**Техническое задание**

**на оказание услуг по разработке локальных нормативных (организационно-распорядительных) документов, регламентирующих вопросы защиты информации**

**Перечень принятых сокращений**

|  |  |
| --- | --- |
| **ГОСТ** | Государственный стандарт |
| **ОКПД** | Общероссийский классификатор продукции по видам экономической деятельности |
| **ФСБ России** | Федеральная служба безопасности Российской Федерации |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |

1. **ОБЩИЕ СВЕДЕНИЯ**
   1. **Наименование услуг**

Разработка локальных нормативных (организационно-распорядительных) документов, регламентирующих вопросы защиты информации (далее – Услуги).

* 1. **Цель оказания услуг**

Основной целью оказания услуг является регламентация вопросов защиты информации при обработке информации ограниченного доступа (коммерческой тайны, персональный данных и иной конфиденциальной информации).

Для достижения поставленной цели в процессе оказания услуг Исполнителем должны быть регламентированы следующие процессы:

* управления информационной безопасностью;
* обеспечения информационной безопасности;
* управление технологическими и/или бизнес-процессами;
* управление ИТ активами;
* обеспечение непрерывности и восстановления деятельности;
* управление инцидентами.
  1. **Этапы и срок оказания услуг**

Работы должны быть выполнены в течение 75 (семидесяти пяти) рабочих дней с даты подписания Договора.

* 1. **Нормативно-технические документы**

Основными документами, которые должны быть использованы при оказании услуг, являются следующие нормативные правовые акты, стандарты и руководящие документы:

* Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
* Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* «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», утверждены ФСБ России 31.03.2015 № 149/7/2/6-432;
* Приказ ФСБ России от 10.07.2014 № 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», утверждены ФСБ России 31.03.2015 № 149/7/2/6-432;
* «Инструкция 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», утвержденная приказом ФАПСИ от 13 июня 2001 года № 152;
* Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и оказания услуг по аттестации объектов информатизации на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну»;
* Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Методический документ. Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05.02.2021;
* ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
* ГОСТ 34.201-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
* ГОСТ 34.602-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
* ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности;
* ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности;
* ГОСТ Р ИСО/МЭК 27003-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности;
* ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Менеджмент информационной безопасности.

1. **ТРЕБОВАНИЯ К УСЛУГАМ**
   1. **Общие требования**

Для взаимодействия с Заказчиком Исполнитель обязан назначить ответственное контактное лицо, выделить телефонную линию службы поддержки, выделить адрес электронной почты для приема данных (запросов, заявок) в электронной форме и уведомить об этом Заказчика. Об изменении контактной информации ответственного лица Исполнитель обязан уведомить Заказчика. При поступлении по электронной почте от Заказчика запроса (заявок, писем) Исполнитель в срок, установленный Заказчиком, но не менее одного рабочего дня, предоставляет ответ Заказчику.

* 1. **Требования к составу и содержанию услуг**

Требования к составу и содержанию услуг, которые должны быть оказаны Исполнителем, а также отчетные документы по результатам оказания услуг приведены в Таблице 1.

