**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на** **оказание услуг по** **проведению аудита, разработке проектной документации, приведению в соответствие требованиям безопасности информации и аттестации информационной системы «Информационная инфраструктура публичного облака Т1Клауд»**

1. Общие сведения

* 1. Полное наименование проекта и его условное обозначение

Полное наименование проекта – «оказание услуг по проведению аудита, разработке проектной документации, приведению в соответствие требованиям безопасности информации и аттестации информационной системы «Информационная инфраструктура публичного облака Т1Клауд» (далее – ИС «Т1Клауд», ИС Заказчика).

* 1. Границы работ

Услуги оказываются в отношении следующих центров обработки данных (далее – ЦОД) и информационных систем:

* ЦОД «РТК Медведково» по адресу: г. Москва, ул. Чермянская, вл. 4;
* ЦОД «IXcellerate» по адресу: Москва, Алтуфьевское ш., д. 33Г;
* ЦОД «DataPro» по адресу: г. Москва, Авиамоторная ул., д. 69;
* ЦОД «РТК Остаповский» по адресу: г. Москва, Остаповский проезд, д. 22, стр. 4.
  1. Плановые сроки начала и окончания работ

Начало выполнения работ: с даты заключения договора и предоставления необходимой информации Заказчиком.

Окончание выполнения работ: не более 45 (сорок пять) рабочих дней с даты предоставления необходимой информации Заказчиком.

Период согласования Заказчиком отчетных документов по результатам работ не входит в сроки выполнения работ.

* 1. Порядок оформления и предъявления Заказчику результатов работ

Документы должны представляться электронных и на бумажном носителях (в случае такого запроса со стороны Заказчика), документы должны быть выполнены на русском языке. Электронное представление документов должно соответствовать формату редакторов Microsoft Word, Microsoft Visio (\*.docx, \*.vsd).

Вся разработанная документация должна быть согласована с уполномоченными представителями Заказчика.

* 1. Перечень документов, на основании которых ведется работа

При проведении работ необходимо учитывать положения следующих документов (с изменениями и дополнениями):

* Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
* Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»;
* Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – приказ ФСТЭК России № 239);
* Приказ 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» (далее – приказ ФСТЭК России № 21);
* Приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (далее – приказ ФСТЭК России № 235);
* Приказ ФСТЭК России от 2 июня 2020 года № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;
* Приказ ФСБ России от 10 июля 2014 года № 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»;
* Приказ ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
* Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021 года;
* ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».
* ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».
* ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения»;
* ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
* ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
* Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (далее – РД АС).

1. НАЗНАЧЕНИЕ И ЦЕЛИ РАБОТ
   1. Назначение работ

Основные задачи, решаемые в ходе оказания услуг:

* Оценка соответствия требованиям ГОСТ Р 57580.1-2017 ИС «Т1Клауд» по первому уровню защиты информации (усиленный);
* Разработка организационно-распорядительной и технической документации, необходимых для выполнения требований по информационной безопасности, установленных приказом ФСТЭК России № 235, приказом ФСТЭК России № 239 по 1-ой категории значимости, приказом ФСТЭК России № 21 по 1-му уровню защищенности;
* Аттестация ИС «Т1Клауд» по 1-ой категории значимости в соответствии с приказом ФСТЭК России № 239, по 1-му уровню защищенности в соответствии с приказом ФСТЭК России № 21, по РД АС (класс 1Г).
  1. Цели проведения работ

Цели проведения работ:

* оценка соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017;
* получение объективных свидетельств выполнения требований по обеспечению реализации первого уровня защиты информации, определенного национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 для объектов информационной инфраструктуры Заказчика;
* формирование перечня рекомендаций по приведению уровня обеспечения защиты информации Заказчика к заданному Заказчиком уровню соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017.
* получение объективных свидетельств (аттестата соответствия) выполнения требований приказа ФСТЭК России № 239 по обеспечению 1-ой категории значимости ИС Заказчика;
* получение объективных свидетельств (аттестата соответствия) выполнения требований приказа ФСТЭК России № 21 по обеспечению 1-ого уровня защищенности ИС Заказчика;
* получение объективных свидетельств (аттестата соответствия) выполнения требований РД АС по обеспечению класса 1Г ИС Заказчика.
  1. Задачи, решаемые в ходе выполнения работ

