Общество с ограниченной ответственностью
«Теплогенерирующий комплекс»

ОГРН 1075503004587, ИНН 5503109356, КПП 550301001
Юр. адрес: ул. Чапаева, 71, г.Омск, 644099, тел. (3812) 65-02-27, факс (3812) 65-34-36
e-mail: tgk.info@mail.ru; www.energocomplex55.ru

«21» 11 2022 года № Т-22-1400

Руководителю организации

О предоставлении коммерческих предложений

Запрос

В соответствии с Федеральным законом от 18.07.2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и Положением о закупках товаров, работ, услуг для нужд ООО «ТГКом» (Протокол от «16» сентября 2022 г. №02/22) ООО «ТГКом» планирует проведение упрощённой закупки с целью заключения **договора на оказание услуг по установке и настройки средств защиты информации, предоставление неисключительного права на использование программы (Средства защиты информации Secret Net Studio 8)** в соответствии с техническим зданием.

Начальная (максимальная) цена договора (далее - НМЦД) – **132 442,00 руб., в т.ч. НДС**.

Прошу Вас подготовить и выслать коммерческое предложение не позднее **17-00 (омского времени) «24» ноября 2022 года** на эл. почту: **energocomplex55@mail.ru.**

Предложение должно содержать информацию о цене, сроке действия предлагаемой цены, сканированные копий документов согласно Приложению № 2.

Предложения участников предоставляются с НДС. Если участник не является плательщиком НДС, то предложения предоставляются, без НДС.

Подведение итогов состоится **«25» ноября 2022 года**. Победителем упрощённой закупки признается Участник, предложивший наименьшую цену. Если в нескольких коммерческих предложениях содержится одинаковая цена, заказчик вправе признать победителем участника, коммерческое предложение, которого поступило ранее коммерческих предложений других участников.

Заказчик вправе в любое время до подписания договора отказаться от проведения упрощённой закупки.

Приложение:

1. Техническое задание – на 21 л.
2. Перечень копий документов – на 1 л.
3. Анкета участника – на 1 л.

Генеральный директор А.Ю. Лунев

К.В. Заславская,
65-98-55

Приложение №2

Перечень копий документов

1. Учредительные документы: Устав, Положение, Свидетельство о регистрации предпринимателя без образования юридического лица;
2. Свидетельство о внесении записи в Единый государственный реестр юридических лиц либо Лист записи ЕГРЮЛ, ЕГРИП;
3. Свидетельство о постановке на учёт в налоговом органе и присвоении ИНН;
4. Копия паспорта гражданина РФ, иной документ удостоверяющий личность (в случае, если договор заключается с физ. лицом);
5. Документы, подтверждающие полномочия лица, заключающего договор (решение общего собрания участников общества об избрании исполнительного органа (для ООО), решение Общего собрания акционеров либо Совета директоров об избрании исполнительного органа (для акционерного общества), приказ о назначении, доверенность на право заключения договора с образцом подписи уполномоченного лица, заверенная печатью предприятия (ИП) в случае наличия печати.
6. Копия годовой бухгалтерской (финансовой) отчётности (бухгалтерский баланс, отчёт о финансовых результатах) за **предшествующий календарный год**, с документом, подтверждающим сдачу бухгалтерской отчётности в ФНС. (Если Участник является ИП или организацией на УСН, необходимо предоставить Декларацию по УСН).
7. Решение (согласия) Общего собрания участников (единственного участника) либо Собрания акционеров, либо Совета директоров о совершении крупной сделки (в случае если совершаемая сделка является для контрагента крупной сделкой либо сделкой с заинтересованностью) либо иного третьего лица, в предусмотренных законом случаях.
8. Выписка из ЕГРЮЛ, ЕГРИП (по состоянию на дату не позднее одного месяца до заключения договора)
9. Копии сведений о среднесписочной численности работников / расчета по страховым взносам (по форме, утвержденной приказом ФНС России) за два предшествующих календарных года (для предприятий, осуществляющих деятельность в течение менее двух календарных лет, – за период, прошедший со дня их государственной регистрации).
10. Анкета участника по форме Приложения № 3.

