**Техническое задание  
на оказание услуг по созданию системы защиты персональных данных**

**и аттестации автоматизированных рабочих мест в администрации**

**Пушкинского муниципального района Московской области**

1. **Наименование оказываемых услуг.**

Услуги по созданию системы защиты персональных данных и аттестации автоматизированных рабочих мест в администрации Пушкинского муниципального района Московской области (далее – Заказчик).

Код бюджетной классификации: 700-0410-1320300010-242 226 330

1. **Объем оказываемых услуг.**

Объем оказываемых услуг представлен в Таблице №1.

Таблица №1

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование оказываемой услуги | Единица измерения | Объем оказываемой услуги |
|  | Инвентаризация информационных систем персональных данных | Усл.ед. | 1 |
|  | Доработка проектов организационно-распорядительной документации | Усл.ед. | 1 |
|  | Поставка, установка, настройка и ввод в эксплуатацию сертифицированных средств защиты информации на автоматизированные рабочие места с необходимым программным обеспечением | Шт. | 98 |
|  | Поставка, установка, настройка и ввод в эксплуатацию сертифицированного средства защиты информации (сервер безопасности) с необходимым программным обеспечением | Шт. | 1 |
|  | Аттестация по требованиям безопасности | Усл.ед. | 1 |

1. **Цели оказываемых услуг.**

Целью оказываемых услуг по защите персональных данных является обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных (далее - ИСПДн) Заказчика путем приведения процесса обработки персональных данных в соответствие с действующим законодательством.

1. **Место оказания услуги.**

Услуги должны быть оказаны по адресу: 141200, Московская обл., г. Пушкино, Московский пр-кт, д.12/2.

1. **Условия оказания услуги.**

Заказчик предоставляет Исполнителю: АРМ и серверы, входящие в состав ИСПДн Заказчика; установленное системное и вспомогательное программное обеспечение, а также средства защиты информации, дистрибутивы, лицензии и сертификаты на него; основные и вспомогательные технические средства; программно-аппаратные комплексы, дистрибутивы, лицензии и сертификаты на него; всю имеющуюся документацию по информационной безопасности.

Исполнитель должен обладать неисключительными правами на распространение приобретаемого программного обеспечения, предоставленные владельцем исключительных прав на программное обеспечение.

Начальная максимальная цена контракта (2 241 000, 00 рублей) определена и обоснована посредством применения метода сопоставимых рыночных цен (анализа рынка). Оплата оказанных услуг осуществляется за счет средств бюджета Пушкинского муниципального района Московской области.

1. **Сроки оказания услуги.**

Услуги должны быть оказаны в течении 20 (двадцати) рабочих дней с момента заключения контракта.

**7. Общие требования к оказанию услуг, требования к их качеству, в том числе к техническим характеристикам поставляемых средств защиты информации.**

* 1. Услуги по обновлению системы защиты информации должны быть оказаны в соответствии с требованиями и рекомендациями следующих нормативных документов:
* Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
* Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
* Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
* Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
* Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
* «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК 15.02.2008.
* «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК 15.02.2008.
* Приказ ФСБ России от 10.07.2014 N 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», а также иные нормативные правовые акты Российской Федерации в области защиты персональных данных.
  1. Требования к составу оказания услуг:
     1. Инвентаризация информационных систем персональных данных.

Содержание:

* Выезд Исполнителя по фактическому месту нахождения ИСПДн Заказчика для проведения обследования и инвентаризации инфраструктуры и информационных систем.
* Определение перечня персональных данных (далее – ПДн) и ИСПДн, подлежащих защите.
* Определение используемых средств обработки ПДн и оценка их соответствия требованиям нормативных документов РФ защиты, используемых на АРМ, обрабатывающих персональные данные.

Результаты:

* Отчет об инвентаризации информационных систем персональных данных, содержащий общее описание, территориальное расположение ИСПДн, физическое размещения объектов информатизации, схемы границ контролируемой зоны, перечень автоматизированных рабочих мест ИСПДн, состав обрабатываемых персональных данных, основания их обработки и другие сведения, являющиеся существенными с точки зрения построения системы защиты персональных данных.
* Проекты актов классификации ИСПДн Заказчика.
  + 1. Доработка проектов организационно-распорядительной документации.

Содержание:

* Анализ процесса обработки персональных данных.
* Анализ действующей организационно-распорядительной документации.
* Составление комплекта документации, регламентирующего процесс обработки персональных данных.

