

Описание объекта закупки (Техническое задание)

1. Наименование предмета закупки: Оказание услуг по подключению к информационно-телекоммуникационной системе с доступом в интернет на базе АРМ.

2. Место (места) оказания услуг: в соответствии с приложением 2 к Контракту «Сведения об обязательствах сторон и порядке оплаты».¹

3. Сроки оказания услуги: в соответствии с приложением 2 к Контракту «Сведения об обязательствах сторон и порядке оплаты».²

4. Общие положения

4.1. Термины и определения:

В настоящем Описании объекта закупки (техническом задании) применены следующие термины с соответствующими определениями:

АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ИС	Информационная система
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство (средства) защиты информации
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
УЗЗ	Уровень защищенности - 3

4.2. Цель оказания услуг: целью оказания услуг является подключение АРМ Заказчика к информационно-телекоммуникационной системе с доступом в интернет защищенная вычислительная сеть ViPNet № 2131 Правительства Московской области.

4.3. Наименование муниципального общеобразовательного учреждения и место нахождения Заказчика: указано в Таблице 3 Приложении № 3 к Описанию объекта закупки (техническому заданию).³

4.3. Технические требования к организации АРМ рабочего места информационной системы персональных данных: указано в Приложении № 2 к Описанию объекта закупки (техническому заданию).⁴

¹ Прилагается отдельным файлом (по каждому Заказчику)

² Прилагается отдельным файлом (по каждому Заказчику)

³ Прилагается отдельным файлом (по каждому Заказчику)

⁴ Прилагается отдельным файлом (по каждому Заказчику)

5. Задачи оказания услуг:

Для достижения цели должны быть решены следующие задачи:

- Обследование ИС заказчиков;
- Разработка Модели угроз и нарушителя безопасности информации;
- Разработка Технического проекта и проектов организационно-распорядительной документации по защите информации ИС;
- Установка и настройка СЗИ, прикладного ПО, в том числе шифровальных (криптографических) средств защиты информации;
- Проведение аттестационных испытаний ИС заказчиков на соответствие требованиям регуляторов в области защиты информации персональных данных по приказу № 21 ФСТЭК Российской Федерации по УЗЗ.

6. Основания оказания услуг:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России 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»;
- Приказ Федеральной службы по техническому и экспортному контролю от 27 февраля 2026 г. № 60 "О внесении изменений в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Утверждено Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.
- Методика оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 г.
- Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состав 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".
- Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании».
- Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Положение о лицензировании деятельности по технической защите конфиденциальной информации».
- Указ Президента Российской Федерации об утверждении перечня сведений конфиденциального характера от 6 марта 1997 г. №188.
- Федеральный закон Российской Федерации от 04 мая 2011 г. №99-ФЗ «О лицензировании отдельных видов деятельности».
- ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении;
- ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

7. Требование к исполнителю:

Исполнитель работ должен иметь действующую на период проведения работ лицензию:

- **Лицензия ФСТЭК России** на деятельность по технической защите конфиденциальной информации в составе следующего перечня выполняемых работ и услуг:

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
д) работы и услуги по проектированию в защищенном исполнении:

- средств и систем информатизации;

е) услуги по установке, монтажу, наладке, 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).

- **Лицензия 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)" в составе следующего перечня

выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств: **п.12, п.13, п.14, п.20, п.21, п.22, п.23, п.25, п.28** в соответствии с Приложением к Положению о лицензировании 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, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя):

п.12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации, и шифровальных (криптографических) средств, разработанных для применения в составе технологии, реализуемой промежуточными элементами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, сертифицированных Федеральной службой безопасности Российской Федерации, а также за исключением случая, если проведение указанных работ предусмотрено эксплуатационной документацией без привлечения лицензиата и они проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя.

п.13. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем, за исключением случая, если проведение указанных работ предусмотрено эксплуатационной документацией без привлечения лицензиата и они проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя.

п.14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем, за исключением случая, если проведение указанных работ предусмотрено эксплуатационной документацией без привлечения лицензиата и они проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя.

