Приложение 1

к извещению об осуществлении закупки

**Описание объекта закупки**

**1.** **Предмет муниципального контракта**: оказание услуг по передаче неисключительных прав на использование программного обеспечения для автоматизации процессов информационной безопасности.

**2.** **Требования к предоставляемым услугам:**

2.1. Перечень оказываемых услуг:

а) дистанционная установка программного обеспечения для автоматизации процессов информационной безопасности;

б) настройка службы заданий (оповещений по электронной почте).

2.2. Срок оказания услуг сопровождения и технической поддержки программного обеспечения - не менее 12 (двенадцати) месяцев с даты подписания Заказчиком документа о приёмке, предусмотренного муниципальным контрактом.

2.3. Тип поставки программного обеспечения - электронный.

**3. Перечень предоставляемых услуг:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Код ОКПД2/ КТРУ | Наименование услуг | Характеристика предоставляемых услуг | Кол-во |
| 1 | 58.29.50.000 | Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение | Передача неисключительных прав на использование программного обеспечения для автоматизации процессов информационной безопасности, бессрочно.  Основные функции программного обеспечения:  - предотвращение утечки или потери конфиденциальных данных;  - контроль действий пользователей ПК;  - учёт рабочего времени пользователей;  - анализ сотрудников на лояльность компании;  - анализ возникающих угроз в автоматическом режиме. | 1 штука |

Предоставляемые услуги включены в поз. 146 приложения 1 к постановлению Правительства Российской Федерации от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц».

**4. Перечень списков и журналов программного обеспечения для автоматизации процессов информационной безопасности:**

4.1. Списки, перечни и каталоги системы.

4.1.1. Общие:

1. Список организаций (филиалов);

2. Список сотрудников;

3. Список подразделений;

4. Список должностей;

5. Список помещений;

6. Информационные системы и объекты;

7. Модели угроз и требования безопасности;

8. Список компьютеров и устройств (СВТ);

9. Список программного обеспечения;

10. Журнал регистрации СЗИ и СКЗИ, эксплуатационной и технической документации к ним;

11. Каталог СЗИ;

12. Каталог инструктажей по информационной безопасности;

13. Комиссии по информационной безопасности;

14. Приказы по информационной безопасности;

15. Аттестации и работы по защите информации;

16. Учёт и реагирование на инциденты ИБ (с формированием файлов НКЦКИ);

4.1.2. Активы (ресурсы) и права пользователей.

17. Перечень защищаемых ресурсов и их администраторов;

18. Каталог прав доступа для ресурсов;

19. Список прав доступа;

20. Учётные записи пользователей;

4.1.3. Внутренние проверки и проверки надзорных органов.

21. Каталог внутренних проверок;

4.1.4. Персональные данные.

22. Перечень обрабатываемых персональных данных и целей обработки;

23. Перечень баз данных ПДн;

4.1.5. КИИ.

24. Перечень критических процессов в организации.

4.2. Служебные журналы, обеспечения процессов.

1. Журнал задач;

2. Назначенные инструктажи и мероприятия;

3. Назначенные внутренние проверки.

4.3. Обеспечиваемые процессы.

1. Планирование и выполнение внутренних проверок по защите информации для

информационных систем;

2. Контроль проведения инструктажей по информационной безопасности, допуск к СКЗИ;

3. Автоматизированная рассылка обучающего материала и тестирование пользователей по

вопросам информационной безопасности;

4. Автоматическое отслеживание прав доступа, носителей информации уволенных

сотрудников;

5. Автоматическое формирование файлов для НКЦКИ и учёт инцидентов информационной

безопасности;

6. Формирование пакетов документов ПДн/ГИС/КИИ на основе данных в системе;

7. Автоматическое ведение журналов учёта по информационной безопасности;

8. Формирование моделей угроз;

9. Автоматическое определение уровня защищённости ПДн, класса ГИС, категорирование

КИИ;

10. Синхронизация данных с внешними источниками (через CSV файлы);

11. Выполнение внешних приложений и скриптов (PowerShell);