Результаты:

* Проекты приказов:
* «О назначении лиц, ответственных за обработку персональных данных».
* «Об организации защиты персональных данных».
* «О назначении комиссии по определению типа актуальных угроз и уровня защищенности информационной системы персональных данных».
* «О назначении комиссии по уничтожению материальных носителей информации, содержащих персональные данные».
* «Об утверждении мест хранения материальных носителей персональных данных».
* «Об утверждении плана мероприятий по защите персональных данных, обрабатываемых в информационных системах персональных данных».
* «Об утверждении форм журналов, используемых при обработке персональных данных, а также при эксплуатации технических средств защиты информации».
* «О вводе в действие документов, регламентирующих порядок обработки персональных данных».
* Модель угроз персональным данным.
* Протокол №1 экспертной оценки вероятности реализации угроз в информационных системах персональных данных.
* Протокол №2 экспертной оценки показателей опасности угроз для информационных систем персональных данных.
* Правила обработки персональных данных.
* Положение по обеспечению безопасности персональных данных
* Инструкции по обеспечению безопасности персональных данных:
* Инструкция администратора информационной системы персональных данных.
* Инструкция администратора безопасности информационной системы персональных данных.
* Инструкция лица, ответственного за организацию обработки персональных данных/
* Инструкция по обеспечению безопасности персональных данных.
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
* Политика в области обработки персональных данных.
* Правила работы с обезличенными персональными данными.
* Правила рассмотрения запросов субъектов персональных данных или их представителей.
* Перечень персональных данных, подлежащих защите в информационных системах персональных данных.
* Перечень информационных систем персональных данных.
* Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.
* Перечень должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.
* Порядок доступа в помещения, в которых ведётся обработка персональных данных.
  + 1. Поставка, установка, настройка и ввод в эксплуатацию сертифицированных средств защиты информации.

Содержание:

* Поставка и ввод в эксплуатацию средств защиты информации в соответствие с таблицей №2.

Таблица №2

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование | Единица измерения | Объем |
|  | Сертифицированное средство защиты с программным обеспечением, реализующим функции средства защиты информации от несанкционированного доступа Dallas Lock 8.0-К | Шт. | 57 |
|  | Сертифицированное средство защиты с программным обеспечением, реализующим функции средства защиты информации от несанкционированного доступа Dallas Lock 8.0-К с модулем «Межсетевой экран» | Шт. | 41 |
|  | Сервер безопасности для Dallas Lock 8.0-K с программным обеспечением, реализующем функции модуля централизованного управления средствами защиты информации от несанкционированного доступа, расширение диапазона. | Шт. | 1 |
|  | Установка, настройка межсетевого взаимодействия с сетью ViPNet № 2131 посредством имеющегося ПАК ViPNet Coordinator HW 1000 | Усл.ед. | 1 |
|  | Передача права на использование версии 4.X программного обеспечения ПАК ViPNet Coordinator HW1000 4.x | Усл.ед. | 1 |
|  | Сертифицированное средство защиты - программное обеспечение ViPNet Client for Windows 4.х бессрочная лицензия[[1]](#footnote-1) | Шт. | 27 |
|  | Установочный комплект ПО ViPNet Client 4.х (КС3) | Шт. | 1 |
|  | Передача прав на использование ПО ViPNet Client 4.х (КС3) в сети ViPNet № 2131 | Усл.ед. | 27 |
|  | Программное обеспечение, реализующее функции многозадачной и многофункциональной системы технической поддержки пользователей Resource Manager 2.5 - адаптивный пакет на 40 пользователей или эквивалент | Шт. | 1 |
|  | Предоставление прав на использование программного обеспечения XSpider 7.8, реализующего функции средства анализа защищенности, лицензия на 32 хоста, гарантийные обязательства в течение 1 года или эквивалент | Усл.ед. | 1 |

Результаты:

* Лицензии на средства защиты информации.
* Установка, настройка и ввод в эксплуатацию сертифицированных средств защиты информации в соответствии с требованиями эксплуатационной документации.
* Акты ввода в эксплуатацию сертифицированных средств защиты информации.
  + 1. Аттестация по требованиям безопасности.

Содержание:

* Анализ состояния информационной безопасности ИСПДн Заказчика.

Результаты:

* Программа и методика аттестационных испытаний.
* Протокол аттестационных испытаний.
* Заключение по результатам аттестационных испытаний.
* Аттестат соответствия (в случае успешного прохождения аттестационных испытаний).
  1. Требования к качественным и техническим характеристикам поставляемых средств защиты информации представлены в пунктах 7.3.1 - 7.3.2.
     1. Требования к качественным и техническим характеристикам программного обеспечения, реализующему функции многозадачной и многофункциональной системы технической поддержки пользователей:

Программа должна представлять собой многозадачную и многофункциональную систему технической поддержки пользователей и инвентаризации. Система представляет собой веб-приложение, для работы с которым необходим только доступ к серверу и браузер.