Для достижения поставленных целей должны быть решены следующие задачи:

* Определение негативных последствий, которые могут наступить от реализации угроз безопасности информации;
* Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
* Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
* Оценка способов реализации угроз безопасности информации;
* Оценка возможности реализации угроз безопасности информации и определение актуальности угроз безопасности информации;
* Оценка сценариев реализации угроз безопасности информации в системе и сети.
* Разработка организационно-распорядительной документации, обеспечивающей регламент обработки конфиденциальной информации в организации;
* Разработка эксплуатационной документации;
* Экспертиза соответствия ИС первому уровню защищенности персональных данных, обрабатываемых в информационных системах персональных данных (УЗ-1), приведение с участием Заказчика указанной ИС в соответствие указанному уровню защищенности;
* Экспертиза соответствия ИС первой категории значимости в части реализации мер по обеспечению безопасности, приведение с участием Заказчика указанной ИС в соответствие указанной категории значимости;
* Экспертиза соответствия ИС требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утвержден председателем Гостехкомиссии России (ФСТЭК России) 30 марта 1992 г.) по уровню **1Г**;
* Разработка Программы и методик аттестационных испытаний ИС и испытаний средств защиты информации, применяемых в них;
* Проведение испытаний средств защиты информации, применяемых в ИС, аттестационных испытаний указанной ИС и разработка протоколов испытаний указанных средств защиты информации;
* Разработка заключения по результатам аттестационных испытаний;
* Выдача аттестата соответствия (в случае положительного заключения по результатам аттестационных испытаний);
* Выдача рекомендаций по приведению ИС в соответствие первому уровню защищенности персональных данных и первой категории значимости, обрабатываемых в информационных системах (в случае отрицательного заключения по результатам аттестационных испытаний);
* Оценка соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 (далее – Оценка соответствия):
* проведена предварительная оценка (аудит) текущего уровня защиты информации на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018;
* разработаны рекомендации по приведению информационной инфраструктуры Заказчика и его бизнес-процессов к необходимому уровню соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017;
* проведена итоговая оценка уровня защиты информации с выдачей заключения о соответствии заданному уровню защиты информации.

1. ТРЕБОВАНИЯ К ПРОВОДИМЫМ РАБОТАМ
   1. Работы по проведению аттестации ИС «Т1Клауд»
      1. Разработка проектной документации на систему защиту информации ИС

В рамках работ по разработке проектной документации на систему защиты информации на ИС должно проводиться:

* Разработка Модели угроз и Модели нарушителей безопасности, обрабатываемых в ИС. Разработка этих моделей осуществляется с учетом методических документов ФСТЭК России и ФСБ России.
* Определение уровней защищенности ПДн и мер обеспечения безопасности   
  для 1 категории значимости для ИС;
* Формирование требований к системе защиты;

По результатам работ должны быть предоставлены:

1. Акт классификации ИС;
2. Модель угроз и нарушителей безопасности;
3. Частное техническое задание на создание подсистемы безопасности;
4. Технический проект системы защиты информации ИС.
   * 1. Приведение в соответствие требованиям Законодательства в области информационной безопасности ИС

В рамках работ данного этапа должен быть разработан комплект организационной документации, необходимый для выполнения требований законодательства по защите, в состав которого должны в том числе войти:

1. Цели и задачи обеспечения безопасности ИС, основные угрозы безопасности информации и категории нарушителей, основные организационные и технические мероприятия по обеспечению безопасности ИС, проводимые Заказчиком, состав и структура системы безопасности и функции ее участников, порядок применения, формы оценки соответствия ИС и средств защиты информации требованиям по безопасности;
2. Планы мероприятий по обеспечению безопасности ИС, модели угроз безопасности информации в отношении ИС, порядок реализации отдельных мер по обеспечению безопасности ИС, порядок проведения испытаний или приемки средств защиты информации, порядок реагирования на компьютерные инциденты, порядок информирования и обучения работников, порядок взаимодействия подразделений (работников) ИС при решении задач обеспечения безопасности ИС, порядок взаимодействия Заказчика с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
3. Проект приказа Об организации работ по защите информации в ООО «Т1Клауд»;
4. Технический паспорт ИС;
5. Положение о порядке организации и проведении работ по защите конфиденциальной информации в ИС;
6. Матрица доступа к ИС;
7. Инструкция по антивирусному контролю в ИС;
8. Инструкция по парольной защите в ИС;
9. Инструкция администратора информационной безопасности ИС;
10. Инструкция Ответственного за защиту информации в ИС;
11. Инструкция администратора ИС;
12. Инструкция пользователя ИС;
13. Список лиц, допущенных к обработке информации конфиденциального характера, в том числе персональных данных, в ИС;
14. Регламент идентификации и аутентификации;
15. Регламент управления доступом;
16. Регламент защиты машинных носителей информации;
17. Регламент аудита безопасности;
18. Регламент антивирусной защиты;
19. Регламент контроля защищенности информации;
20. Регламент ограничения программной среды;
21. Регламент обеспечения целостности;
22. Регламент защиты технических средств и систем;
23. Регламент управления конфигурацией информационной (автоматизированной) системы;
24. Регламент защиты среды виртуализации;
25. Регламент обеспечения доступности информации;
26. Политика безопасности при использовании средств криптографической защиты информации;
27. Регламент управления обновлениями программного обеспечения;
28. Регламент реагирования на компьютерные инциденты;
29. Регламент информирования и обучения персонала;
30. Регламент предотвращения вторжений (компьютерных атак);
31. Регламент защиты информационной (автоматизированной) системы и ее компонентов;
32. Регламент планирования мероприятий по обеспечению защиты информации.

Итоговый состав и формы организационно-распорядительных документов могут быть изменены по согласованию с Заказчиком.

* + 1. Анализ защищенности ИС

Условием начала работ по данному этапу является реализованная система защиты информации в соответствии с техническим проектом.

В процессе выполнения работ по анализу защищенности ИС должно быть выполнено:

* Сбор информации о локальной сети из источников, доступных потенциальному нарушителю (файлы, диски, сетевые шары и т. п.);
* Сканирование узлов сетевого периметра, определение типов устройств, операционных систем, приложений;
* Идентификация уязвимостей сетевых служб и приложений;
* Анализ сервисов сетевой инфраструктуры;
* Анализ возможности получения злоумышленником несанкционированного доступа к конфиденциальной информации;

Результатом работ данного этапа является Отчет об анализе защищенности ИС.

В случае если Исполнителем выявлены критичные уязвимостей, препятствующие аттестации ИС, то Исполнитель сообщает Заказчику о необходимости устранения таких уязвимостей. Заказчик самостоятельно своими силами осуществляет устранение критичных уязвимостей.

* + 1. Аттестация ИС

На данном этапе Исполнитель обязан провести аттестацию на соответствие требованиям по информационной безопасности, установленных приказом ФСТЭК России № 239 по 1-ой категории значимости, приказом ФСТЭК России № 21 по 1-му уровню защищенности, РД АС по классу 1Г.

Условиями начала работ по данному этапу являются:

* реализованная система защиты информации в соответствии с техническим проектом;
* утвержденные в организации Заказчика организационно-распорядительные документы;
* отсутствие критичных уязвимостей, препятствующих аттестации ИС.

В состав работ этапа должны войти:

* Оценка (подтверждение) соответствия применяемых в ИС средств защиты информации в форме испытаний;
* Разработка Программы и методик аттестационных испытаний ИС;
* Проведение аттестационных испытаний ИС;
* Разработка заключения по результатам аттестационных испытаний ИС;
* Разработка аттестата соответствия (в случае положительного заключения по результатам аттестационных испытаний).
  + - 1. Требования к оценке (подтверждению) соответствия применяемых в ИС средств защиты информации в форме испытаний

Оценка (подтверждение) соответствия применяемых в ИС Заказчика средств защиты информации в форме испытаний проводится комиссией в составе работников Исполнителя и Заказчика и включает проведение комплекса организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие указанных средств защиты информации требованиям защиты информации, установленным Заказчиком в целях реализации Состава и содержания организационных и технических мер по обеспечению безопасности для значимого объекта первой категории значимости в соответствии с приказом ФСТЭК России № 239 и Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями 1-го уровня защищенности персональных данных, утвержденных приказом ФСТЭК России № 21.

По результатам проведения указанных испытаний Исполнителем оформляются Протоколы испытаний средств защиты информации и заключения об их соответствии или несоответствии установленным требованиям, подписываемые членами указанной комиссии и утверждаемые Исполнителем и Заказчиком.

