

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Оказание комплекса специальных технических услуг в области информационной безопасности

1. Цель оказания услуг

Оказание комплекса специальных технических услуг в области информационной безопасности в соответствии с требованиями руководящих документов ФСТЭК России и ФСБ России.

2. Требования к исполнителю

Исполнитель должен иметь лицензии в соответствии со ст.27 Закона РФ «О государственной тайне» № 5485-1 от 21 июля 1993г., пунктом 2 «Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 года № 333, перечисленные ниже:

- - **Лицензия ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.**

Требование установлено в соответствии с:

- статьей 27 Федерального закона от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

- пунктом 2 «Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 года № 333.

- - **Лицензия ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).**

Требование установлено в соответствии с:

- статьей 27 Федерального закона от 21 июля 1993 года N 5485-1 «О государственной тайне»;

- пунктом 2 «Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением

мероприятий и (или) оказанием услуг по защите государственной тайны» утвержденного постановлением Правительства Российской Федерации от 15 апреля 1995 года № 333.

3. Основные сокращения, обозначения

Сокращения:

СЗИ – средства защиты информации

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ФСБ – Федеральная Служба Безопасности

РСП - режимно-секретное подразделение

АС – автоматизированная система

4. Наименование объектов информатизации Заказчика.

Объект информатизации: «Автоматизированная система» - кол-во 1.

Состав технических средств и видов услуг и работ:

№ п/п	Наименование работ	Кол-во	Технические характеристики
1. Проведение мероприятий по аттестации автоматизированной системы по требованиям безопасности информации			
1.1	Оценка соответствия объекта информатизации, а также условий его эксплуатации требованиям о защите информации	1	- оценка соответствия технического паспорта объекта информатизации, акта категорирования объекта информатизации, акта классификации информационной (автоматизированной) системы, а также содержания документов по технической защите информации владельца объекта информатизации требованиям о защите информации; - проверка наличия у владельца объекта информатизации заключений о специальной проверке технических средств и систем, предписаний на эксплуатацию, оформленных по результатам специальных исследований технических средств и систем, протоколов специальных исследований технических средств и систем, эксплуатационной документации на сертифицированные средства защиты информации; - оценку соответствия объекта информатизации, а также условий его эксплуатации требованиям о защите информации и сведениям, приведенным в техническом паспорте объекта информатизации, акте категорирования объекта информатизации, акте классификации информационной (автоматизированной) системы эксплуатационной документации на систему защиты информации объекта информатизации и на отдельные средства защиты информации, документах по технической защите информации владельца объекта информатизации;
1.2	Анализ организационной структуры объекта информатизации	1	- проверка наличия у владельца объекта информатизации назначенных работников, ответственных за обеспечение технической защиты информации в ходе эксплуатации объекта информатизации, контроль состояния технической защиты информации; - оценка уровня знаний и умений работников владельца

			объекта информатизации, ответственных за создание (эксплуатацию) объекта информатизации, а также за организацию и контроль состояния технической защиты информации на объекте информатизации, по вопросам эксплуатации системы защиты информации объекта информатизации, настройки и эксплуатации средств защиты информации; - оценка соответствия принятых на объекте информатизации организационных мер требованиям о защите информации
1.3	Анализ системы защиты информации на объекте	1	- проверка наличия сведений . о средствах защиты информации, установленных на объекте информатизации, в государственном реестре сертифицированных : средств защиты информации, ведение которого осуществляет ФСТЭК России в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. №55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063); - проверка соответствия примененных параметров настройки средств защиты информации требованиям о защите информации и эксплуатационной документации на средства защиты информации
1.4.	Оценка эффективности защиты (защищенности) информации от утечки за счет несанкционированного доступа	1	- проверка соответствия примененных параметров настройки средств защиты информации требованиям о защите информации и эксплуатационной документации на средства защиты информации; - анализ уязвимостей информационной (автоматизированной) системы, испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной (автоматизированной) системе в обход ее системы защиты информации
1.5	Оценка эффективности защиты (защищенности) информации от утечки по техническим каналам	1	- оформление протоколов оценки эффективности защиты (защищенности) информации и заключения по результатам аттестационных испытаний объекта информатизации; - вывод о возможности или невозможности выдачи аттестата соответствия или о необходимости доработки системы защиты информации объекта информатизации; - выдача аттестата соответствия по окончании доработки системы защиты информации объекта информатизации в случае несоответствия объекта требованиям безопасности информации.

Требования по информационной безопасности объектов информатизации:

Технические решения по защите информации информационной (автоматизированной) системы, указанной в техническом задании, должны соответствовать требованиям, предъявляемым:

- «Требованиям по технической защите информации, содержащей сведения, составляющие государственную тайну», утвержденных приказом ФСТЭК России от 20 октября 2016г. №025.