Приложение №3

Анкета Участника

Наименование	Сведения об Участнике
1. Наименование организации (полное)	
2. Наименование организации (сокращенное)	
3. Форма собственности	
4. Адрес юридический	
5. Адрес фактический	
6. Должность руководителя	
7. ФИО руководителя	
8. Телефон руководителя	
9. Факс	
10. Электронная почта	
11. Ответственное лицо	
12. Телефон ответственного лица	
13. ОГРН	
14. ИНН/КПП	
15. ОКПО	
16. ОКОПФ	
17. ОКТМО	
18. Дата постановки на учет в налоговом органе	
19. Номер расчетного счета	
20. Номер корреспондентского счета	
21. БИК	
22. Полное наименование банка	
23. ФИО уполномоченного лица на подписание договора	
24. Должность уполномоченного лица (при наличии)	
25. Номер, дата доверенности	

(должность, ФИО) (подпись, М.П.)

Приложение №1

Техническое задание

на оказание услуг по установке и настройки средств защиты информации, предоставление неисключительного права на использование программы (Средства защиты информации Secret Net Studio 8), проведение комплекса работ по аттестации информационной системы Государственная информационная система Омской области «Тариф» Общества с ограниченной ответственностью «Теплогенерирующий комплекс»

Общие сведения

1.1 Полное наименование системы и ее условное обозначение

Полное наименование: Государственная информационная система Омской области «Тариф» Общества с ограниченной ответственностью «Теплогенерирующий комплекс».

Условное обозначение: ГИС «Тариф»

1.2 Заказчик

Общество с ограниченной ответственностью «Теплогенерирующий комплекс» (далее – ООО «ТГКом»).

Адрес: 644099, Омская обл., г. Омск, ул. Чапаева, 71.

1.3 Основание проведения работы

Основаниями проведения настоящей работы являются:

- требования законодательства Российской Федерации в области защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
- требования законодательства Российской Федерации в области защиты персональных данных;
- наличие в Обществе с ограниченной ответственностью «Теплогенерирующий комплекс» абонентского пункта, подключенного к ГИС «Тариф».

1.4 Документы, на основании которых проводятся работы

Работы должны осуществляться на основании и в соответствии с требованиями нормативных актов РФ:

- Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006г. №152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 11 февраля 2013г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСБ России от 10 июля 2014г. №378 «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»;

– «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», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015);

– Приказ ФСТЭК России от 29 апреля 2021 №77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

– Методический документ «Меры защиты информации в государственных информационных системах» утвержден ФСТЭК России 11 февраля 2014;

– «Методика оценки угроз безопасности информации», утвержденная ФСТЭК России 5 февраля 2021г.;

– ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения;

– ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний;

– Иные нормативно-правовые, организационно-распорядительные и нормативно-технические документы Российской Федерации в области обеспечения безопасности персональных данных, в том числе утвержденные ФСТЭК России, ФСБ России.

1.5 Срок выполнения работ

Начало выполнения работ – с момента заключения Договора.

Предельный срок выполнения работ – 90 календарных дней.

Календарные сроки выполнения этапов, а также порядок их документального оформления определяются Договором.

Заявки, не обеспечивающие выполнение работ в указанные сроки, к участию в открытом аукционе в электронной форме не допускаются.

1.6 Источник финансирования

Источник финансирования – средства Заказчика.

1.7 Порядок оформления и предъявления Заказчику результатов работ

Разработка итоговой документации должна вестись в соответствии с ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Передача документации для согласования, через открытые каналы связи без шифрования – запрещена.

Шифрование должно выполняться с помощью, предоставленного Исполнителем, веб-сервиса, который позволяет выполнять на компьютере пользователя следующие операции с электронными документами:

- зашифровать и расшифровать документ;
- шифрование и расшифрование отдельных файлов и архивов данных;
- шифрование без ограничения размера шифруемых данных;
- шифрование данных по алгоритму ГОСТ 34.12-2018, ГОСТ 34.13-2018;
- просмотр списка ключевых контейнеров;
- сохранение и отправка из сервиса по электронной почте пакета документов одним архивом, содержащим зашифрованный документ и инструкцию по расшифрованию документа;
- поддержка криптопровайдеров (CSP) «КриптоПро CSP», «ViPNet CSP»;
- поддержка ключевых носителей Rutoken и eToken, eSmart, JaCarta.