Таблица 1 – Требования к составу и содержанию услуг

| **№ п/п** | **Процесс** | **Наименование документа** | **Описание, требования и ограничения** | **Этап разработки** |
| --- | --- | --- | --- | --- |
|  | Управление информационной безопасностью | Стратегия информационной безопасности | Взаимосвязь со стратегией развития Общества и интеграция с ИТ-стратегией (при их наличии).  Соответствие структуры и содержания положениям ISO 27001. | 1 |
| Политика обеспечения информационной безопасности | Документ должен содержать:   * собственную классификацию информационных систем с привязкой к критичности для бизнеса; * общие требования к информационной безопасности, обеспечению непрерывности бизнеса (резервирование компонентов, резервное копирование, мониторинг, восстановление и др.); * требования к взаимодействию с третьими лицами. | 2 |
| Политика анализа эффективности и совершенствования системы управления информационной безопасности | Общие положения и метрики оценки эффективности согласно ISO 2700х | 2 |
| Положение о работе с конфиденциальной информацией | Должны быть учеты требования для информации конфиденциального характера (относимой к конфиденциальной/для служебного пользования, коммерческой тайне).  Должен содержать:   * порядок отнесения к сведениям конфиденциального характера; * порядок доступа к сведениям конфиденциального характера; * порядок обращения с сведениями конфиденциального характера; * порядок раскрытия сведений конфиденциального характера; * порядок предоставления сведений конфиденциального характера; * порядок контроля; * перечни сведений конфиденциального характера, с отсылкой на Реестр процессов. | 2 |
| Формы приказов о:   * назначении ответственных лиц; * определений мест обработки и хранения носителей конфиденциальной информации; * определения мест проведения конфиденциальных переговоров; * создании комиссий и положений, регламентирующих их деятельность; * допуске к работе с конфиденциальной информацией; * и др. | - | 4 |
| Формы журналов учета. | - | 4 |
| Формы отчетов, актов, соглашений, планов и др. | - | 4 |
|  | Обеспечение информационной безопасности | Положение по порядку обращения с конфиденциальной информацией | - | 2 |
| Требования безопасности к информационным системам различной степени критичности | Ограничения: верхнеуровневый документ, без жесткой привязки и адаптации под особенности процессов разработки и эксплуатации систем (без разработки вытекающих регламентов). | 3 |
| Требования безопасности по конфигурировании компонентов ИТ-инфраструктуры | Ограничения: верхнеуровневый документ, без жесткой привязки и адаптации под особенности процессов разработки и эксплуатации ИТ-инфраструктуры (без разработки вытекающих регламентов). | 3 |
| Требования безопасности к конфигурации приложений | Ограничения: верхнеуровневый документ, без жесткой привязки и адаптации под особенности процессов разработки и эксплуатации приложений (без разработки вытекающих регламентов). | 3 |
| Требования безопасности при удаленном доступе к информационной инфраструктуре | Ограничения: верхнеуровневый документ, общие требования к порядку организации и типам применяемых средств защиты (без разработки вытекающих регламентов). | 3 |
| Требования безопасности беспроводных сетей | Ограничения: верхнеуровневый документ, общие требования к порядку организации и применяемым технологиям (без разработки вытекающих регламентов). | 3 |
| Требования безопасности при предоставлении доступа к информационной инфраструктуре третьим лицам | Ограничения: верхнеуровневый документ, общие требования к порядку организации и применяемым мерам защиты информации (без разработки вытекающих регламентов). | 3 |
|  | Управление технологическими и/или бизнес-процессами | Регламент описания технологическими и/или бизнес-процессами | - | 1 |
| Реестр процессов | Должен содержать сведения по технологическими и бизнес-процессами, в том числе следующие сведения:   * о владельцах процессов, цели процесса, перечне этапов; * о составе обрабатываемых данных и их отнесения к информации конфиденциального характера, основании для обработки данных; * об информационных потоках; * о местах размещения и/или хранения данных (носителей данных); * о составе информационных систем, задействованных в процессе; * о взаимодействии с третьими лицами и порядке взаимодействия; * о запретах и ограничениях в рамках процесса или обрабатываемых данных.   Ограничения: описание только двух процессов (кадровой деятельности и управления изменениями ИТ-инфраструктуры) | 1 |
|  | Управление ИТ активами | Политика управления ИТ-активами | - | 2 |
| Регламент управления изменениями | - | 3 |
|  | Обеспечение непрерывности и восстановления деятельности | План обеспечения непрерывности и восстановления деятельности бизнеса | Ограничения: оценка рисков без детализации, реализация модели с резервной площадкой | 2 |
| Руководство по обеспечению непрерывности | Должен включать:   * форму плана восстановления для критичной информационной системы. | 2 |
| Плана восстановления критичной информационной системы | Ограничения: сопровождение подготовки только одного плана восстановления. | 3 |
|  | Управление инцидентами | Политика управления инцидентами информационной безопасности | Основа документа согласно ГОСТ Р 59709-2022, ГОСТ Р 59710-2022, ГОСТ Р 59711-2022.  Ограничения: верхнеуровневый документ, без детальной классификации инцидентов с привязкой на компоненты ИТ-инфраструктуры. | 2 |
| План реагирования на компьютерные инциденты | Основа документа согласно ГОСТ Р 59709-2022, ГОСТ Р 59711-2022.  Прямая увязка на процесс обеспечения непрерывности и восстановление деятельности, в части касающейся.  Ограничения: общий план реагирования, без индивидуальных сценариев | 3 |

Итоговый комплект документов может быть дополнен Исполнителем, в случае необходимости детализации отдельных аспектов, регламентирующих вопросы защиты информации. Наименования документов, приведенных в Таблице 1, могут быть изменены Исполнителем по согласованию с Заказчиком.

Исполнитель должен собрать и проанализировать информацию, необходимую для оказания услуг, используя экспертно-документальный метод:

* очное, по месту проведения работ, и удаленное анкетирование и интервьюирование специалистов, участвующих в процессах обработки конфиденциальной информации;
* получение и анализ имеющейся локальной нормативной, организационно-распорядительной, эксплуатационной, рабочей и иной документации, регламентирующие вопросы обработки и обеспечения безопасности информации ограниченного доступа, не составляющей государственную тайну.

