# Приложение №1

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ:** |
|  |
| Директор по информационным технологиям |
| *(должность начальника подразделения – Инициатора)* |
| Нестеров А.В. |
| *(Ф. И. О. Начальника подразделения – Инициатора)* |
|  |
| *(подпись)* |
|  |
| **ТЕХНИЧЕСКОЕ ЗАДАНИЕ** **для ДОГОВОРА ВОЗМЕЗДНОГО ОКАЗАНИЯ услуг по разработке моделей угроз и нарушителей** |
|  |
| Требования к предмету Закупки |
|  |
| Общие требования к качеству |
| В соответствии с данным техническим заданием Исполнитель оказывает услуги по разработке моделей угроз и нарушителей, в соответствии с требованиями и в объеме, указанным в п.1.6 данного Технического задания. |
|  |
| Требования к техническим характеристикам |
| Отсутствуют |
|  |
| Требования к размерам (заполняется для товаров) |
| Отсутствуют |
|  |
| Требования к упаковке (заполняется для товаров) |
| Отсутствуют |
|  |
| Требования к отгрузке (заполняется для товаров) |
| Отсутствуют |
|  |
| Количество товара, объем работ, услуг |
| Исполнитель оказывает услуги по разработке моделей угроз и нарушителей для 13 информационных систем (12 объектов КИИ с присвоенной категорией значимости, информационная система персональных данных).В рамках выполнения работ по моделированию угроз и нарушителя необходимо решить следующие задачи: в рамках требований к обеспечению информационной безопасности в информационных системах персональных данных и значимых объектов критической информационной инфраструктуры выполнить оценку угроз безопасности информации в соответствии с методикой, утвержденной ФСТЭК России 5 февраля 2021 г.Разрабатываемые документы должны содержать: * Систематизированный перечень угроз безопасности информации (для составления перечня должны использоваться угрозы, содержащиеся в банке данных угроз безопасности информации ФСТЭК России), связанных с: несанкционированным, в том числе случайным, доступом к информационным системам с целью изменения, копирования, неправомерного распространения информации или деструктивных воздействий на элементы информационных систем с использованием программных и программно-аппаратных средств.
* Определение актуальных категорий нарушителя.
* Результаты анализа актуальности угроз.
* Обоснование необходимого уровня криптографической защиты информации при её передаче по каналам связи.

Исполнитель должен обладать действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, включая услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизацииИсполнитель обязан во время проведения работ, а также после их выполнения обеспечить защиту сведений, полученных в рамках выполнения работ по данному ТЗ, в соответствии с законодательством Российской Федерации.Должно быть разработано 13 моделей угроз и нарушителя для каждого из перечисленных объектов.Срок исполнения работ должен составлять не более 60 рабочих дней с момента заключения Договора и предоставления Исполнителю необходимых сведений.  |
|  |
| Место, сроки (периоды), иные условия Закупки |
|  |
| Место поставки товара, выполнения работ, оказания услуг  |
| г. Санкт-Петербург, Пулковское шоссе, д. 41, лит. ЗИ.Контактное лицо: Винниченко Алексей НиколаевичE-mail: A.Vinnichenko@pulkovo-airport.com. |
|  |
| Сроки (периоды, стадии) поставки товара, выполнения работ, оказания услугСогласно коммерческому предложению потенциального поставщика, но не позднее 21.10.2022 г. |
|  |
| Иные условия поставки товара, выполнения работ, оказания услуг |
|  |
| Требования к Поставщику |
|  |  |
| наличие прав на осуществление определенных действий (деятельности):  |  |
|  |  |
| лицензии:Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации, включая услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации. | [x]  |
|  |  |
| участие в профессиональных объединениях (например, саморегулируемых организациях) [указать, каких];  | [ ]  |
|  |  |
| допуски, разрешения [указать, какие];  | [ ]  |
|  |  |
| сертификаты, декларации [указать, какие];  | [ ]  |
|  |  |
| договор об осуществлении деятельности от имени третьих лиц (например, в качестве официального дилера, поставщика и т. д.) [указать, какой];  | [ ]  |
|  |  |
| права на результаты интеллектуальной деятельности (лицензионные договоры, патенты, свидетельства и т. д.) [указать, какие];  | [ ]  |
|  |  |
| иные:  | [x]  |
| Исполнитель должен иметь в штате и привлечь при проведении работ не менее 3 (трёх) компетентных специалистов, имеющих высшее образование по направлению «информационная безопасность» и имеющих сертификаты OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), OSWE (Offensive Security Web Expert), OSWP (Offensive Security Wireless Professional), CISM (Certified Information Security Manager). Должны быть предоставлены копии сертификатов, дипломов, трудовых договоров. Исполнитель должен обладать опытом проведения вышеуказанных работ в объеме не менее 5 успешных проведенных разработок моделей угроз и нарушителей за 2 календарных года до момента начала подачи заявок, не менее двух договоров должно быть заключено в рамках 44-ФЗ или 223-ФЗ. Должны быть предоставлены копии договоров и актов, благодарственные письма, ссылки на протоколы подведения итогов. Исполнитель должен предоставить подтверждение в момент подачи заявки.  |  |
| квалификационные требования:  |  |
|  |  |
| требования к персоналу: | [ ]  |
|  |  |
| требования к производственным мощностям, технологиям, оборудованию [указать, какие];  | [ ]  |
|  |  |
| иные: | [ ]  |