Веб-сервис должен корректно функционировать на операционных Windows с установленным криптопровайдером (CSP).

Результаты оказания работ передаются комплектом документов, который должен быть передан на бумажном носителе и в электронном виде (форматы *.docx, *.pdf, *.vsd) Заказчику. Установочные комплекты и лицензии, поставляемых средств защиты информации должны быть переданы вместе с комплектом документов.

2 Назначение и цели проведения работ

2.1 Назначение проведения работ

Задачей создания системы защиты информации (далее – СиЗИ) и проведения комплекса организационных и технических мероприятий (аттестационных испытаний) информационных систем Заказчика (далее – ИС) является поддержка высокой доступности технических, программных и информационных ресурсов ИС пользователям ИС в соответствии с предоставленными им правами и полномочиями и проведение оценки соответствия обеспечения защиты персональных данных (далее – ПДн), обрабатываемых в ИС от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

2.2 Цели проведения работ

Основными целями проведения настоящих работ являются:

- защита ПДн, обрабатываемых в ИС, от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;
- защита ПДн, передаваемых по открытым каналам связи, от утечки, искажения и подмены авторства сообщения;
- обнаружение атак и предотвращение инцидентов в области информационной безопасности;
- определение соответствия ИС требованиям положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты ПДн.

2.3 Площадки проведения работ

Перечень площадок проведения работ перечислен в таблице 2.1.

Таблица 2.1

№ п/п	Адрес площадки	Наименование площадки
1	644099, Омская обл., г Омск, ул. Чапаева, 71	ООО «ТГКом»

3 Общая характеристика информационных систем

3.1 Описание информационной системы

В целях развития ***регионального сегмента*** федеральной государственной информационной системы «Единая информационно-аналитическая система «ФСТ России - РЭК - субъекты регулирования» в феврале 2015 года внедрена ***государственная информационная система Омской области «Тариф»***.

Согласно приказу Региональную энергетическую комиссию Омской области (далее – Комиссия) от 10 февраля 2015 года №12/6 «О внедрении государственной информационной системы Омской области «Тариф» юридические лица и индивидуальные предприниматели, осуществляющие регулируемые виды деятельности, а также органы местного самоуправления предоставляют в РЭК Омской области информацию по устанавливаемым Комиссией электронным формам отчётности по ГИС «Тариф».

3.2 Информация, обрабатываемая в информационной системе

Юридические лица и индивидуальные предприниматели, осуществляющие регулируемые виды деятельности, а также органы местного самоуправления предоставляют в Комиссию информацию по вопросам установления, изменения и применения цен (тарифов), регулируемых Комиссией, определения и применения нерегулируемых цен на электрическую энергию, раскрытия информации, платы граждан за коммунальные услуги, а также для целей функционирования ГИС "Тариф" по устанавливаемым Комиссией электронным формам отчетности (далее - шаблон) по ГИС "Тариф".

Комиссия запрашивает шаблоны путем направления по "ГИС "Тариф" запросов, состоящих из файла шаблона и сопроводительного письма.

3.3 Методы управления доступа

Во внутреннем контуре ГИС «Тариф» реализован дискреционный метод разграничения доступа к ресурсам.

Режим доступа субъектов доступа к объектам доступа в ГИС «Тариф» – многопользовательский, с различными правами доступа.

4 Требования к системе защиты информации

4.1 Требования к системе в целом

СиЗИ Заказчика в целом должна быть совместима с используемыми программными и техническими решениями и соответствовать требованиям руководящих и нормативных документов в области защиты информационных систем персональных данных.

4.1.1. Требования к совместимости

Применяемые средства защиты информации (далее – СЗИ) для создания СиЗИ должны быть совместимы с сетевой, канальной инфраструктурой ИС, используемым оборудованием и программным обеспечением и не накладывать ограничений на функционирование ИС.