п.20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением

случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

п.21. Передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации, и шифровальных (криптографических) средств, разработанных для применения в составе технологии, реализуемой промежуточными элементами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, сертифицированных Федеральной службой безопасности Российской Федерации.

п.22. Передача защищенных с использованием шифровальных (криптографических) средств информационных систем.

п.23. Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.

п.25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

п.28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

8. Требования к порядку, составу и объему оказания услуг:

Услуга разбивается на пять основных частей и оказываются в соответствии с перечнем услуг и порядком сдачи приемки результатов их оказания (Таблица 1 Приложение № 1 к Описанию объекта закупки (техническому заданию)⁵.

8.1 Обследование ИС заказчиков:

Обследование информационной системы, аппаратного и программного обеспечения АРМ заказчиков производится лично представителем Исполнителя непосредственно по месту расположения АРМ Заказчика.

Удаленное обследование не допускается.

Обследование должно включать в себя:

- Анализ соответствия аппаратного и программного обеспечения АРМ Заказчика Техническим требованиям к организации АРМ рабочего места информационной системы персональных данных (Приложение № 2 к Описанию объекта закупки (техническому заданию));
- Анализ организационной структуры объекта информатизации, состава и структуры основных технических средств, системы защиты информации на объекте информатизации;
- Анализ состава объекта и субъектов доступа к информации, средств обработки и передачи информации в соответствии с разрешительной системой доступа персонала к информации на объекте информатизации;
- Анализ обобщенной технологической схемы с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой, хранимой и передаваемой информации и соответствия ее реальной практике, сложившейся на объекте информатизации;

⁵ Прилагается отдельным файлом (по каждому Заказчику)

- Проверка организации допуска персонала к защищаемой информации.

В случае несоответствия АРМ Заказчика по аппаратному обеспечению техническим требованиям рабочего места информационной системы персональных данных (Приложение

№ 2 к Описанию объекта закупки (техническому заданию), Исполнитель в течение одного рабочего дня с момента обследования АРМ должен предложить Заказчику системные, технические, программные и организационные решения по доработке ИС и модернизации АРМ в соответствии с Техническими требованиями (Приложение № 2 к Описанию объекта закупки (техническому заданию)).

При необходимости Исполнитель за свой счёт проводит работы по приведению АРМ Заказчика в соответствие с указанными требованиями. В случае необходимости замены комплектующих, Заказчик предоставляет необходимые запасные части, после чего работы по модернизации должны быть завершены в течение 2 (двух) рабочих дней.

8.2 Разработка Модели угроз и нарушителя безопасности информации.

8.2.1 Требования к разработке модели угроз и нарушителя безопасности информации ИС:

Модель угроз и нарушителя безопасности информации должна содержать описание ИС и ее структурно-функциональные характеристики, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз и нарушителя безопасности информации должна включать следующие разделы и их структуру:

- Общие положения:
 - назначение и область действия документа;
 - нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз;
 - наименование обладателя информации, заказчика, оператора ИС;
 - подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) ИС.
- Описание ИС, особенностей их функционирования, их характеристик как объектов защиты:
 - наименование ИС, для которых разработана модель угроз безопасности информации;
 - класс защищенности, уровень защищенности персональных данных;
 - нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют ИС;
 - цели и задачи (функции), решаемые ИС;
 - номенклатура и правовой режим защищаемых данных, обрабатываемых в ИС, и функциональных задач, для решения которых они используются;
 - назначение и структура объектов информатизации, основные автоматизируемые процессы;
 - описание структурно-функциональных характеристик ИС (состав технических и программных средств, сетевая инфраструктура);
 - описание наличия (отсутствия) взаимосвязей с другими информационными системами (подсистемами) и телекоммуникационными сетями;
 - описание групп внешних и внутренних пользователей ИС, уровней их полномочий и типов доступа;
 - описание процессов обеспечения информационной безопасности;
 - описание технологии обработки информации.
- Возможные негативные последствия от реализации (возникновения) угроз безопасности информации:
 - описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов;

- описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба).
- Описание потенциального нарушителя информационной безопасности с учетом особенностей объектов информатизации:
 - описание внешних нарушителей;
 - описание внутренних нарушителей;
- предположения о квалификации нарушителей и их возможностей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре ИС;
- предположения о технической вооруженности нарушителей.
- Описание объектов защиты, целей и способов атак:
 - перечень объектов защиты;
 - описание векторов атак:
 - возможные способы НСД к объектам защиты;
 - описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации.
 - каналы, используемые внутренним нарушителем для НСД к объектам защиты;
 - каналы, используемые внешним нарушителем для НСД к объектам защиты;
 - описание предполагаемых способов атак;
 - актуальные угрозы безопасности информации, включая:
 - наименование угрозы безопасности информации;
 - возможности нарушителя по реализации угрозы (соответствие угроз безопасности и субъектов атак);
 - используемые уязвимости ИС;
 - описание способов реализации угрозы безопасности информации;
 - объекты воздействия;
 - способ(ы) атаки;
 - возможные результат и последствия от реализации угрозы безопасности информации.
- Выводы о классификации нарушителей;
- Перечень актуальных угроз информационной безопасности;
- Выводы о необходимости применения сертифицированных СКЗИ с указанием класса СКЗИ.

При идентификации возможных угроз безопасности информации, в т.ч. должен использоваться Банк данных угроз безопасности информации, сформированный ФСТЭК России (<http://bdu.fstec.ru/>), учитывая структурно-функциональные особенности Системы, возможные источники угроз.

8.3 Разработка Технического проекта и проектов организационно-распорядительной документации по защите информации ИС.

8.3.1 Требования к техническому проекту на разработку системы защиты информации ИС:

На основе перечня актуальных угроз и возможностей нарушителя безопасности информации должны быть определены требования по защите информации, подлежащие реализации в составе СЗИ ИС. Требования к СЗИ ИС должны разрабатываться с учетом ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» и, в том числе, содержать:

- цель и задачи обеспечения защиты информации;
- класс защищенности ИС;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать ИС;

- перечень объектов защиты ИС;
- требования к мерам и средствам защиты информации, применяемым в ИС;
- этапы работ создания системы защиты ИС;
- перечень эксплуатационной и организационно-распорядительной документации;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

- функции Заказчика по обеспечению защиты информации на ИС.

8.3.2 Требования к разработке эксплуатационной документации на СЗИ ИС:

Эксплуатационная документация на СЗИ ИС, должна включать в себя:

- Инструкция администратора безопасности СЗИ ИС;
- Инструкция пользователя СЗИ ИС;
- Инструкция по антивирусному контролю ИС;
- Журнал периодических антивирусных проверок ИС;
- Журнал проверок контроля целостности ИС;
- Журнал учета обновления антивирусного ПО ИС;
- Журнал учета защищаемых носителей информации в ИС;
- Описание технологического процесса обработки информации в ИС;
- Технический паспорт ИС.

Инструкция администратора безопасности СЗИ ИС должна содержать инструкции по установке, настройке, регламентным работам, а также формы журналов учета, связанных с эксплуатацией СЗИ ИС.

Инструкция пользователя ИС должна содержать инструкции, необходимые для работы с ИС.

Технический паспорт ИС должен содержать сведения об используемых технических средствах, средствах защиты информации и программном обеспечении.

Описание технологического процесса обработки информации в ИС должно в полной мере описывать процесс обработки информации в ИС.

8.3.3 Требования к разработке организационно-распорядительной документации по организации деятельности по технической защите конфиденциальной информации и защите информации, обрабатываемой в ИС:

Разрабатываемая организационно-распорядительная документация по защите информации должна устанавливать порядок организации работ по защите информации, соответствовать требованиям и рекомендациям по обеспечению защиты информации Заказчика в соответствии с требованиями законодательства Российской Федерации в сфере защиты информации.

Должны определяться основные цели и задачи, а также должны быть выработаны единые принципы комплексного обеспечения безопасности информации Заказчика и мероприятия по их реализации.

Организационно-распорядительная документация на ИС и СЗИ ИС, должна включать в себя:

- Внутренний нормативный документ регламентирующий организацию деятельности по технической защите конфиденциальной информации;
- Перечень конфиденциальных сведений, обрабатываемых с использованием ИС;
- Разрешительная система доступа персонала к защищаемым ресурсам ИС;
- Перечень лиц, допущенных к ИС.

