проведению проверок надзорным органом в области информационной безопасности; возможность назначения и проведения видео-инструктажей для сотрудников организации; * информирование пользователей посредством SMS и Email-уведомлений о назначениях инцидентов, задач, а также изменениях в организационно-распорядительной документации; * ведение документооборота с системой согласования в том числе ведение юридически-значимых документооборота с подписанием усиленной квалифицированной электронной подписью; * предоставление доступа к данным системы посредством WEB-интерфейса и мобильного приложения.   В рамках функционирования ПО должно осуществляться взаимодействие со следующими внешними системами:   * система SMS-уведомлений; * система Email-уведомлений; * внешняя система юридически-значимого электронного документооборота.   Взаимодействие с системой SMS-уведомлений должно осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом данной системы.  Взаимодействие с системой Email-уведомлений должно осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом данной системы.  Взаимодействие с внешней системой юридически-значимого электронного документооборота осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом системы ЭДО Русь-Телеком.  ПО должно иметь клиент-серверную архитектуру и предусматривать WEB-интерфейс работы пользователя с базой данных и подсистемой ввода–вывода данных, в котором все операции бизнес-логики производятся на сервере. ПО должно поддерживать работу с использованием WEB-браузеров: Internet Explorer 10 и выше, Microsoft Edge, Google Chrome, Mozilla Firefox 3.0 и выше.  ПО должно быть зарегистрировано в государственном реестре программ и баз данных в соответствии с действующим законодательством как самостоятельная программа для ЭВМ.  Комплект поставки включает:   * лицензия на неисключительное право использования ПО в электронном виде. | 1 |