4.1.2. Требования по надежности

СЗИ должны иметь возможность осуществления резервирования настроек, резервного копирования файлов конфигураций и восстановления в случаях сбоев.

4.1.3. Требования по стандартизации, унификации и сертификации

Разработка СиЗИ должна проводиться с соблюдением действующих государственных стандартов в соответствии с областью их распространения.

Комплексная защита информации и информационных ресурсов должна обеспечиваться с помощью общесистемных и специализированных, программных и аппаратно-программных СЗИ, сертифицированных ФСТЭК России и ФСБ России, включая средства криптографической защиты информации (далее – СКЗИ). Используемые СЗИ должны иметь соответствующие сертификаты ФСТЭК России и/или ФСБ России.

4.1.4. Требования по патентной чистоте

Программные и аппаратно-программные СЗИ, приобретаемые у сторонних организаций, должны сопровождаться документацией, подтверждающей правомочность этих организаций поставлять данную продукцию.

4.1.5. Требования к безопасности

Сведения, полученные Исполнителем при выполнении работ и не указанные в настоящем техническом задании, являются информацией ограниченного доступа.

Исполнитель работ обязуется:

- не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации ограниченного доступа;
- не передавать информацию ограниченного доступа о настоящих работах и полученных результатах третьей стороне;
- не осуществлять несанкционированный доступ к информационным ресурсам;

– не проводить незаконное копирование информации, циркулирующей или хранящейся в ИС;

– не предпринимать манипулирование информацией, циркулирующей или хранящейся в ИС (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

– не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

– не внедрять в ИС программы-вирусы (загрузочные, файловые и др.);

– не устанавливать программные и аппаратные закладные устройства в технические средства ИС;

– не устанавливать в технические средства ИС программное обеспечение, зараженное вирусами;

– не осуществлять передачу материалов работ по создаваемой СиЗИ на объекте сторонним организациям, а также публикацию их в открытой печати без разрешения Заказчика.

Нарушение настоящих требований влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.1.6. Перспективы развития, модернизации системы

Проектируемая и создаваемая СиЗИ должна быть масштабируемая и обеспечивать подключение новых участников безопасного информационного обмена без ухудшения функционирования (снижения степени защищённости) ИС.

Должна быть предусмотрена возможность дальнейшего развития ИС в следующих направлениях:

- расширение состава прикладных функций ИС;
- интеграция ИС с другими ИС и ресурсами.

4.1.7. Требования к эргономике и технической эстетике

Разрабатываемая СиЗИ не должна вносить значительных задержек в работу пользователей ИС.

Программные СЗИ должны обладать интуитивно-понятным интерфейсом управления, иметь документацию на русском языке. Регламент работы пользователей в части СЗИ, а также порядок реагирования на события информационной безопасности должны быть описаны в эксплуатационной документации.

4.1.8. Требования к регламенту обслуживания

Регламентные проверки технических СЗИ должны проводится в соответствии с требованиями производителя, указанными в эксплуатационной документации к техническим средствам.

4.2 Требования руководящих документов

В СиЗИ должны быть реализованы меры защиты информации, установленные для соответствующего уровня защищенности ПДн, обрабатываемых в ИС, в соответствии с требованиями приказа ФСТЭК от 11 февраля 2013г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В СиЗИ должны быть реализованы организационные и технические меры по обеспечению безопасности ПДн необходимые для выполнения установленных приказом ФСБ России от 10 июля 2014 г. № 378 «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» требований для соответствующего уровня защищенности ПДн, обрабатываемых в ИС.

4.3 Требования к видам обеспечения

4.3.1. Требования к программному и техническому обеспечению

Меры по обеспечению безопасности реализуются в том числе посредством применения в ИС СЗИ. Технические характеристики поставляемых СЗИ, приведены в таблице 4.1.

