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-2024-08-29-004778-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 (ліцензії на продовження права користування програмним забезпеченням для обладнання захисту електронної пошти (Cisco Secure Email Essential Inbound Malware Defense andANYL), (ESA McAfee Anti-Malware License), адміністрування поштових карантинів (Сentralized Email Management Reporting License) за кодом 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).

Реалізація засад з забезпечення кібербезпеки Держмитслужби, а саме забезпечення захисту програмно-технічного комплексу Держмитслужби «Електронна пошта» в режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень для всіх вхідних та вихідних повідомлень.

3.Обґрунтування обсягів закупівлі (відповідно до чого визначено обсяги закупівлі або підставі чого обраховано).

Обсяги закупівель визначені відповідно до потреб замовника на 2024 рік.

Ліцензії на продовження права користування програмним забезпеченням для обладнання захисту електронної пошти (Cisco Secure Email Essential Inbound Malware Defense andANYL), (ESA McAfee Anti-Malware License); адміністрування поштових карантинів (Сentralized Email Management Reporting License), код ДК 021:2015-72260000-5 (Послуги, пов’язані з програмним забезпеченням).

Метою закупівлі послуг є забезпечення захищеності електронного декларування та цифрових комунікацій в частині забезпечення захисту Програмно-технічного комплексу Держмитслужби «Електронна пошта» в режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень для всіх вхідних та вихідних повідомлень в межах Державної митної служби України.

У 2016 році Державною фіскальною службою України в рамках реалізації Стратегії розвитку ІТ в Державній фіскальній службі України, відповідно до договору від 05 грудня 2016 року № 179, було придбано та введено в експлуатацію програмно-апаратне обладнання Cisco ESA C690 та Cisco SMA M690 (акт введення в експлуатацію від 26.12.2016).

На базі придбаного обладнання розгорнуто програмно-технічний комплекс захисту інформації електронної пошти Державної фіскальної служби України з доступом до мережі Інтернет (далі Комплекс захисту ЕП).

Після реорганізації Державної фіскальної служби України Комплекс захисту ЕП відповідно до Розподільчого балансу передано у підзвіт Державній митній службі України.

Функціонування електронної пошти Держмитслужби в мережі Інтернет регламентовано наказом Державної митної служби України від 25.01.2024
№ 105 «Про затвердження Положення про порядок використання програмно-технічного комплексу Держмитслужби «Електронна пошта».

Відповідно до вимог Закону України від 05.10.2017 № 2163-VIII “Про основні засади забезпечення кібербезпеки в Україні”, та відповідно до п. 24 Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів, а також повинно бути забезпечено централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

Комплекс захисту ЕП використовується Державною митною службою України для захисту програмно-технічного комплексу Держмитслужби «Електронна пошта» в режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень.

Комплекс захисту ЕП передбачає підвищення рівня захищеності засобів електронної пошти та призначений для:

- захисту від проникнення шляхом поштових повідомлень на робочі станції користувачів шкідливого програмного забезпечення;

- попередження поширення небажаних поштових повідомлень та спаму в інформаційній мережі;

- реалізації єдиної політики антивірусного захисту поштової системи Держмитслужби;

- являється складовою частиною електронного митного декларування;

- задіяний в обміні інформацією між структурними підрозділами Держмитслужби та її територіальними органами, зі сторонніми організаціями, органами державної влади та митними/податковими органами іноземних держав.

З метою забезпечення функціонування Комплексу захисту ЕП необхідно продовження терміну дії наступних ліцензій:

**Ліцензія на продовження права користуванням програмним забезпечення для обладнання захисту електронної пошти (Cisco Secure Email Essential Inbound Malware Defense andANYL), (ESA McAfee Anti-Malware License), що активує наступний функціонал продукту:**

* Sophos Anti-Virus (забезпечення інтегрованого захисту від зловмисного програмного забезпечення за допомогою сканування вхідної та вихідної пошти на наявність зловмисного кода);
* IronPort Anti-Spam (надає можливість виявляти більшість небажаних листів, в тому числі графічний спам та зловмисні URL посилання);
* Incoming Mail Handling (забезпечує приймання вхідних електронних листів);
* Outbreak Filters (ідентифікує нові спалахи вірусної активності та розміщує в карантині підозріли повідомлення);
* Bounce Verification (забезпечує захист від спеціальних bounce-орієнтованих атак за допомогою спеціальної сигнатури у вихідне повідомлення).