* + - 1. Требования к разработке программы и методик аттестационных испытаний ИС

Аттестация ИС Заказчика включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие ИС Заказчика требованиям защиты информации.

Программа и методики аттестационных испытаний ИС Заказчика должны быть должны быть разработаны Исполнителем в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденными приказом ФСТЭК России от 29 апреля 2021 г. № 77, и согласованы с Заказчиком до начала аттестационных испытаний.

В ходе аттестационных испытаний Программа и методики аттестационных испытаний могут быть уточнены и скорректированы по согласованию с Заказчиком.

Программа и методики аттестационных испытаний должна быть выполнена в виде единого документа. Текст документа должен отвечать следующим требованиям:

* соответствовать действующим нормативным правовым актам, методическим документам и документам по стандартизации в области защиты информации, и при необходимости, иметь ссылки на них;
* формулировки в тексте должны быть четкими, изложенными в логической последовательности и не допускать различных толкований.

Программа и методики аттестационных испытаний должны состоять, как минимум, из следующих разделов:

* общие положения;
* программа аттестационных испытаний на соответствие требованиям безопасности информации;
* методики аттестационных испытаний на соответствие требованиям безопасности информации.

По результатам данного этапа Исполнителем должны быть разработаны Программа и методики аттестационных испытаний ИС Заказчика.

* + - 1. Требования к проведению аттестационных испытаний и разработке протоколов аттестационных испытаний

Аттестация ИС Заказчика проводится Исполнителем в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденными приказом ФСТЭК России от 29 апреля 2021 г. № 77, и Программой и методиками аттестационных испытаний ИС, разрабатываемыми и утверждаемыми Исполнителем и согласуемыми с Заказчиком.

Аттестационные испытания должны включать следующие мероприятия и работы:

* оценку соответствия технических паспортов ИС, подлежащих аттестации, актов классификации, состава и содержания эксплуатационной документации на систему защиты и документов по защите информации Заказчика действующим требованиям по защите информации;
* обследование ИС, подлежащих аттестации, на предмет оценки соответствия ИС, подлежащих аттестации, и условий их эксплуатации требованиям по защите информации;
* проверку наличия сведений о средствах защиты информации, установленных в ИС, подлежащих аттестации, в реестре сертифицированных средств защиты информации ФСТЭК России, или документов, подтверждающих проведение оценки соответствия средств защиты информации требованиям по безопасности информации в формах, отличных от сертификации;
* проверку наличия у Заказчика работников, ответственных за обеспечение защиты информации в ходе эксплуатации ИС, подлежащих аттестации, в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты (администраторов безопасности), управление конфигурацией ИС, подлежащих аттестации, реагирование на инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации;
* оценку уровня знаний и умений работников Заказчика, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации Заказчика;
* оценку соответствия принятых в ИС, подлежащих аттестации, организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для ИС, подлежащих аттестации, угроз безопасности информации;
* оценку соответствия принятых в ИС, подлежащих аттестации, технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для ИС, подлежащих аттестации, угроз безопасности информации.

По результатам аттестационных испытаний Исполнителем оформляются Протоколы аттестационных испытаний ИС Заказчика.

* + - 1. Требования к разработке заключений по результатам аттестационных испытаний и разработке аттестатов соответствия

По результатам аттестационных испытаний Исполнителем также оформляются:

* Заключение о соответствии ИС Заказчика требованиям защиты информации;
* Аттестат соответствия ИС Заказчика требованиям защиты информации (при условии положительного заключения по результатам аттестационных испытаний);
* Рекомендации по приведению ИС в соответствии требованиям, предъявляемым к ИС (в случае отрицательного заключения по результатам аттестационных испытаний).

Заключение по результатам аттестационных испытаний должно быть подписано членами аттестационной комиссии, утверждено Исполнителем и доведено до Заказчика.

Если Заключение по результатам аттестационных испытаний содержит выводы о возможности выдачи аттестата соответствия, Исполнитель должен оформить и выдать Заказчику аттестат соответствия ИС требованиям безопасности информации. В противном случае Исполнитель разрабатывает рекомендации по устранению выявленных замечаний и приведению системы защиты информации в соответствие с установленными требованиями. При несоответствии системы защиты информации ИС требованиям безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки Исполнитель принимает решение об отказе в выдаче аттестата соответствия.