Таблица 4.1

№ п/п	Наименование	Характеристики
1.	Модуль защиты от несанкционированного доступа «Комплексного программного средства защиты информации для конечных точек»	***Должно осуществлять:*** защиту серверов и рабочих станций от несанкционированного доступа; контроль входа пользователей в систему, в том числе и с использованием дополнительных аппаратных средств защиты; разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации; разграничение доступа пользователей к информации; контроль утечек информации; регистрацию событий безопасности и аудит. ***Требования к функциональности:*** Средство должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин. Средство должно выполнять следующие функции по защите информации: Контроль входа пользователей в систему и работа пользователей в системе:

№ п/п	Наименование	Характеристики
		◦ проверка пароля пользователя при входе в систему; ◦ поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭП, Рутокен Lite, Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ; ◦ 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. 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. Полномочное (мандатное) управление доступом: ◦ 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. Контроль вывода конфиденциальных данных на печать: ◦ возможность ограничить перечень мандатных меток информации для печати на заданном принтере; ◦ теневое копирование информации, выводимой на печать; ◦ 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. Контроль аппаратной конфигурации компьютера и подключаемых устройств: ◦ Должны контролироваться следующие устройства: ▪ последовательные и параллельные порты; ▪ локальные устройства; ▪ сменные, физические и оптические диски;

№ п/п	Наименование	Характеристики
		▪ 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. Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации. 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 ЭП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭП. 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. Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. Функциональный контроль ключевых компонентов системы.

№ п/п	Наименование	Характеристики
		Регистрация событий безопасности в журнале. - Должна быть возможность формирования отчетов по результатам аудита. - Должна быть возможность поиска и фильтрации при работе с данными аудита. Получение отчета по параметрам системы защиты. ***Требования к операционной платформе и аппаратной части:*** Средство должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы): - Windows 10; - Windows 8/8.1; - Windows 7 SP1; - Windows Server 2012/2012 R2; - Windows Server 2008 SP2/2008 R2 SP1. Средство должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix. Средство должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMware ESX(i) и Microsoft Hyper-V. Средство с централизованным управлением должно функционировать совместно с Microsoft Active Directory; Средство должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. ***Требования к сертификации:*** Средство должно иметь сертификат соответствия ФСТЭК России, который подтверждает соответствие требованиям руководящих документов по 4 уровню доверия, 5 классу защищенности СВТ, 4 классу защиты СКН (ИТ.СКН.П4.ПЗ), Средство может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно
2.	Средство антивирусной защиты	***Требуемые характеристики:*** резидентный антивирусный мониторинг; программные средства защиты от сетевых атак; эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; обнаружение скрытых процессов; антивирусное сканирование по команде пользователя или администратора и по расписанию; антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.; антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем; защиту электронной корреспонденции, как от вредоносных программ, так и от спама. Проверку трафика на следующих протоколах: IMAP, SMTP, POP3, независимо от используемого почтового клиента; NNTP (только проверка на вирусы), независимо от почтового клиента; независимо от типа протокола (в том числе MAPI, HTTP) в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!; защиту HTTP-трафика - проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP, FTP; проверку скриптов - проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете; запуск задач по расписанию и/или сразу после загрузки операционной системы; защиту от еще не известных вредоносных программ на основе анализа их поведения и контроле изменений системного реестра, с возможностью

№ п/п	Наименование	Характеристики
		автоматического восстановления изменённых вредоносной программой значений системного реестра; защиту от программ-маскировщиков, программ автодозвона на платные сайты, блокировку баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц и распознавание фишинг-сайтов; осуществлять контроль работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных. ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; настройки проверки критических областей компьютера в качестве отдельной задачи; технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей. ***Требования к поставке:*** Поставка CAB должна включать в себя: фирменную коробку; CD\DVD-диск в фирменном конверте, на котором записаны дистрибутивы сертифицированных ФСТЭК России продуктов; заверенные копии сертификатов ФСТЭК России; формуляр, в котором содержатся эталонные значения контрольных сумм сертифицированных ФСТЭК России продуктов CAB. ***Требования к сертификации и применению в информационных системах:*** Средство антивирусной защиты должно иметь сертификат соответствия ФСТЭК России на соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВ3.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВ3.Г2.ПЗ» (ФСТЭК России, 2012)
3.	Средство анализа защищенности	***Требования к функционалу:*** Средство анализа защищенности должно обеспечивать: Обеспечение загрузки доверенной среды с любого компьютера (по технологии Live- CD/Live-flash) с автоматическим определением сетевого оборудования, подключенного к вычислительной сети; Поиск остаточной информации на накопителях, подключенных к узлам сети (поддерживаются различные кодировки); Локальный (на любом ПК) и сетевой аудит парольной защиты; Инвентаризация (фиксация) ресурсов компьютерной сети (узлов, портов, сервисов); Выявление (сканирование) уязвимостей сетевых сервисов; Проверка возможности осуществления атак на отказ в обслуживании и подмены адреса; Анализ сетевого трафика (в т.ч. в коммутируемых сетях, физически разделенных) Аудит парольной информации для множества протоколов; Гарантированная очистка информации на носителях; Контрольное суммирование файлов, папок, а также посекторное суммирование для машинных носителей информации; Аудит установленных обновлений ОС Windows; Анализа защищенности беспроводных (Wi-Fi) сетей. ***Требования к сертификации:***