Ліцензія в електронному вигляді на примірник програмного забезпечення **Email McAfee Anti-Virus** використовується для забезпечення антивірусного захисту від зловмисного програмного забезпечення за допомогою сканування вхідної та вихідної пошти (кількість поштових скриньок, що захищається – 5000 шт) на наявність зловмисного коду на 12 місяців;

* сканування на віруси;
* забезпечення захисту від атак 0-day для того, щоб заблокувати цільові email атаки на додаток до 0-day вірусним атакам;
* забезпечення динамічного карантину, куди відправляються підозрілі на вірус повідомлення до тих пір, поки не з'явиться підтверджена сигнатура або поки не закінчиться максимальний час зберігання повідомлень;
* завантаження сигнатури автоматично за розкладом;
* сканування стислих і архівних файлів;
* виявлення офісних документів популярних форматів (ms office ole та xml) за макросами та визначення для них окремих правил обробки.

**Ліцензія на продовження права користування програмним забезпеченням для адміністрування поштових карантинів (Centralized Email Management Reporting License), що активує наступний функціонал:**

* забезпечення централізованого звітування,
* відстеження повідомлень та карантину для декількох пристроїв безпеки електронної пошти (повідомлення електронною поштою + відстеження + централізовані карантини).

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.

**ТЕХНІЧНІ ВИМОГИ НАДАННЯ ПОСЛУГ**

**Послуги, пов’язані з програмним забезпеченням − за кодом ДК 021:2015 72260000-5**

Постачання програмного забезпечення (ліцензії на продовження права користування програмним забезпеченням для обладнання захисту електронної пошти (Cisco Secure Email Essential Inbound Malware Defense andANYL), (ESA McAfee Anti-Malware License); адміністрування поштових карантинів (Сentralized Email Management Reporting License) (далі – Послуги)

1. **Загальні відомості**

**1.** **Призначення Ліцензій на продовження права користування програмним забезпеченням для обладнання захисту електронної пошти**

З метою забезпечення захисту Програмно-технічного комплексу Держмитслужби «Електронна пошта» в режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень для всіх вхідних та вихідних повідомлень в межах Державної митної служби України функціонує Програмно-технічний комплекс захисту інформації електронної пошти Державної митної служби України з доступом до мережі Інтернет (далі – Комплекс захисту ЕП).

Комплекс захисту ЕП побудовано на базі обладнання захисту електронної пошти Cisco ESA C690 Email Security Appliance та Cisco SMA M690 Security Management Appliance і відповідного програмного забезпечення.

Комплекс захисту ЕП повинен забезпечувати захист близько 2 000 email Програмно-технічного комплексу Держмитслужби «Електронна пошта» у режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень для всіх вхідних та вихідних повідомлень у межах Державної митної служби України.

Продовження права користування програмним забезпеченням у складі Комплексу захисту ЕП передбачить підвищення рівня захищеності засобів Програмно-технічного комплексу Держмитслужби «Електронна пошта» та забезпечить:

захист від проникнення засобами ЕП на робочі станції користувачів шкідливого програмного забезпечення шляхом фільтрації вхідної/вихідної поштової кореспонденції на наявність загроз (шкідливе ПЗ, посилання, спам, віруси тощо);

попередження поширення (відправлення) небажаних поштових повідомлень та спаму від Держмитслужби;

захист від атак 0-day;

динамічний карантин;

автоматично, за розкладом, оновлення сигнатури антивірусних баз;

сканування стислих і архівних файлів;

виявлення офісних документів популярних форматів (ms office ole та xml) за макросами та визначення для них окремих правил обробки;

централізоване звітування (reporting), відстеження повідомлень та карантину для декількох пристроїв безпеки електронної пошти.