12. Простановка штампов времени, с применением электронной подписи для подтверждения подлинности штампов;

13. Разграничение прав доступа пользователей к электронным журналам, полям, разделам системы;

14. Создание сертификатов простой электронной подписи для пользователей;

15. Управление учётными записями пользователей (создание, изменение, блокировка, разблокировка, удаление) с возможностью рассылки новым пользователям информационных сообщений с информацией об учётной записи и смене пароля;

16. Выполнение множественных операцией с СКЗИ (постановка на учёт, передача, списание) с автоматическим формированием актов и созданием записей в журналах;

17. Подписание выгружаемых печатных форм журналов электронной подписью (квалифицированной и простой) для подтверждения юридической значимости;

18. Автоматический сбор электронных подписей для неподписанных записей в журналах по электронной почте;

19. Ведение учёта машиночитаемых доверенностей (МЧД);

20. Автоматизация процесса ознакомление сотрудников с распорядительными документами под электронную подпись с автоматическим формированием записей в журнале ознакомления;

21. Подписание всех журналов и документов по информационной безопасности с помощью квалифицированной электронной подписи либо простой электронной подписи;

22. Комиссионное подписание актов жизненного цикла СКЗИ с механизмом сбора подписей по электронной почте с каждого члена комиссии;

23. Применение сертифицированных криптопровайдеров для создания электронной подписи (в том числе ViPNet CSP);

24. Рассылка оповещений пользователям о задачах, неподписанных записях с помощью микросервиса отправки почтовых сообщений с возможностью настройки параметров подключения к почтовому сервису.

4.4. Журналы:

1. Журнал учёта машинных носителей информации;

2. Журнал выдачи/возврата машинных носителей информации;

3. Журнал периодического тестирования средств защиты информации;

4. Журнал учёта нештатных ситуаций ИСПДн, выполнения профилактических работ,

установки и модификации программных средств на компьютерах ИСПДн;

5. Журнал проверок электронных журналов;

6. Журнал антивирусных проверок автоматизированных систем;

7. Журнал проведённых внутренних проверок режима защиты персональных данных;

8. Журнал проведения инструктажа по информационной безопасности;

9. Журнал резервного копирования и восстановления данных;

10. Журнал учёта актов;

11. Журнал регистрации СЗИ и СКЗИ, эксплуатационной и технической документации к ним;

12. Журнал поэкземплярного учёта выдачи/подключения/изъятия криптосредств (СКЗИ);

13. Журнал учёта установки/изъятия средств защиты информации;

14. Журнал учёта хранилищ;

15. Журнал регистрации выдачи/приёма хранилищ (помещений, сейфов, пеналов, печатей, ключей);

16. Журнал заседания комиссий по допуску к СКЗИ;

17. СКЗИ пользователя;

18. Журнал поэкземплярного учёта и выдачи ключевых документов (носителей);

19. Журнал опечатывания (опломбирования) технических средств;

20. Технический (аппаратный) журнал СКЗИ;

21. Журнал учёта передачи персональных данных;

22. Журнал учёта обращений субъектов персональных данных и их законных представителей;

23. Журнал назначения прав пользователям;

24. Журнал учёта машиночитаемых доверенностей;

25. Журнал ознакомления с документами;

26. Импорт сведений об используемых СКЗИ в организации из файлов CSV, с автоматическим созданием записей в соответствующих журналах.

4.5. Формируемые документы:

*Общие документы по организации.*

1. Акт классификации информационной системы (на ГИС и на ГИС с обработкой ПДн);

2. Модель угроз безопасности информации (документ формируется на каждую информационную систему);

3. Технический паспорт (документ формируется на каждую информационную систему);

4. Приказ/распоряжение/постановление о комиссии по определению класса ГИС и уровня защищённости ПДн;

5. Приказ/распоряжение/постановление об ответственном за защиту информации, не содержащей сведения, составляющие государственную тайну;

6. Приказ/распоряжение/постановление об утверждении перечня ИС, обрабатывающих защищаемую информацию, и перечня защищаемой информации, обрабатываемой в ПК, входящих в состав ИС;