№ п/п	Наименование	Характеристики
		Программный комплекс должен иметь действующий сертификат ФСТЭК России на соответствие требованиям руководящего документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) – по 4 уровню доверия и технических условий

4.3.2. Требования к метрологическому обеспечению

Тестирование (диагностика) СиЗИ должно проводиться посредством специальной контрольной аппаратуры, тестовых средств и специализированного программного (аппаратно-программного) обеспечения, обладающего соответствующими сертификатами ФСТЭК России, подтверждающими соответствие используемых программных (аппаратно-программных) средств требованиям, предъявляемым к средствам контроля защищённости информации.

4.3.3. Требования к методическому обеспечению

В целях формирования и закрепления организационных мер защиты ПДн, как неотъемлемых мер обеспечения безопасности ПДн, необходимо актуализировать комплект проектов организационно-распорядительных документов.

Комплект организационно-распорядительных документов определен в таблице 4.2.

Таблица 4.2

№ п/п	Наименование документа
1.	Приказ о создании комиссии по защите информации ограниченного доступа
2.	Акт определения класса защищенности информационной системы
3.	Акт определения уровня защищенности персональных данных при их обработке в информационной системе
4.	Приказ о защите информации (назначение ответственных лиц, определение границ контролируемой зоны, определение списка допущенных лиц к обработке информации ограниченного доступа)
5.	Инструкция ответственного за организацию обработки персональных данных
6.	Инструкция ответственного за защиту информации в информационных системах
7.	Инструкция администратора информационных систем
8.	Инструкция по эксплуатации информационных систем
9.	Порядок обращения со съемными машинными носителями информации ограниченного доступа
10.	Инструкция по обращению с криптографическими средствами защиты информации
11.	Перечень помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним
12.	Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа
13.	Регламент реагирования на инциденты информационной безопасности
14.	Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации
15.	Правила доступа в помещения
16.	Перечень персональных данных, обрабатываемых на объекте информатизации
17.	Приказ о хранилищах
18.	Положение о разрешительной системе доступа

№ п/п	Наименование документа
19.	Матрица доступа субъектов абонентского пункта Государственной информационной системы Омской области «Тариф»
20.	Журнал учета съемных машинных носителей информации ограниченного доступа
21.	Журнал учета лиц, имеющих доступ к обработке информации ограниченного доступа
22.	Журнал учета ознакомления пользователей с правилами работы шифровальных (криптографических) средств
23.	Журнал поэкземплярного учета шифровальных (криптографических) средств защиты информации
24.	Приказ о допуске к работе со средствами криптографической защиты информации
25.	Журнал учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей от хранилищ, личных печатей от хранилищ
26.	Положение об обеспечении безопасности информации ограниченного доступа
27.	Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации
28.	Приказ о проведении испытаний системы защиты информации
29.	План мероприятий по защите информации в соответствие с требованиями законодательства в области информации ограниченного доступа

4.3.4. Требования к предоставляемым материалам (документам)

Разработка документации должна вестись в соответствии с ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Подготавливаемая в рамках оказания услуг документация должна соответствовать требованиям следующих профильных стандартов на разработку технической документации ИС:

- ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению»;
- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
- ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения»;
- ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
- ГОСТ 2.105-95 «Единая система конструкторской документации. Общие требования к текстовым документам»;

- ГОСТ 2.106-96 «Единая система конструкторской документации. Текстовые документы».