8.4 Установка и настройка СЗИ, прикладного ПО, в том чисел шифровальных (криптографических) средств защиты информации.

8.4.1 Требования к установке, настройке сертифицированных по требованиям безопасности информации программных и программно-технических средств защиты информации, прикладного ПО, в том чисел шифровальных (криптографических) средств защиты информации:

В рамках выполнения работ по подключению к информационно-телекоммуникационной системе с доступом в интернет на базе АРМ, для каждой ИС Заказчика, Исполнитель должен предоставить СЗИ и оказать услуги по установке и

настройке СЗИ, с учётом имеющейся информационно-телекоммуникационной инфраструктуры, в том числе её оборудования и ПО.

Заказчик при оказании Исполнителем услуг по установке и настройке СЗИ обязан допустить сотрудников Исполнителя к местам оказания услуг.

Услуги по установке и настройке СЗИ должны заключаться в следующем:

- установка СЗИ на ИС Заказчика;
- настройка взаимодействия подсистем СЗИ между собой;
- настройка учётных записей Заказчика на СЗИ;

- установка прикладного ПО на ИС Заказчика;
- установка шифровальных (криптографических) средств защиты информации.

Точные места установки СЗИ Исполнитель обязан согласовать с Заказчиком и ответственным (эксплуатирующим) лицом Заказчика.

На данном этапе оказания услуг Исполнитель должен произвести настройку СЗИ в соответствии с разрабатываемой Исполнителем разрешительной системой доступа (матрицей доступа), а также в соответствии с имеющимся у Заказчика технологическим процессом обработки информации. После установки и настройки СЗИ Исполнитель обязан проверить работоспособность и корректность работы установленных СЗИ с отражением по требованию заказчика результатов в Актах установки и настройки СЗИ.

По результатам установки и настройки СЗИ Исполнителем по требованию Заказчика составляется и подписывается Акт установки и настройки СЗИ в ИС отдельно для каждого АРМ Заказчика.

Перечень сертифицированных по требованиям безопасности информации программных средств защиты информации, прикладного ПО, в том числе шифровальных (криптографических) средств защиты информации, нуждающихся в установке и настройке:

№ п/п	Наименование ПО ⁶	Описание ПО	Количество
1	Средство защиты информации Secret Net Studio, Реестровая запись № 3855 от 16.08.2017 в реестре российского ПО	Право на использование комплекта «Постоянная защита» Средства защиты информации Secret Net Studio 8, срок использования – на срок действия исключительных прав	1
2	Средство защиты информации Secret Net Studio, Реестровая запись № 3855 от 16.08.2017 в реестре российского ПО	Право на использование комплекта «Дополнительная защита» Средства защиты информации Secret Net Studio 8, срок использования - 3 года	1
3	ViPNet Client 4, Реестровая запись №778 от 16.05.2016 в реестре российского ПО	Право на использование ПО ViPNet Client for Windows 4.x (КСЗ), срок использования – на срок действия исключительных прав	1
4	ViPNet Client 4, Реестровая запись №778 от 16.05.2016 в реестре российского ПО	Дистрибутив ViPNet Client for Windows	1
5	Средство анализа защищенности «Сканер-ВС», Реестровая запись №231 от 18.03.2016 в реестре российского ПО	Право на использование средство анализа защищённости «Сканер-ВС», Лицензия на 1 (один) год	1

⁶ Предоставление эквивалента невозможно в связи с использованием данных средств защиты информации в информационной системе (на рабочих местах) Заказчика, в связи с несовместимостью товаров, на которых размещаются другие товарные знаки, и необходимость обеспечения взаимодействия таких товаров с товарами, используемыми заказчиком в соответствии с пп. «б» п. 1 ч. 1 ст. 33 Федерального закона от 05.04.2013 г. №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд».

Дистрибутивы СЗИ и СКЗИ предоставляются Исполнителем.

