|  |  |
| --- | --- |
|  | **ДЕРЖАВНЕ ПІДПРИЄМСТВО****«МІЖНАРОДНИЙ АЕРОПОРТ «БОРИСПІЛЬ»** 08300, Україна, Київська обл., Бориспільський район, село Гора, вулиця Бориспіль -7, код 20572069, юридична особа/ суб'єкт господарювання, який здійснює діяльність в окремих сферах господарювання, зазначених у п. 4 ч.1 ст. 2 Закону України «Про публічні закупівлі» |
| Обґрунтування технічних та якісних характеристик предмета закупівлі та очікуваної вартості предмета закупівлі |

Підстава: пункт 4-1 постанови Кабінету Міністрів України від 11 жовтня 2016 р. № 710 «Про ефективне використання державних коштів»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Пункт Кошторису** | **Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником** | **Очікувана вартість предмета закупівлі згідно річного плану закупівель** | **Очікувана вартість предмета закупівлі згідно ОГОЛОШЕННЯ про проведення відкритих торгів** | **Ідентифікатор процедури закупівлі** |
| п. 41.29 (2025) | **Послуги для систем безпеки, код ДК 021:2015 - 72260000-5 - Послуги, пов’язані з програмним забезпеченням**  | 1 928 279,70 грн. з ПДВ | 1 606 899,75 грн. без ПДВ  | UA-2025-06-17-014445-a |

**Обґрунтування на виконання вимог Постанови КМУ від 11.10.2016 № 710:**

|  |  |  |
| --- | --- | --- |
| 1 | Обґрунтування очікуваної вартості предмета закупівлі | 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, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 та відповідно до затвердженої на підприємстві методики №50-06-1 від 17.05.2022. Очікувана вартість предмета закупівлі визначена методом порівняння ринкових цін на підставі отриманих комерційних пропозицій. Очікувану вартість закупівлі розраховано, як середньоарифметичне значення масиву отриманих даних. |
| 2 | Обґрунтування технічних та якісних характеристик предмета закупівлі | Технічні та якісні характеристики предмета закупівлі визначені з урахуванням реальних потреб підприємства та оптимального співвідношення ціни та якості. |
| 3 | Інша інформація | Інвентарні номери об’єкту основних засобів до яких планується закупівля послуг: - Міжмережевий екран Cisco Firepower 2110 NGFW, Appliance FPR2110-NGFW-K9, S/N JMX2209Y06B Інв.№56263/ВТ; - Міжмережевий екран Cisco Firepower 2110 NGFW, Appliance FPR2110-NGFW-K9, S/N JMX2209Y05X Інв.№56262/ВТ; - Програмне забезпечення системи безпеки електронної пошти Cisco Email Security Virtual Appliance (Cisco ESVA) Інв. №574; - Програмне забезпечення системи безпеки доступу до мережі Інтернет Cisco Web Security Virtual Appliance (Cisco WSVA) Інв.№575. |