5 Состав и содержание работ

Исполнитель должен выполнить работы в порядке и объеме, представленном в таблице 5.1.

Таблица 5.1

№ п/п	Стадии	Этапы работ	Разрабатываемая документация
1	Формирование требований к СиЗИ АП ГИС «Тариф»	– Обследование объекта. – Формирование требований пользователя к СиЗИ АП ГИС «Тариф». – Оформление описания ИС.	Описание ИС.
2	Разработка концепции СиЗИ АП ГИС «Тариф»	– Изучение объекта. – Разработка вариантов концепции СиЗИ АП ГИС «Тариф», удовлетворяющей требованиям пользователя. – Оформление описания ИС (дополнение документа из п.1).	– Модель угроз безопасности информации; – Частная модель угроз безопасности персональных данных, обрабатываемых в информационной системе и защищаемых с использованием сертифицированных средств криптографической защиты информации.
3	Техническое задание	Разработка и утверждение технического задания на создание СиЗИ АП ГИС «Тариф».	Техническое задание на создание СиЗИ.
5	Технический проект	– Разработка проектных решений по СЗИ ИС и ее частям. – Разработка документации на СиЗИ АП ГИС «Тариф» и ее части. – Разработка и оформление документации на поставку изделий для комплектования СиЗИ АП ГИС «Тариф» и (или) технических требований (технических заданий) на их разработку.	Технический проект на создание СиЗИ.
6	Рабочая документация	– Разработка рабочей документации на СиЗИ АП ГИС «Тариф» и ее части.	– Приказ о создании комиссии по защите информации ограниченного доступа; – Приказ о защите информации (назначение ответственных лиц, определение границ контролируемой зоны, определение списка допущенных лиц к обработке информации ограниченного доступа); – Инструкция ответственного за организацию обработки персональных данных; – Инструкция ответственного за защиту информации в ИС; – Инструкция администратора ИС; – Инструкция по эксплуатации ИС; – Порядок обращения со съемными машинными носителями информации ограниченного доступа; – Инструкция по обращению с криптографическими средствами защиты информации; – Перечень помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним; – Регламент проведения внутреннего

№ п/п	Стадии	Этапы работ	Разрабатываемая документация
			контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа; – Регламент реагирования на инциденты информационной безопасности; – Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации; – Правила доступа в помещения.
7	Ввод в действие	– Подготовка объекта к вводу СиЗИ АП ГИС «Тариф» в действие. – Подготовка персонала. – Комплектация СиЗИ поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями). – Пусконаладочные работы. – Проведение предварительных испытаний. – Проведение опытной эксплуатации. – Проведение приемочных испытаний. – Проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СиЗИ требованиям по безопасности информации.	– Акт установки и настройки СЗИ; – Технический паспорт ИС; – Программа и методика испытаний СиЗИ; – Акт приемки в опытную эксплуатацию СиЗИ; – Акт о завершении опытной эксплуатации СиЗИ; – Акт приемки в постоянную эксплуатацию СиЗИ; – Протокол испытаний; – Программа и методика аттестационных испытаний; – Протокол аттестационных испытаний; – Заключение о соответствии ИС требованиям о защите информации; – Аттестат соответствия ИС требованиям о защите информации.
8	Сопровождение АП ГИС «Тариф»	– Выполнение работ в соответствии с гарантийными обязательствами. – Послегарантийное обслуживание.	План мероприятий по защите информации в соответствие с требованиями законодательства в области информации ограниченного доступа.