5. Общие требования

5.1. При оказании услуг и выполнения работ необходимо руководствоваться следующими документами:

- ГОСТ 29339-92 Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования
- Закон Российской Федерации от 21.07.1993 г. № 5485-1 "О государственной тайне".
- Федеральный закон Российской Федерации от 28.12.2010 № 390-ФЗ "О безопасности".
- «Инструкции по обеспечению режима секретности в Российской Федерации», Постановление Правительства РФ № 3-1 от 05.01.2004 г.
- «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», введенное в действие постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51.
- «Модель иностранных технических разведок до 2030 года» (Модель ИТР-2030).
- «Требования по технической защите информации, содержащей сведения, составляющие государственную тайну», утвержденный приказом ФСТЭК России от 20 октября 2016 г. №025
- Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащей сведения, составляющие государственную тайну, утвержден приказом ФСТЭК России от 28 сентября 2020 г. №110
- Требования к средствам активной защиты информации от утечки за счет ПЭМИН
- Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок
- «Нормы защиты речевой информации, обрабатываемые техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)» (Гостехкомиссия России, 1998);

6. Требования к оказываемым услугам и к отчетным документам

6.1. Разработка и согласование отчетных материалов по итогам оказания услуг производится в строгом соответствии с действующими руководящими и нормативно-методическими документами ФСБ и ФСТЭК России.

6.2. Отчетные материалы должны быть представлены в описательной, графической (при необходимости) и табличной форме, в одном экземпляре, на бумажных носителях, имеющих установленный руководящими документами гриф секретности.

6.3. Отчетные документы (Протоколы, Заключение, Акты и т.д.) по результатам оказания услуг аттестационной комиссии оформляются в строгом соответствии с требованиями ГОСТ Р 7.0.97-2016 и других нормативных документов.

6.4. Отчетные документы должны быть исполнены без опечаток и описок. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

6.5. Гриф секретности отчетных документов должен соответствовать степени секретности сведений, содержащихся в документах.

6.6. Перечень отчетных документов и материалов по результатам оказания услуг по защите информации и аттестации объектов информатизации:

- протокол измерения побочных электромагнитных излучений и расчета контролируемой зоны от технических средств;
- акты установки сертифицированных средств защиты информации
- протокол инструментального контроля защищенности акустической речевой информации и выполнения норм противодействия акустической речевой разведке в помещении;
- заключение по результатам контроля защищенности объекта информатизации на соответствие требованиям по безопасности информации.
- заключение по результатам проведения мероприятий по аттестации на соответствие требованиям по безопасности информации.
- Аттестат соответствия по требованиям безопасности информации.

7. Требования по допуску аттестационной комиссии и специалистов исполнителя на объект информатизации:

7.1. Исполнитель должен заблаговременно представить в режимно-секретное подразделение Заказчика утвержденный список своих специалистов, с паспортными данными для оказания услуг по защите информации и членов аттестационной комиссии для проведения аттестационных испытаний, а также список (перечень) оборудования и контрольно-измерительной аппаратуры, необходимых для оказания услуг (для заказа пропусков на внос и вынос в здание).

7.2. Каждый член аттестационной комиссии и специалист для получения доступа к объектам проведения оценки защищенности должен постоянно иметь при себе документы, удостоверяющие личность, справку о допуске и предписание на оказание услуг.

8. Требования по безопасности информации

8.1 Услуги должны оказываться в соответствии с лицензиями ФСТЭК России, ФСБ России (в части касающейся обеспечения безопасности информации).

8.2 Допуск сотрудников Исполнителя на объекты заказчика и порядок организации услуг должен производиться в соответствии с требованиями Закона Российской Федерации от 21.07.1993 г. № 5485-1 «О государственной тайне».

9. Требования к документам при проведении аттестации объектов информатизации

Перед проведением работ Исполнитель отправляет на согласование, доработку и утверждение в электронном виде в установленном порядке макеты следующих документов:

- а) технический паспорт объекта информатизации;
- б) акт категорирования объекта информатизации;
- в) акт классификации информационной (автоматизированной) системы
- г) документы по технической защите информации, регламентирующие правила эксплуатации объекта информатизации, в том числе по управлению системой защиты информации объекта информатизации, управлению конфигурацией объекта информатизации

Для проведения работ по аттестации объекта информатизаций владелец объекта информатизации представляет в орган по аттестации в электронном виде копии следующих утвержденных документов:

- а) технический паспорт объекта информатизации;
- б) акт категорирования объекта информатизации;

в) техническое задание на создание (модернизацию) объекта информатизации или частное техническое задание на создание (модернизацию) системы защиты информации объекта информатизации (для объектов капитального строительства - задание на проектирование (реконструкцию) объекта капитального строительства);

г) проектная документация на объект информатизации или систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);

д) эксплуатационная документация на систему защиты информации объекта информатизации и отдельные средства защиты информации;

е) документы по технической защите информации владельца объекта информатизации, регламентирующие правила эксплуатации объекта информатизации, в том числе по управлению системой защиты информации объекта информатизации, управлению конфигурацией объекта информатизации, оценке эффективности принимаемых на объекте информатизации мер по технической защите информации.

В случае необходимости уточнения данных об объектах информатизации орган по аттестации проводит обследование объекта информатизации в условиях его эксплуатации.

10. Порядок приемки.

Завершение работ оформляется «Актом сдачи-приемки услуг».

Место оказания услуг: 360017, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, 19.

Срок оказания услуг: с момента подписания Контракта и согласования списков на допуск на территорию с органами безопасности, после согласования выполнить работы в течении 45 (сорока пяти) рабочих дней, но не позднее 31.12.2026.