ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ

(оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))

**Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія: Держмитслужба м. Київ , вул. Дегтярівська, 11г, ЄДРПОУ 43115923.**

**Вид та ідентифікатор процедури закупівлі:** UA-2024-09-27-008766-a .

1. Предмет закупівлі: (зазначається назва предмета закупівлі та код ДК 021:2015 із застосуванням Єдиного закупівельного словника (див. пункт 2.3 розділу ІІ Порядку організації планування та проведення публічних закупівель в Державній митній службі України)).

постачання програмного забезпечення Системи запобігання витоку інформації та контролю даних Data Leak Prevention (DLP) та послуги з його впровадження, код ДК 021:2015-72260000-5 (Послуги, пов’язані з програмним забезпеченням)

2.Обґрунтування доцільності закупівлі (чим зумовлена необхідність закупівлі, мета закупівлі, посилання на вимоги чинного законодавства).

Основною метою закупівлі програмного забезпечення Системи запобігання витоку інформації та контролю даних Data Leak Prevention (DLP) та послуг з його впровадження (далі – Програмне забезпечення) є запобігання навмисним і випадковим витокам конфіденційної інформації із інформаційно-комунікаційних систем Державної митної служби України.

Придбання Програмного забезпечення дозволить захистити робочі станції користувачів, сервери та забезпечити безперебійне функціювання бізнес критичних сервісів, що наддасть змогу більш оперативно та ефективно надавати інформацію та підвищити безпеку та схоронність даних.

Серед головних завдань Програмного забезпечення можна виділити:

- організація захисту робочих станцій кінцевих користувачів та серверів від складних та невідомих кібер загроз та внутрішніх зловмисників, відстеження поведінки зловмисного ПЗ та реагування на кібер загрози

- надання можливості пошуку конфіденційної інформації, що знаходиться на робочих станціях та файлових серверах (з можливістю переміщення знайдених файлів в карантин та залишення на місці таких файлів інформації /текстових файлів/ про причини такого переміщення)

- забезпечення функціоналу захисту кінцевих точок від витоків інформації з кінцевих пристроїв та контролю витоку конфіденційних даних мережевими каналами

- забезпечення інструментів реакції на інциденти: автоматичне повідомлення відповідальної особи або власника інформації, блокування відправки по електронній пошті, блокування відправки даних через веб-форми, виконання скрипту, видалення конфіденційної інформації, можливість ескалації інциденту та запуску додаткових дій

- забезпечення класифікації файлів, текстових документів та зображень при пошуку даних у стані спокою та в русі, контроль копіювання файлів на рівні буферу обміну, блокування таких операцій в залежності від рівня класифікації файлу.

- контроль каналів потенційного витоку конфіденційної інформації: вихідні SMTP-з'єднання, вихідні HTTP-з'єднання, вихідні HTTPS-з'єднання, вихідні IM-з'єднання, копіювання інформації на зовнішні носії інформації та інформаційні ресурси, друк інформації на локальному\мережевому принтері.

Придбання та впровадження Програмного забезпечення дозволить забезпечувати виявлення і запобігання випадкам витоку конфіденційної інформації при використанні типових засобів обміну даними, в тому числі корпоративної електронної пошти, Web-пошти, мережевого друку, записів електронних даних на знімні носії, передачі конфіденційної інформації на внутрішні та зовнішні ресурси (в тому числі -файлові та хмарні сервіси), в тому числі ресурси та сервіси Office 365.

У результаті придбання Програмного забезпечення будуть вирішені наступні задачі з кіберзахисту даних:

• Запобігання комплексним атакам, збір необроблених метаданих подій для автоматичного розпізнавання шкідливої діяльності, забезпечення видимості процесів, активне полювання на загрози та криміналістичне розслідування;

• Забезпечення потужної реакції на кібер інциденти, ізоляції, дослідження та оновлення скомпрометованих кінцевих пристроїв користувачів;

• Виявлення втрати даних у разі передачі файлів з кінцевої точки на мобільний пристрій;

• Відстеження користувачів з високими правами дозволу;

• Можливість класифікувати файли та контролювати витоки за рівнем класифікації;

• Можливість блокувати передачу конфіденційних даних з ПК у папку спільного використання Fileshare та з Fileshare на ПК.

Загалом, буде забезпечено можливість запобігання витоку інформації, захисту конфіденційних даних, контроль та можливість класифікації оперативних й застарілих даних, стеження за виконанням норм й методики дотримання конфіденційності, виконувати аналіз поведінки користувачів щодо роботи з конфіденційною інформацією, розпізнавання даних, попередження втрати цінної інформації. Програмне забезпечення забезпечить можливість побудови гнучкої інфраструктурі для швидкого реагування на внутрішні випадкові і навмисні загрози, та виконання головної функції основна функція DLP-технології — блокування передачі інформації, в рамках існуючого законодавства та згідно внутрішніх норм організації, при цьому буде забезпечено гнучку систему налаштувань й управлінням процесами контроля за даними та користувачами.

Побудова рішення, що дозволить в режимі реального часу відслідковувати та керувати адаптивним механізмом дій користувачів, роботою служб та фонових процесів автоматизованих робочих місць.

3.Обґрунтування обсягів закупівлі (відповідно до чого визначено обсяги закупівлі або підставі чого обраховано).Обсяги закупівель визначені відповідно до потреб замовника на 2024 рік.

**ОПИС поСЛУГ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Найменування** | **Короткий опис** | **Кількість** | **Примітки** |
| 1. | Постачання програмного забезпечення Системи запобіганню витоку інформації Data Leak Prevention (DLP) та послуги з його впровадження для захисту 500 об’єктів, на 1 рік. | 1. Програмне забезпечення (ліцензія(ї)) в електронному вигляді для здійснення запобігання навмисним і випадковим витокам конфіденційної інформації із інформаційно-комунікаційних систем Державної митної служби України. | 1  комплект | Детальний опис наведено у таблиці 1 |

4.Обґрунтування технічних та якісних характеристик закупівлі (якісні характеристики) визначено відповідно до потреб замовника та з урахуванням загальноприйнятих норм і стандартів для зазначеного предмета закупівлі.

5.Обґрунтування бюджетного призначення та/або очікуваної вартості предмета закупівлі:

**Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі:** 1 500 000,00 грн, інформацію стосовно вартості послуг сформовано на підставі самостійного аналізу цін на аналогічні за технічними характеристиками послуги, яка міститься у відкритих джерелах (у тому числі на сайтах виробників та/або постачальників відповідної продукції, спеціалізованих торгівельних майданчиках, в електронних каталогах, рекламі, прайс-листах, тощо) з урахуванням вимог Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Мінекономіки від 18.02.2020 № 275.