6 Порядок проведения аттестационных испытаний

Аттестация ИС должна быть проведена Исполнителем в соответствии с ГОСТ РО 0043–003–2012, ГОСТ РО 0043–004–2013 и включать проведение комплекса организационных и технических мероприятий (аттестационных испытаний) по требованиям безопасности информации путем:

- проведения анализа и оценки исходных данных об аттестуемом объекте информатизации (полное и точное наименование объекта информатизации и его назначение, сведения об организационно-режимных мерах защиты, принятых на объекте информатизации, перечень сертифицированной продукции, используемой в целях защиты информации, наличие и характер взаимодействия с другими объектами информатизации), анализа организационной структуры объекта информатизации (проверку условий размещения, монтажа и эксплуатации технических средств, изучение технологического процесса обработки, передачи и хранения информации, анализ информационных потоков, определение состава использованных для обработки, передачи и хранения информации технических средств);
- проведения комплексных испытаний ИС в соответствии с разработанной программой и методиками аттестационных испытаний;
- оформления отчетной документации – протоколов аттестационных испытаний ИС, заключений по результатам аттестационных испытаний на соответствие ИС требованиям безопасности информации.

При наличии положительного заключения по результатам аттестационных испытаний Исполнитель должен оформить аттестат соответствия требованиям по безопасности информации в ИС.

В период действия Аттестата, подтверждающего наличие условий по соблюдению конфиденциальности информации, являющегося результатом оказания услуг по аттестации на соответствие требованиям по защите информации, Заказчик обязуется организовывать проведение периодического контроля защищённости согласно программе и методикам аттестационных испытаний объекта информатизации, а также в соответствии с требованиями нормативно-правовых актов в области защиты информации для соответствующего типа объекта информатизации.

7 Порядок оказания услуг

Перед проведением работ Исполнителем должны быть определены условия соблюдения конфиденциальности при выполнении работ.

Все работы необходимо проводить в согласованное со специалистами Заказчика время, не нарушая основную рабочую деятельность.

Исполнитель обязуется оказать работы своими силами и средствами, с помощью своего оборудования и материалов. Исполнитель может привлекать соисполнителей только по согласованию с Заказчиком.

8 Требования к сопровождению

Исполнитель должен гарантировать качество и надежность функционирования программных средств системы в течение гарантийного срока.

В течение 12 месяцев после выполнения работ Исполнитель предоставляет гарантийное сопровождение в виде консультации технических специалистов Заказчика с использованием всех доступных средств связи (телефон, электронная почта, электронные средства on-line общения и т.д.). В случае наличия замечаний ФСТЭК России к подготовленному Исполнителем пакету документов по результатам создания СиЗИ, Исполнитель безвозмездно устраняет указанные замечания при условии отсутствия изменений в составе системы защиты ИС Заказчика.

Время работы линии технической поддержки Исполнителя – с 9:00 до 18:00 местного времени в рабочие дни.

9 Спецификация поставляемых средств защиты информации и перечня работ

№ п/п	Наименование, виды и перечень (содержание и объемы) услуг	Объем поставки	
		Единицы измерения	Количество
1	Поставка средств защиты информации		
1.1.	Право на использование модуля защиты от несанкционированного доступа «Комплексного программного средства защиты информации для конечных точек»	шт.	1
1.2.	Сертифицированный дистрибутив «Комплексного программное средство защиты информации для конечных точек»	шт.	1
1.3.	Право на использование «Средство анализа защищенности»	шт.	1
1.4.	Сертифицированный дистрибутив «Средство анализа защищенности»	шт.	1
1.5.	Сертифицированный дистрибутив «Средство антивирусной защиты»	шт.	1
2	Установка и настройка средств защиты информации	Услуга	1
3	Подготовка документации, регламентирующей порядок и правила обработки персональных данных, а также обеспечение безопасности персональных данных в информационных системах.	Услуга	1
4	Разработка «Модели угроз» и технической документации	Услуга	1
5	Аттестация объекта информатизации по требованиям безопасности информации (1 АРМ, 1 ГИС)	Услуга	1

Перечень принятых сокращений и обозначений

АП – абонентский пункт

ГИС «Тариф» – Государственная информационная система Омской области «Тариф»

ИС – информационная система

ПДн – персональные данные

САВ – средство антивирусной защиты

СиЗИ – система защиты информации

СЗИ – средство защиты информации

ФСБ России – Федеральная служба безопасности

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

Начальник отдела ИТО О.В. Пасевин