7. Приказ/распоряжение/постановление о сотрудниках, осуществляющих обработку защищаемой информации, и имеющих доступ к обрабатываемой защищаемой информации;

8. Приказ/распоряжение/постановление о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты информации;

9. Приказ/распоряжение/постановление о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них;

10. Приказ/распоряжение/постановление о сотрудниках, имеющих доступ к содержанию электронного журнала сообщений;

11. Приказ/распоряжение/постановление об обеспечении безопасности материальных носителей защищаемой информации;

12. Приказ/распоряжение/постановление об обеспечении безопасности помещений, в которых размещены ИС и сохранности носителей защищаемой информации;

13. Приказ/распоряжение/постановление об утверждении форм документов, необходимых в целях выполнения требований законодательства в области защиты информации;

14. Приказ/распоряжение/постановление об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала учёта посетителей;

15. Приказ/распоряжение/постановление о системе разграничения доступа в ИС;

16. Приказ/распоряжение/постановление о комиссии по уничтожению защищаемой информации (документ формируется при наличии соответствующей комиссии);

17. Приказ/распоряжение/постановление о введении в эксплуатацию системы видеонаблюдения (документ формируется при наличии системы видеонаблюдения);

18. Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, при ее обработке в ИС;

19. Приказ/распоряжение/постановление об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности;

20. Приказ/распоряжение/постановление об ответственном за управление (администрирование) подсистемой безопасности (системой защиты информации);

*Комплект документов по эксплуатации СКЗИ.*

21. Приказ/распоряжение/постановление об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации;

22. Список допущенных к работе с ключами СКЗИ;

23. Заключение о готовности к работе с СКЗИ;

24. Перечень допущенных в помещения с ключами СКЗИ;

25. Акт уничтожения криптографических ключей;

26. Акт установки СКЗИ;

27. Акт изъятия СКЗИ;

*Документы КИИ.*

28. План мероприятий по реализации требований Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов;

29. Приказ/распоряжение/постановление об утверждении Положения о комиссии по категорированию объектов КИИ;

30. Приказ/распоряжение/постановление о комиссии по категорированию объектов КИИ;

31. Приказ/распоряжение/постановление об утверждении перечня объектов КИИ, подлежащих категорированию (в том числе форма отправки сведений во ФСТЭК России);

32. Акт категорирования объекта КИИ;

33. Сопроводительное письмо в ФСТЭК с перечнем объектов КИИ, подлежащих категорированию;

34. Форма утверждения перечня объектов КИИ с ФСТЭК;

35. Сопроводительное письмо в ФСТЭК с результатами категорирования объектов КИИ;

36. Сведения о результатах присвоения объекту КИИ категории значимости (документ формируется на каждый объект);

37. Приказ/распоряжение/постановление о назначении администратора безопасности значимых объектов КИИ;

38. Приказ/распоряжение/постановление об ответственном за обеспечение безопасности КИИ;

39. Приказ/распоряжение/постановление о силах обеспечения безопасности значимых объектов КИИ;

*Документы ПДн.*

40. Список работников, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения их служебных обязанностей;

41. Приказ/распоряжение/постановление об ответственном за организацию обработки ПДн;

42. Приказ/распоряжение/постановление об ответственном за обеспечение безопасности ПДн в ИС;

43. Приказ/распоряжение/постановление об утверждении перечня ПДн;

44. Политика в отношении обработки персональных данных;

45. Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, при их обработке в ИС;

46. Порядок хранения, использования и передачи ПДн сотрудников;

47. Акт оценки вреда, который может быть причинён субъектам ПДн;

48. Акт определения уровня защищённости ПДн при их обработке в ИС (на ИСПДн);

49. Согласие на обработку ПДн;

50. Согласие на поручение обработки ПДн;

51. Согласие на передачу ПДн;

52. Согласие на включение ПДн в общедоступные источники;

53. Уведомление о намерении осуществлять обработку ПДн;

54. Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн;

55. Информационное письмо о прекращении обработки ПДн.

Согласовано:

Контрактная служба: О.В. Дергилев