1. **Мета використання Комплексу захисту ЕП**

Захищеність електронного декларування та цифрових комунікацій в частині забезпечення захисту Програмно-технічного комплексу Держмитслужби «Електронна пошта» в режимі реального часу від зловмисного програмного забезпечення та спам-повідомлень для всіх вхідних та вихідних повідомлень в межах Державної митної служби України.

1. **Вимоги законодавства та підзаконних нормативних актів**

Митний кодекс України;

Закон України від 05 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах»;

Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України»;

Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;

Постанова Кабінету Міністрів України від 17 січня 2018 року № 55 «Деякі питання документування управлінської діяльності»;

Постанова Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».

## Вимоги до постачання програмного забезпечення

4.1. Замовник протягом 5 (п’яти) календарних днів з дати укладання Договору письмово (документом, підписаним з використанням кваліфікованого або удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті відкритого ключа (далі – Електронний підпис) або рекомендованим листом) надає Виконавцю інформацію щодо назви акаунту Замовника на вебсайті виробника програмного забезпечення/обладнання.

4.2. Виконавець протягом 30 (тридцяти) календарних днів з дати укладання Договору постачає програмне забезпечення, а саме забезпечує організацію розміщення в офіційному акаунті Замовника на вебсайті виробника програмного забезпечення/обладнання ліцензії на продовження права користування програмним забезпеченням для обладнання захисту електронної пошти (Cisco Secure Email Essential Inbound Malware Defense andANYL), (ESA McAfee Anti-Malware License); адміністрування поштових карантинів (Сentralized Email Management Reporting License) (далі – Програмне забезпечення).

4.3. Замовник активує Програмне забезпечення після закінчення строку дії попередніх ліцензій.

## Загальні вимоги до технічної підтримки

5.1. Технічна підтримка програмного забезпечення має відповідати таким вимогам:

5.2. Термін гарантійної (технічної, сервісної) підтримки Програмного забезпечення повинен складати не менш ніж 12 (дванадцять) місяців з дня активації Програмного забезпечення.

5.2.1. Надання консультацій телефоном та електронною поштою з питань налаштування і використання Програмного забезпечення в робочі дні з 9.00 до 18.00 годин;

5.2.2. Приймання запитів щодо налаштування і використання Програмного забезпечення в режимі 24х7х365, за телефоном, електронною поштою або через веб-сайт;

5.2.3. Реагування на запити щодо налаштування і використання Програмного забезпечення протягом 1 години з моменту отримання запиту на обслуговування за телефоном чи електронною поштою в робочі години;

5.2.4. Виконання обслуговування через вебсайт цілодобово у робочі, вихідні та святкові дні;

5.2.5. Доступ до закритої частини сайту виробника ([за](http://www.cisco.com) наявності) і онлайн бази знань виробника з великою кількістю технічної інформації та корисними інструментами;

5.2.5. Постійний (в режимі 24х7х365) доступ до Центру Технічної Підтримки виробника, електронною поштою або по телефону;

5.2.6. Надання Замовнику основних та перехідних версій Програмного забезпечення виробника за допомогою веб-сайту виробника.

5.3. Умови сервісної підтримки повинні включати в себе можливість реєстрації сервісних випадків в режимі 8х5хNBD, оновлення мікрокоду Комплексу захисту ЕП і версій встановленого Програмного забезпечення.

**ПЕРЕЛІК ОБЛАДНАННЯ ЗАМОВНИКА:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ з/п** | **Найменування обладнання** | **Одиниця виміру** | **Кількість** |
| 1. | Система управління, кешування та карантину Cisco SMA M690 Security Management Appliance (виробник Cisco Systems, Inc.) | комплект | 1 |
| 2. | Шлюз обробки пошти Cisco ESA C690 Email Security Appliance (виробник Cisco Systems, Inc.) | комплект | 2 |

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

**Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі:** **2 409 312,00** гривень. Визначення очікуваної вартості предмета закупівлі обумовлено статистичним аналізом загальнодоступної інформації про ціну предмета закупівлі на підставі затвердженої центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері публічних закупівель, примірної методики визначення очікуваної вартості предмета закупівлі, а саме: згідно з пунктом 1 розділу ІІІ наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 інформацію стосовно вартості послуг отримано від виробника обладнання/програмного забезпечення на основі Global Price List.