8.4.2 Требования к дистрибутивам программного обеспечения:

Дистрибутивы СЗИ предоставляются Исполнителем и должны включать:

- ПО на оптическом носителе или в электронном виде;
- комплект эксплуатационной документации;
- формуляр;
- копию сертификата соответствия ФСТЭК на СЗИ от НСД, ФСБ, в том числе шифровальных (криптографических) средств защиты информации.

8.4.3 Требования к обеспечению бесперебойности работы информационных систем Заказчика и Пользователей ИС Заказчика:

При оказании услуг по установке и настройке СЗИ и ПО в ИС Заказчика Исполнитель обязан не нарушить работоспособность установленных в ИС технических средств и программного обеспечения, параметров их настройки, включая программное обеспечение средств защиты информации, управления учетными записями пользователей, системы восстановления работоспособности технических и программных средств.

При этом Исполнитель оказывает услуги по установке и настройке СЗИ и ПО в ИС Заказчика – в рабочие дни с 14:00 до 16:00. Исполнитель обязан уведомлять о времени проведения работ ответственное (эксплуатирующее) лицо Заказчика не позднее чем за пять рабочих дней до проведения работ. Оказание услуг Исполнителем в иное время допускается только по письменному согласованию отдельно с каждым ответственным (эксплуатирующим) лицом Заказчика. Допустимое время работы в каждой ИС Заказчика не должно превышать 2 (двух) часов.

8.5 Проведение аттестационных испытаний ИС заказчиков на соответствие требованиям регуляторов в области защиты информации персональных данных по приказу №21 ФСТЭК Российской Федерации по УЗЗ.

8.5.1 Общие требования к проведению аттестации по требованиям безопасности информации ИС:

Аттестация ИС должна включать проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых должно подтверждаться соответствие требованиям по защите информации Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», предъявляемым к 3-му уровню защищенности персональных данных.

Программа и методики оценки аттестационных испытаний, перечень работ, требуется провести для оценки и подтверждения выполнения предъявляемых требований по безопасности информации, перечень объектов аттестационных испытаний с указанием продолжительности работ и используемых при этом методов проверок и испытаний.

Программа аттестационных испытаний должна включать:

- проверку структуры, состава и условий эксплуатации СЗИ ИС;
- проверку правильности классификации ИС;
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации;
- проверку уровня подготовки специалистов, обеспечивающих защиту информации, и распределения ответственности должностных лиц, эксплуатирующих ИС, за выполнение требований безопасности информации;
- проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации;

- проведение испытаний ИС на соответствие требованиям по защите информации от утечки по техническим каналам;
 - проведение испытаний ИС на соответствие требованиям по защите от НСД;
-
- подготовку отчетной документации и оценку результатов испытаний аттестуемой ИС;
 - проверку комплектности документов и соответствия их содержания установленным требованиям к системе защиты информации;
 - проведение испытаний на соответствие требованиям к системе защиты информации, установленным в Описание объекта закупки (техническое задание) и нормативных документах по защите информации;
 - подготовку отчетной документации и оценку результатов аттестационных испытаний системы защиты информации.
 - оформление материалов аттестационных испытаний (протоколов испытаний и заключения по результатам аттестационных испытаний);
 - установление продолжительности работ по пунктам программы;
 - проведение контроля соответствия системы защиты информации, аттестованной ИС требованиям безопасности в процессе эксплуатации.

Методики аттестационных испытаний должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке количественных и качественных характеристик системы защиты информации, перечень требований, подлежащих проверке и условий, в которых проводится проверка, а также критерии, по которым делаются выводы о соответствии объекта проверки требованиям безопасности информации, установленных в техническом задании.

Методики испытаний должны включать:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств ИС;
- исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки и передачи информации технических средств;
- проверку состояния организации работ и выполнения организационных и технических требований по защите информации, оценку правильности классификации (уровня защищенности), оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации;
- проверку условий эксплуатации СЗИ;
- проверку выполнения функциональных требований к СЗИ;
- проверку соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверку наличия действующих сертификатов ФСТЭК России или ФСБ России в пределах их компетенции на используемые СЗИ;
- проверку программной совместимости и корректности функционирования всего комплекса используемых СВТ и с продукцией, используемой в целях защиты информации;
- проверку комплектности эксплуатационной документации на СЗИ;
- проверку реализации организационных мер;
- проверку функций НСД доступа путем соответствующих настроек и пробного запуска СЗИ и наблюдения за выполнением их функций;
- проверку СЗИ от НСД, целостности применяемых СЗИ.