1. **ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ОКАЗЫВАЕМЫХ УСЛУГ**

Исполнитель должен взять на себя обязательства соблюдать конфиденциальность информации, ставшей ему известной в ходе оказания услуг, не открывать и не разглашать вышеуказанную информацию без предварительного письменного согласия, за исключением предоставления такой информации государственным, налоговым и аналогичным органам, если это требуется по действующему законодательству или решению суда.

Информация, полученная Исполнителем ходе оказания услуг, подлежит защите в соответствии с частью 4 статьи 16 Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1. **ТРЕБОВАНИЯ К ПОРЯДКУ И ОРГАНИЗАЦИИ ОКАЗАНИЯ УСЛУГ**

Исполнитель до выполнения работ обязан предоставить и согласовать с Заказчиком квалификацию сотрудников Исполнителя для реализации настоящего Технического задания.

Качество результатов работ определяется:

* отсутствием объективных замечаний со стороны работников (профильных специалистов) Заказчика к выполнению требований к документированию.
* соблюдением установленных сроков выполнения работ.

Оказание услуг осуществляется по рабочим дням с 09:00 до 18:00 МСК.

Место оказания услуг располагается на территории Заказчика. При необходимости Заказчик организовывает рабочие места для исполнителя. Место оказания услуг может быть изменено по договоренности Заказчика и Исполнителя. Заказчиком и Исполнителем может быть согласован дистанционный режим оказания услуг без необходимости присутствия сотрудников исполнителя в офисе Заказчика.

Исполнитель может осуществлять разработку документации с использованием собственной инфраструктуры.

Исполнитель гарантирует качество работ и обязуется своими силами и за свой счет устранить выявленные недостатки к разработанным документам.

1. **ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

Состав документов, разрабатываемых в рамках оказания услуг по настоящему Описанию объекта закупки определен в разделе 2.

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств.

Документация предоставляется в электронном виде в формате ODT, DOC (DOCX) или PDF. Заказчик в срок не более 5 рабочих дней с момента получения документации должен рассмотреть и, в случае отсутствия замечаний, согласовать направленную документацию.

В случае наличия замечаний по документации Заказчик в срок не более 5 рабочих дней с момента получения документа направляет Исполнителю замечания. Исполнитель в срок не более 5 рабочих дней с момента получения замечаний должен устранить замечания и направить документ на согласование Заказчиком.

1. **ТРЕБОВАНИЯ К УЧАСТНИКАМ ЗАКУПКИ**
   1. **Общие требования (ресурсы, опыт и квалификация)**

Исполнитель должен обладать материальными, техническими и людскими ресурсами и иметь возможность подтвердить наличие этих ресурсов.

Опыт оказания услуг по разработке локальных нормативных (организационно-распорядительных) документов за 2023 год.

Сотрудники Исполнителя, принимающие участие в оказании услуг, должны состоять в штате организации-Исполнителя. Исполнителем должна быть сформирована рабочая группа для оказания услуг в соответствии с настоящим Техническим заданием.

В состав рабочей группы должны входить работники Исполнителя, имеющие:

* высшее профессиональное образование по направлению подготовки (специальности) в области информационной безопасности или прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность»;
* высшее профессиональное образование по направлению подготовки (специальности) в области юриспруденции или прохождение обучения по программе профессиональной переподготовки по направлению «Юриспруденция»;
* высшее профессиональное образование по направлению подготовки (специальности) в области управления проектами или прохождение обучения по программе профессиональной переподготовки по направлению «Руководитель проектов».

В состав рабочей группы должны входить работники Исполнителя, имеющие:

* Информационная безопасность: не менее 1 человека;
* Юриспруденция: не менее 1 человека;
* Руководитель проектов: не менее 1 человека.

Исполнитель должен иметь возможность на этапе квалификационного отбора предоставить Заказчику следующие документы:

* согласие на обработку персональных данных;
* копии сертификатов и резюме сотрудников;
* копии договоров по выполненным аналогичным проектам (не менее 2 проектов за прошедший год).
  1. **Требования к лицензиям**

Исполнитель должен обладать следующими, действующими в период выполнения работ, лицензиями:

* ФСТЭК России на деятельность по технической защите конфиденциальной информации.

1. **УСЛОВИЯ ПРИВЛЕЧЕНИЯ СУБПОДРЯДНЫХ ОРГАНИЗАЦИЙ**

Настоящим техническим заданием не предусматривается возможность привлечения субподрядных организаций для выполнения данных работ.

Все положения данного технического задания является неотъемлемой частью договора.