Исполнитель вправе отказать Заказчику в выдаче аттестата соответствия в случае отрицательных результатов аттестационных испытаний ИС. При этом Исполнитель должен:

* указать в заключении по результатам аттестационных испытаний все выявленные нарушения и несоответствия;
* согласовать с Заказчиком порядок и сроки устранения выявленных нарушений и несоответствий;
* после их устранения провести повторные аттестационные испытания ИС   
  и выдать аттестат соответствия ИС требованиям безопасности информации.
  1. Проведение оценки соответствия требованиям ГОСТ Р 57580.1-2017

Для достижения целей по Оценке соответствия Исполнитель должен выполнить следующий комплекс работ, состоящий из 3 этапов:

* Оценка (аудит) текущего уровня защиты информации на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018.
* Исполнитель определяет область оценки соответствия требованиям стандарта ГОСТ 57580.1-2017: определение перечня мер стандарта ГОСТ 57580.1-2017, применимых к Заказчику с учетом модели угроз и нарушителя безопасности информации, утвержденной Заказчиком;
* Выезд к Заказчику на место проведения работ в целях выполнения обследования, включающего:
* интервьюирование сотрудников, участвующих в основных бизнес-процессах Заказчика;
* анализ реализованных организационных мер защиты;
* обследование инфраструктуры (в т.ч. серверного оборудования, сетевого оборудования, системного и прикладного ПО);
* осмотр рабочих мест сотрудников, задействованных в основных бизнес-процессах Заказчика;
* анализ конфигурации средств обеспечения безопасности

Исполнитель проводит расчет оценки выполнения требований национального стандарта Российской Федерации ГОСТ 57580.1-2017 в соответствии с методикой, определенной национальным стандартом Российской Федерации ГОСТ 57580.2-2018, включая:

* предварительную оценку Исполнителем выбора Заказчиком организационных и технических мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации;
* предварительную оценку Исполнителем полноты реализации Заказчиком организационных и технических мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему организации и управления защитой информации;
* предварительную оценку Исполнителем обеспечения Заказчиком защиты информации на этапах жизненного цикла автоматизированных систем.

Согласование с представителями структурного подразделения по информационной безопасности Заказчика результатов работ по оценке текущего уровня соответствия требованиям стандарта ГОСТ 57580.1-2017.

По итогам этапа должен быть разработан Отчет по результатам оценки соответствия, содержащий:

* сведения об Исполнителе;
* сведения о руководителе и членах проверяющей группы Исполнителя;
* сведения о Заказчике;
* цель оценки соответствия требованиям стандарта ГОСТ 57580.1-2017;
* сроки проведения оценки требованиям стандарта ГОСТ 57580.1-2017;
* область оценки соответствия требованиям стандарта ГОСТ 57580.1-2017;
* перечень неоцениваемых областей оценки соответствия требованиям стандарта ГОСТ 57580.1-2017 с обоснованием их исключения из области оценки соответствия;
* обоснование применения компенсирующих мер защиты информации при невозможности реализации отдельных выбранных мер защиты информации;
* краткое изложение процесса оценки соответствия требованиям стандарта ГОСТ 57580.1-2017, включая элемент неопределенности и/или проблемы, которые могли отразиться на надежности заключения по результатам оценки соответствия;
* числовое значение итоговой оценки соответствия требованиям стандарта ГОСТ 57580.1-2017, характеризующей соответствие информационной инфраструктуры и бизнес-процессов Заказчика установленным требованиям на дату завершения оценки соответствия;
* подтверждение того, что цель оценки соответствия требованиям стандарта ГОСТ 57580.1-2017 была достигнута в области оценки соответствия;
* неразрешенные разногласия между проверяющей группой Исполнителя и Заказчиком (при наличии);
* перечень и сведения о представителях Заказчика, которые сопровождали проверяющую группу Исполнителя при проведении оценки соответствия требованиям стандарта ГОСТ 57580.1-2017;
* сведения о конфиденциальном характере содержания отчета по результатам оценки соответствия требованиям стандарта ГОСТ 57580.1-2017;
* опись документов (копий документов) на бумажных носителях, прилагаемых к отчету по результатам оценки соответствия требованиям стандарта ГОСТ 57580.1-2017, с указанием общего количества томов приложений, количества и наименований документов, а также количества листов в каждом из них;
* приложения к Отчету, являющиеся его неотъемлемой частью:
* заполненные листы для сбора свидетельств оценки процессов защиты информации и направлений защиты информации, подтверждающих выставленные оценки, по форме, приведенной в приложении А стандарта ГОСТ 57580.2-2018;
* перечень нарушений в процессах защиты информации, выявленных членами проверяющей группы Исполнителя в результате оценки соответствия требованиям стандарта ГОСТ 57580.1-2017, которые могли или могут привести к инцидентам безопасности, наносящим ущерб финансовой организации или ее клиентам;
* таблицы, содержащие числовые значения оценок процессов защиты информации и направлений защиты информации по результатам оценки соответствия требованиям стандарта ГОСТ 57580.1-2017 и заполненные по формам, приведенным в приложении В стандарта ГОСТ 57580.1-2017;
* копии документов Заказчика или документов третьих лиц на бумажных носителях, являющихся свидетельствами выполнения (невыполнения) требований стандарта ГОСТ 57580.1-2017;
* машинные носители информации с электронными документами и файлами данных, являющихся свидетельствами выполнения (невыполнения) требований стандарта ГОСТ 57580.1-2017.
  + 1. Разработка рекомендаций по приведению информационной инфраструктуры Заказчика и его бизнес-процессов к необходимому уровню соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017