Враховуючи зазначене, замовник прийняв рішення стосовно застосування таких технічних та якісних характеристик предмета закупівлі:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Найменування Послуги | Одиницявиміру | Кількість | Технічні та якісні характеристики предмета закупівлі |
| 1 | Послуга з передачі сервісного пакету для системи безпеки (підписка Threat Defense Threat Malware and URL для розширення функціоналу та можливостей пристрою Firepower серії 2110) | **послуга** | **2** | Послуга з передачі сервісного пакету для системи безпеки включає в себе: ­ підписку на AnyConnect для 100 кінцевих пристроїв (або підключень) Cisco AnyConnect Plus License, 1YR. L-AC-PLS-1Y-S2 (L-AC-PLS-LIC) на 12 місяців для забезпечення віддаленого підключення працівників до ІТ-сервісів підприємства. ­ підписку Threat Defense Threat Malware and URL на сервіси для пристрою Firepower серії 2110 на 12 місяців та включає в себе застосування на обладнанні наступних функцій: • виявлення та запобігання вторгненням, що дозволяє аналізувати мережевий трафік на предмет здійснення несанкціонованого доступу (вторгнення), використання уразливостей (експлойтів) та, за необхідністю, видалення кінцевих пакетів. • керування файлами, що дозволяє виявляти та, за бажанням, блокувати користувачів від надсилання або отримання файлів конкретних типів за конкретними протоколами додатків. • фільтрації, що дозволяє використовувати чорний список конкретних IP/URL-адрес та доменних імен DNS для обмеження (заборони) трафіку, перш ніж цей трафік буде підданий аналізу у відповідності до правил доступу. • виявлення користувачів, які здійснюють надсилання/отримання файлів конкретних типів за конкретними протоколами додатків. • автоматичне блокування або розблокування виявлених файлів, на основі списків дозволених/заборонених файлів. Можливість включення файлу до списку має бути наявна в політиці файлу. • застосування можливості писати правила контролю доступу, які визначають трафік, що може перетинати мережу на основі URL-адрес, запитуваних відстежуваними хостами, з кореляцією інформації про такі URL-адреси з метою отримання детального контролю над веб-трафіком. Послуга передбачається для наявного в Замовника обладнання, а саме: • міжмережевий екран Cisco Firepower 2110 NGFW, Appliance FPR2110-NGFW-K9, S/N JMX2209Y05X; • міжмережевий екран Cisco Firepower 2110 NGFW, Appliance FPR2110-NGFW-K9, S/N JMX2209Y06B. |
| 2 | Послуга з підтримки системи безпеки електронної пошти Cisco Email Security Virtual Appliance | **послуга** | **1** | Послуга передбачається для наявного у Замовника програмного продукту систем безпеки електронної пошти Cisco Email Security Virtual Appliance з наступними вимогами: ­ забезпечення обслуговування не менше \*550 користувачів. ­ забезпечення отримання основних та проміжних релізів програмного забезпечення через сайт Виробника, підтримка програмних кодів у актуальному стані Завдання на закупівлю від 30.05.2025 № 23-25-48 Аркуш 3 з 9 відповідно до рекомендацій Виробника протягом 12 місяців. Послуга з підтримки системи безпеки електронної пошти Cisco Email Security Virtual Appliance включає в себе підписку Cisco Secure Email Inbound Essentials plus Malware Defense and Cisco Threat Grid на 12 місяців з наступними функціями: - антиспам, репутація домену відправника та фільтрування URL-адрес. - Outbrake фільтри - розпізнавання та ізоляція підозрюваних загроз, поки не буде визначено, що вони безпечні; - захист від спуфінга за допомогою функції Forged Email Detection (FED); - вбудований антивірусний захист - для сканування електронної пошти; - виявлення загроз і реагування за допомогою функцій автоматизації; - динамічний аналіз розширених загроз. |
| 3 | Послуга з підтримки системи безпеки доступу до мережі Cisco Web Security Virtual Appliance | **послуга** | **1** | Послуга передбачається для наявного у Замовника програмного продукту системи безпеки доступу до мережі Інтернет Cisco Web Security Virtual Appliance (Cisco WSVA) з наступними вимогами: - забезпечення обслуговування не менше 550 користувачів. - забезпечення отримання основних та проміжних релізів програмного забезпечення через сайт Виробника, підтримка програмних кодів у актуальному стані відповідно до рекомендацій Виробника протягом 12 місяців. Послуга з підтримки системи безпеки доступу до мережі Cisco Web Security Virtual Appliance включає в себе підписку рівня Secure Web Appliance Essentials на 12 місяців з наступними функціями: - комплексний веб-захист за допомогою мережі виявлення загроз Cisco Talos; - наявність функції L4 моніторингу трафіку; - видимість і контроль додатків; - управління політиками; - можливість створення звітів; - наявність URL-фільтрації. - можливість інтеграції з іншими зовнішніми DLP системами для більш глибокої перевірки. |

**Додаткова інформація.**

**1.** У місцях, де технічна специфікація містить посилання на стандартні характеристики, технічні регламенти та умови, вимоги, умовні позначення та термінологію, пов’язані з товарами, роботами чи послугами, що закуповуються, передбачені існуючими міжнародними, європейськими стандартами, іншими спільними технічними європейськими нормами, іншими технічними еталонними системами, визнаними європейськими органами зі стандартизації або національними стандартами, нормами та правилами, **біля кожного такого посилання вважати вираз «або еквівалент»**. Таким чином вважається, що до кожного посилання додається вираз **«або еквівалент»**.

У місцях, де технічна специфікація містить посилання 1)на конкретну марку чи виробника або на конкретний процес, що характеризує продукт, чи послугу певного суб’єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва, **вважати наявним вираз «або еквівалент»**. Таким чином вважається, що до кожного посилання додається вираз «або еквівалент» ***(1) таке посилання обумовлено наданням Учасникам загального уявлення про технічні та якісні характеристики чи складові предмету закупівлі тощо)***.

Під «еквівалентом» розуміється це щось рівноцінне, рівнозначне, рівносильне, таке що повністю відповідає встановленим вимогам Замовника (технічні та якісні характеристики, запропонованого еквіваленту повинні відповідати встановленим в **Додатку 1** технічним та якісним характеристикам предмета закупівлі).