Программное обеспечение предназначено для работы с базой данных IT, телекоммуникационного оборудования, а также программного обеспечения, установленного на предприятии. Имеется возможность ведения учета расходных материалов и организации службы технической поддержки по расписанию и по заявкам пользователей. Программа автоматизирует процесс инвентаризации компьютеров предприятия. Клиентская часть программы должна устанавливаться на инвентаризируемые машины, которые добавляют подробную информацию о системе, подключенных устройствах и программном обеспечение в выделенную базу данных.

Возможности системы:

• управление заявками пользователей (заявки на обслуживание и техподдержку);

• интеграция с ActiveDirectory и почтовыми серверами (POP / IMAP);

• контроль за исполнением заявок;

• бизнес-правила при открытии тикетов (настраиваемые контактные лица);

• возможность автоматического назначение специалиста по категориям заявок пользователей (Заказчик, Источник запроса, Категория);

• SLA;

• статистика по заявкам, инженерам, пользователям и т.д. с возможностью построения графиков;

• учет компьютеров, периферийного оборудования, сетевых устройств, обычных принтеров и связанных с ними компонентами;

• инвентаризация компьютеров сети с описанием их компонентов (полная поддержка русского языка);

• возможность установки как на открытые операционные системы (Linux, BSD), так и на системы семейства Windows;

• сбор информации с компьютеров и мобильных устройств под управлением Windows\Windows Mobile, Android, Linux, MacOS, BSD, Solaris;

• инвентаризация программного обеспечения компьютеров: учитывает его, показывать изменения ПО, считает количество установленных версий (полная поддержка русского языка);

• назначение задач, планирование работ;

• управление лицензиями программного обеспечения;

• назначение оборудования по географическим регионам для пользователей и групп;

• управление статусом работы оборудования (зарезервировано, неисправно, плановое обслуживание и т.д.);

• учет и распределение поступлений запчастей для вышедшего из строя оборудования;

• возможность управления затратами на основе данных системы;

• использование нескольких интерфейсов, позволяющих пользователю отправить запрос в службу поддержки (web, e-mail), с возможностью загрузки файлов, скриншотов ошибок;

• уведомление ответственного специалиста по e-mail о поступлении новой заявки на его имя;

• управление документами, договорами, и связанных с ними товарно-материальных ценностей;

• резервирование оборудования;

• создание баз часто задаваемых вопросов "FAQ" и "Базы знаний";

• генерация отчетов и статистики в форматах PDF, CSV, SLK , PNG и SVG (полная поддержка русского языка);

• расширенный генератор отчетов PDF (по компонентам): аппаратное обеспечение, тех. поддержка (заявки) (полная поддержка русского языка);

• возможность выбора параметров (компонентов) генерация отчетов и статистики;

• данные хранятся в базе данных MySQL;

• возможность сохранения / восстановления базы данных в форматах SQL, XML;

• программа должна поддерживать русский язык;

• развертка агента инвентаризации в сети средствами ActiveDirectory;

• возможность автоматического графического генерирования структуры сети предприятия;

• возможность создания мульти-структуры организации(й);

• настраиваемые выпадающие списки;

• встроенная поисковая система;

• возможность автозагрузки с внешнего носителя;

• консультационная поддержка на 1 год;

• техническая поддержка на 1 год в режиме 8/5;

Комплект поставки: Электронная лицензия на 40 пользователей.

* + 1. Требования к качественным и техническим характеристикам программного обеспечения, реализующего функции средства анализа защищенности:

Должно осуществлять:

* Анализ и классификацию уязвимостей на 32 узлах защищаемой сети.

Требования по совместимости:

* Поддержка работы на ЭВМ под управлением следующих версий ОС: Microsoft Windows XP Professional SP 3 (x86), Microsoft Windows 2008 R2 Standard Edition SP1 (x64), Microsoft Windows 7 Professional SP 1 (x86, x64).
* Возможность использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах.

Требования по сертификации:

* Наличие сертификата соответствия требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по 4 уровню контроля отсутствия НДВ.

Должно обеспечивать:

* Проверку всех возможных уязвимостей независимо от программной и аппаратной платформы узлов: начиная от рабочих станций под Windows и заканчивая сетевыми устройствами Cisco, устройствами под управлением \*nix;Solaris, Novell, AS400 и т.д.;
* Возможность проверки на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты
* Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы.

|  |  |
| --- | --- |
| ЗАКАЗЧИК: | исполнитель: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. |

1. В целях обеспечения совместимости пунктов 1-5 Таблицы №2 с уже имеющимися у Заказчика средствами защиты данные позиции приобретаются без указания параметров эквивалентности. [↑](#footnote-ref-1)