МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ КУЛЬТУРЫ И ИСКУССТВ ИМЕНИ МИХАИЛА МАТУСОВСКОГО» (АКАДЕМИЯ МАТУСОВСКОГО)

пл. Красная, д. 7, г. Луганск, г.о. город Луганск, ЛНР, 291001. Тел. +7 (8572) 59-02-62. E-mail: ilgaki@mail.ru
ИНН 9403019280 КПП 940301001 ОГРН 1229400075453

17.06.2025 № 882

На № _____ от _____

Руководителям предприятий, организаций, учреждений

Запрос ценовых предложений

Академия Матусовского в соответствии с Федеральным законом от 05.04.2013 г. №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», руководствуясь Постановлением Правительства Российской Федерации от 31.12.2022 г. № 2559 «О мерах по обеспечению режима военного положения и об особенностях планирования и осуществления закупок для обеспечения государственных нужд Донецкой Народной Республики, Луганской Народной Республики, Запорожской области, Херсонской области и муниципальных нужд муниципальных образований, находящихся на их территориях, и о внесении изменений в некоторые акты Правительства Российской Федерации» в целях формирования обоснования цены Контракта просит всех заинтересованных лиц предоставить ценовое предложение для организации закупки **предоставления услуг по обновлению средств защиты информации**

Из ответа на запрос должны однозначно определяться цена за единицу, срок действия предлагаемой цены.

Академия Матусовского не будет использовать ценовую информацию: предоставленную лицами, сведения о которых включены в реестр недобросовестных поставщиков; полученную из анонимных источников.

Настоящий запрос не является извещением о проведении закупки, не включает каких-либо обязательств Заказчика.

Адрес предоставления ценовой информации: Российская Федерация, ЛНР, г.о.город Луганск, г.Луганск, пл.Красная, д.4, каб. 1.12.

Адрес электронной почты для предоставления сканированных копий предложений: **akademzakupki@yandex.ru**

Контактное лицо: Казанцева Елена Алексеевна (8572) 50-19-25.

Срок предоставления ценовой информации до 20.06.2025 г.

Предполагаемый срок проведения закупки: июнь-июль 2025 г.

И.о. заведующего отделом закупок **Рыжова Л. Ю.**

Приложение
к запросу ценовых
предложений от 17.06.25 № 882

Техническое задание

Объект закупки: предоставление услуг по обновлению средств защиты информации
Общие требования к объекту закупки:

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
1.	Программный комплекс «ФИС ГИА» с дополнительными функциональными возможностями для защищенного подключения к ФИС ГИА и Приема	Программный комплекс «ФИС ГИА» с дополнительными функциональными возможностями предназначен для обеспечения выполнения требований регламента подключения (в том числе для продления подключения) к ФИС ГИА и Приема посредством защищенной сети передачи данных (сеть ViPNet № 2458). С помощью программного комплекса «ФИС ГИА» также можно создавать и проверять электронные подписи, зашифровывать и расшифровывать файлы, передаваемые по открытым каналам связи. Для выполнения криптографических операций программный комплекс «ФИС ГИА» использует алгоритмы формирования и проверки электронной подписи данных ГОСТ Р 34.10-2012 (с вычислением хэш-функции по ГОСТ Р 34.11-2012) и алгоритм шифрования информации ГОСТ 34.12-2018 и ГОСТ 34.13-2018. Программный комплекс «ФИС ГИА» включен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» (https://reestr.digital.gov.ru/), реестровая запись № № 26399 от 12.02.2025.. Предоставление должно быть в виде передачи: – неисключительного права использования программного комплекса «ФИС ГИА» с дополнительными функциональными возможностями для защищенного подключения к ФИС ГИА и Приема сроком на 1 год. ПК «ФИС ГИА» включает в себя:	1

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– сертификат прямой технической поддержки, уровень «Расширенный», на срок не менее 1 (одного) года для средства криптографической защиты информации, реализующего функции клиента	
2.	Средство защиты информации от несанкционированного доступа с дополнительными функциональными возможностями: 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: «Требование по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия; «Требования к межсетевым экранам» (ФСТЭК России, 2016) «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК	1

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		России, 2016), «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)»; «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 средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014); «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014); «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011); «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2011); «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности. 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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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;	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– 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.	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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).	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– 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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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 34.13-2018. – 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.	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– 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.	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– 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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		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.	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		– 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	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		безопасности). **Комплект должен содержать:** Неисключительное право на использование программного обеспечения средства 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.	

Описание мероприятий, входящих в состав дополнительных функциональных возможностей ПК «ФИС ГИА»

1. Установка и настройка СЗИ и СКЗИ.

1.1. Сублицензиар обновляет, устанавливает и настраивает СЗИ и СКЗИ на АРМ Сублицензиата (согласно требованиям, приведенным в Приложении № 1 к настоящему Техническому заданию).

1.2. Установка и настройка СЗИ и СКЗИ осуществляется Сублицензиаром в соответствии с требованиями нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с эксплуатационной документацией на СЗИ и СКЗИ. Сублицензиар предоставляет Сублицензиату акт установки СЗИ и СКЗИ.

1.3. Сублицензиат предоставляет технические и программные средства для установки средств защиты информации в срок, указанный Сублицензиаром. Состав программных и аппаратных средств, предоставляемых Сублицензиатом, должен соответствовать требованиям, указанным в формулярах на предоставляемые СЗИ и СКЗИ.

2. Актуализация (при необходимости) организационно-распорядительной и технической документации, требуемой для периодического технического контроля (испытания) ИСПДн.

3. Проведение периодического технического контроля.

3.1. **Сублицензиаром проводятся испытания** ИСПДн на соответствие требованиям по безопасности информации. Испытания проводятся в соответствии с представленной Сублицензиатом «Программой и методиками аттестационных испытаний».

3.2. Проверка состояния технологического процесса автоматизированной обработки защищаемой информации, включающая в себя:

– анализ обобщённой технологической схемы ИСПДн с существующими информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации;

– 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.

3.3. **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.

3.4. **По результатам испытаний ИСПДн Сублицензиаром оформляются Протокол периодического контроля и Заключение с выводом о соответствии объекта информатизации требованиям по безопасности информации.**

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

4. Проведение проверки схемы подключения ИСПДн к ФИС ГИА и Приема (защищенная сеть ViPNet № 2458).