Исполнитель разрабатывает перечень рекомендаций по приведению уровня обеспечения защиты информации Заказчика к необходимому уровню соответствия требованиям стандарта ГОСТ 57580.1-2017, включая:

* представление Исполнителем рекомендаций по внесению изменений в действующие и (или) разработке Исполнителем новых внутренних нормативных документов Заказчика в области защиты информации, процессов защиты информации Заказчика (если необходимо);
* внесение Исполнителем изменений (актуализация, доработка) в действующие и (или) разработка новых внутренних нормативных документов Заказчика в области защиты информации, процессов защиты информации Заказчика (если необходимо).

Согласование с представителями структурного подразделения по информационной безопасности Заказчика результатов работ по разработке перечня рекомендаций по приведению информационной инфраструктуры Заказчика и его бизнес-процессов к необходимому уровню соответствия требованиям стандарта ГОСТ 57580.1-2017.

По итогам этапа должны быть разработаны:

* перечень рекомендаций по приведению уровня обеспечения защиты информации Заказчика к необходимому уровню соответствия требованиям стандарта ГОСТ 57580.1-2017;
* скорректированный комплект организационно-распорядительной документации, соответствующий по содержанию требованиям стандарта ГОСТ 57580.1-2017 по заданному уровню защиты информации (при необходимости).
  + 1. Итоговая оценка уровня защиты информации с выдачей заключения о соответствии заданному уровню защиты информации

Выезд к Заказчику на место проведения работ в целях выполнения проверки реализации рекомендаций по повышению уровня соответствия требованиям стандарта ГОСТ 57580.1-2017.

Исполнитель проводит расчет итоговой оценки выполнения требований национального стандарта Российской Федерации ГОСТ 57580.1-2017 в соответствии с методикой, определенной национальным стандартом Российской Федерации ГОСТ 57580.2-2018, включая:

* итоговую оценку Исполнителем выбора Заказчиком организационных и технических мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации;
* итоговую оценку Исполнителем полноты реализации Заказчиком организационных и технических мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему организации и управления защитой информации;
* итоговую оценку Исполнителем обеспечения Заказчиком защиты информации на этапах жизненного цикла автоматизированных систем.

Согласование с представителями структурного подразделения по информационной безопасности Заказчика результатов работ по оценке итогового уровня соответствия требованиям стандарта ГОСТ 57580.1-2017.

По итогам этапа должен быть разработан Отчет по результатам оценки соответствия и приложения к нему, скорректированные с учетом проведенных изменений, совершенных на основе рекомендаций по повышению уровня соответствия требованиям стандарта ГОСТ 57580.1-2017.