На этапе аттестации ИС, Исполнителем должны быть выполнены:

- анализ структуры объекта информатизации, информационных потоков, комплекса технических средств и программного обеспечения, разработанной документации на систему защиты информации объекта;
- оценка правильности классификации объекта информатизации, выбора и применения продукции, используемой для защиты информации в целях исключения опасных технических каналов утечки информации и возможных угроз безопасности

информации, связанных с несанкционированным доступом к информации и специальным воздействием на информацию или носители информации;

- проверка наличия сертификатов соответствия на продукцию, используемую в целях защиты информации;
- проведение аттестационных испытаний в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований безопасности информации на различных этапах технологического процесса обработки;
- оформление протоколов аттестационных испытаний;
- оформление заключений по результатам аттестационных испытаний.

При проведении аттестационных испытаний Исполнителем должны применяться следующие методы, проверки и испытания:

- экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации объекта информатизации установленным требованиям безопасности информации на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств;
- проверку соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверку СЗИ от НСД, целостности применяемых СЗИ от НСД;
- проверку программной совместимости и корректности функционирования всего комплекса используемых СВТ с продукцией, используемых в целях защиты информации;
- испытания СЗИ от НСД путем осуществления попыток НСД к тестовой защищаемой информации.

Экспертно-документальный метод должен предусматривать проверку соответствия СЗИ, обрабатываемых в ИС, на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также на основании соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств.

По результатам аттестационных испытаний Исполнитель подготавливает отчетную документацию (в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 27 февраля 2026 г. № 60 "О внесении изменений в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77):

- 1) протоколы по результатам аттестационных испытаний;
 - 2) заключения по результатам аттестационных испытаний с выводами о соответствии (или несоответствии) ИС требованиям по безопасности информации;
- оформление, регистрация и выдача аттестатов соответствия при выполнении требований по безопасности информации (требованием к выдаче Аттестата соответствия является согласованные и подписанные эксплуатационные и организационно-распорядительные документы Заказчиком).

Исполнитель обязан провести аттестацию ИС Заказчика в соответствии с согласованными с Заказчиком Программами и методиками аттестационных испытаний по требованиям безопасности и согласно национальных стандартов, а также методических документов, разработанных и утвержденных ФСТЭК России.

Места размещения ИС Заказчика могут быть изменены.

Точные места расположения ИС подлежащих аттестации по требованиям безопасности информации Заказчик обязан согласовать с Исполнителем.

9.Гарантийные обязательства

9.1 Требования к гарантийному обязательству

Срок гарантии, предоставляемой Исполнителем на поставленные СЗИ должен быть не менее срока гарантии, предоставляемой правообладателем или производителем СЗИ.

Под сроком предоставления гарантии Аттестации по требованиям безопасности информации информационных систем Заказчика понимается период времени, начинающийся с момента подписания Сторонами Акта сдачи-приемки выполненных работ и заканчивающийся по истечении 36 (Тридцати шести) месяцев.

Техническое регулирование в отношении оказываемых услуг должно осуществляться в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

Неотъемлемой частью настоящего Описания объекта закупки (технического задания) являются приложения № 1-4, а именно⁷:

- Приложение № 1 – «Перечень услуг и порядок сдачи приемки результатов их оказания».
- Приложение № 2 – «Технические требования к организации АРМ рабочего места информационной системы персональных данных».
- Приложение № 3 – «Наименование муниципального общеобразовательного учреждения и место нахождения».
- Приложение № 4 – «Название информационной системы».

Заказчик:

_____/_____/

Электронная подпись должностного лица
с правом подписи контракта

Исполнитель:

_____/_____/

Электронная подпись должностного лица
с правом подписи контракта

⁷ Прилагаются отдельным файлом (по каждому Заказчику)