**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на проведение работ по созданию системы защиты персональных данных МФЦ на трёх автоматизированных рабочих местах**

1. **Цели проекта:**

* обеспечение защиты от несанкционированного доступа (далее НСД) к информации и базам данных, находящимся на автоматизированных рабочих местах (далее АРМ) в МАУ ЩМР «МФЦ Щёлковского муниципального района»

1. **Наименование и содержание работ:**

Выполнение комплекса работ по построению системы защиты информации.

Содержание работ:

* установка и настройка сертифицированных средств защиты информации.
* приобретение сертифицированных средств защиты информации.

1. **Основание для выполнения работ:**

Работы должны проводиться в соответствии со следующими нормативными правовыми актами:

1. **Перечень и количество поставляемых программных средств защиты информации, а также перечень и объем выполняемых работ:**
   1. Перечень и количество поставляемых программных и программно-аппаратных средств защиты информации приведен в таблице 1.

Таблица 1 – Перечень и количество поставляемых программных средств защиты информации:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Перечень  программных и программно-аппаратных средств защиты информации | Кол-во | Материалы (техническая документация, носители и иное), представляемые Подрядчиком в ходе выполнения работ |
|  | Право на использование Средства защиты информации Secret Net 7. Клиент (автономный режим работы) или эквивалент | 3 | Лицензия на неисключительное право на использование программных средств на бумажном носителе – 1 шт. |
|  | Установочный комплект. Средство защиты информации Secret Net 7 (автономный) или эквивалент | 3 | Установочный дистрибутив (автономный вариант) - 3 комплектов.  Формуляр в печатном виде - 3 шт. Сертификат в бумажном виде - 3 шт. |
|  | Лицензия на право использования средства криптографической защиты информации КриптоПро CSP 3.9 (бессрочная) или эквивалент | 3 | Лицензия на неисключительное право на использование программного средства на бумажном носителе – 3 шт. |
|  | Программно-аппаратный комплекс "Соболь". Версия 3.0, Mini PCI-E Half Size - комплект с eToken PRO (Java), сертификат ФСТЭК России или эквивалент | 3 | Плата Mini PCI-E Half Size – 3 шт.  Диск с ПО и документацией – 3 шт.  Паспорт в печатном виде – 3 шт.  Копия сертификата (ФСТЭК России) – 3 шт.  Специальный защитный знак – 3 шт.  USB-ключ- 6 шт. |

* 1. Перечень и объем выполняемых работ по установке и настройке программных средств защиты информации приведен в таблице 2.

Таблица 2 – Перечень и объем выполняемых работ по установке и настройке программных средств защиты информации:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование работы | Кол-во | Обеспечение |
|  | Установка и настройка Средства защиты информации Secret Net 7. Клиент (автономный режим работы) или эквивалента | 3 усл. | Акт установки и настройки СЗИ |
|  | Установка и настройка ПО СКЗИ КриптоПро CSP 3.9 или эквивалента | 3 усл. | Акт установки и настройки СЗИ |
|  | Изготовление сертификата ключа проверки электронной подписи - срок действия сертификата 1 год | 3 усл. | Сертификат электронно-цифровой подписи в электронном виде |
|  | Установка и настройка ПАК "Соболь". Версия 3.0, Mini PCI-E Half Size - комплект с eToken PRO (Java) или эквивалента | 3 усл. | Акт установки и настройки СЗИ |
|  | Акты установки и настройки СЗИ (для каждой СЗИ) | 3 усл. | 3 документа на бумажном носителе |

1. **Место выполняемых работ**

Работы должны быть выполнены по следующему адресу:

* 141100, Московская обл., г. Щёлково, ул. Свирская, д. 2а.

1. **Место поставки средств защиты информации**

Поставку средств защиты информации необходимо осуществить по адресу:

* 141100, Московская обл., г. Щёлково, ул. Свирская, д. 2а.

1. **Требования к используемым технологиям.**

Построение системы защиты информации должно осуществляться на базе применения современных информационных технологий и обеспечивать:

* расширяемость и гибкость управления конфигурацией системы;
* надежность и отказоустойчивость аппаратных и программных средств системы.

Средства защиты должны быть совместимы с программными и аппаратными средствами автоматизированной обработки и защиты ПДн, используемыми заказчиком.

Архитектура СЗПДн должна быть открытой, масштабируемой и строиться по модульному принципу, каждый модуль должен обеспечивать свою часть функциональности решения задач в целом.

1. **Требования к обеспечению безопасности в ходе разработки и внедрения СЗПДн.**

Все сведения о составе и характеристиках СЗПДн являются конфиденциальной информацией.

Исполнитель СЗПДн обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации циркулирующей и хранящейся в ИС;
* не осуществлять несанкционированный доступ к информационным ресурсам ИС;
* 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.

Нарушение настоящих требований влечет за собою гражданско-правовую и иную ответственность, предусмотренную действующим законодательством.

**13. Требования к стандартизации, унификации и к гарантийному сроку**

13.1. Средства защиты информации должны соответствовать соглашениям и стандартам, в части работы с клавиатурой, отображения информации на экране, вызова справочной информации, организации пользовательского интерфейса и т.п.

13.2. Требования к гарантийному сроку и (или) объему предоставления гарантий качества средств защиты информации.

Объем предоставления гарантий качества средств защиты информации – 100%.

Подрядчик гарантирует качество поставляемых средств защиты информации в полном соответствии с требованиями действующего законодательства Российской Федерации.

Гарантийный срок на компакт диски не менее 12 месяцев.

Гарантийный срок на средства защиты информации не менее 12 месяцев.

Директор И.Ю. Кривошеева.