1. Сводный состав, сроки и описание работ

| **№**  **Этапа** | **Наименование работ** | **Сроки**  **работ** | **Результаты работ** |
| --- | --- | --- | --- |
| **Работы по проведению аттестации ИС «Т1Клауд»** | | | |
| 1.1 | Разработка проектной документации на систему защиту информации ИС | 10 рабочих дней | Акт классификации ИС  Модель угроз и нарушителей безопасности;  Частное техническое задание на создание подсистемы безопасности  Технический проект системы защиты информации ИС  Акт сдачи-приемки этапа выполненных работ |
| 1.2 | Разработка комплекта организационной документации, необходимый для выполнения требований законодательства по защите | 10 рабочих дней | 1. Проект приказа Об организации работ по защите информации в ООО «Т1Клауд»;  2. Технический паспорт ИС;  3. Положение о порядке организации и проведении работ по защите конфиденциальной информации в ИС;  4. Матрица доступа к ИС;  5. Инструкция по антивирусному контролю в ИС;  6. Инструкция по парольной защите в ИС;  7. Инструкция администратора информационной безопасности ИС;  8. Инструкция Ответственного за защиту информации в ИС;  9. Инструкция администратора ИС;  10. Инструкция пользователя ИС;  11. Список лиц, допущенных к обработке информации конфиденциального характера, в том числе персональных данных, в ИС;  12. Регламент идентификации и аутентификации;  13. Регламент управления доступом;  14. Регламент защиты машинных носителей информации;  15. Регламент аудита безопасности;  16. Регламент антивирусной защиты;  17. Регламент контроля защищенности информации;  18. Регламент ограничения программной среды;  19. Регламент обеспечения целостности;  20. Регламент защиты технических средств и систем;  21. Регламент управления конфигурацией информационной (автоматизированной) системы;  22. Регламент защиты среды виртуализации;  23. Регламент обеспечения доступности информации;  24. Политика безопасности при использовании средств криптографической защиты информации;  25. Регламент управления обновлениями программного обеспечения;  26. Регламент реагирования на компьютерные инциденты;  27. Регламент информирования и обучения персонала;  28. Регламент предотвращения вторжений (компьютерных атак);  29. Регламент защиты информационной (автоматизированной) системы и ее компонентов;  Регламент планирования мероприятий по обеспечению защиты информации. |
| 1.3 | Анализ защищенности ИС | 4 рабочих дня | Отчет об анализе защищенности ИС |
| 1.4 | Аттестация ИС | 7 рабочих дней | Программа и методики аттестационных испытаний ИС  Протокол аттестационных испытаний ИС  Заключение по результатам аттестационных испытаний ИС  Аттестат соответствия (в случае положительного заключения по результатам аттестационных испытаний)  Рекомендации по приведению ИС в соответствии требованиям, предъявляемым к ИС (в случае отрицательного заключения по результатам аттестационных испытаний) |
| **Проведение оценки соответствия требованиям ГОСТ Р 57580.1-2017** | | | |
| 2.1 | Оценка (аудит) текущего уровня защиты информации на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 | 5 рабочих дней | Отчет по результатам оценки соответствия |
| 2.2 | Разработка рекомендаций по приведению информационной инфраструктуры Заказчика и его бизнес-процессов к необходимому уровню соответствия требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 | 2 рабочих дней | Перечень рекомендаций по приведению уровня обеспечения защиты информации Заказчика к необходимому уровню соответствия требованиям стандарта ГОСТ 57580.1-2017 |
| 2.2 | Итоговая оценка уровня защиты информации с выдачей заключения о соответствии заданному уровню защиты информации | 7 рабочих дня | Отчет по результатам оценки соответствия |

1. Требования к Исполнителю

В рамках Договора должны быть выполнены работы по аттестации ИС, которые должны исполняться лицами, соответствующим следующим критериям:

* Наличие у исполнителя работ опыта по проведению работ и услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и системы информатизации облачных инфраструктур/центров обработки данных. Такой опыт может подтверждаться предоставлением следующих документов: исполненных договоров, актами выполненных работ.
* Наличие лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации в части работ и  услуг, утверждённых постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» на услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации, услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите, услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).
* Наличие лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и  телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) в части работ, предусмотренных пунктами 2, 3, 8, 9 перечня выполняемых работ и оказываемых услуг, составляющих деятельность, в отношении шифровальных (криптографических) средств, являющегося 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), утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.