**Технічні (якісні) вимоги до предмета закупівлі:**

Пакети мережевого програмного забезпечення

ДК 021:2015: 48210000-3 — Пакети мережевого програмного забезпечення.

**Очікувана вартість предмета закупівлі: 500 000,00 грн.**

**Ідентифікатор закупівлі: UA-2021-02-05-012264-a.**

**При проведенні даної процедури закупівлі Замовник встановлює наступні технічні, якісні та кількісні критерії предмету закупівлі:**

7 штуки.

Місце поставки товарів або місце виконання робіт чи надання послуг: 03057, Україна, м. Київ, м. Київ, вул. Смоленська, 10.

Строк поставки товарів, виконання робіт чи надання послуг: 31 грудня 2021.

* 1. Ліцензія на використання програмного забезпечення закуповується до наявного у Замовника обладнання компаній-виробників Fortinet (FortiGate-60E, FortiGate-60D, FortiGate-100D, FortiGate-300D, FortiAnalyzer-400E) та HPE (HPE Aruba 7030 (RW) 64 AP Branch Cntlr (JW686A)) із технічною підтримкою протягом 1 (одного) року.
  2. Всі посилання на конкретну торгівельну марку чи фірму, патент, конструкцію або тип предмета закупівлі, джерело його походження або виробника, слід читати з виразом «або еквівалент». Технічні та якісні характеристики еквіваленту не повинні бути гіршими, а запропонована ліцензія на використання програмного забезпечення обов’язково повинно бути повністю сумісним з наявним у замовника обладнанням компанії-виробника Fortinet, НРЕ та забезпечувати повноцінну роботу всіх його функцій).
  3. Учасники процедури закупівлі повинні надати в складі тендерних пропозицій інформацію та документи, які підтверджують відповідність тендерної пропозиції Учасника технічним, якісним, кількісним та іншим вимогам до предмета закупівлі, наведеним у цьому додатку тендерної документації.
  4. Невідповідність пропозиції Учасника торгів вимогам цього додатку тендерної документації призводить до її відхилення. Неповні пропозиції відхиляються та участі у конкурсній процедурі не беруть.
  5. Відповідність технічних, якісних та кількості характеристик запропонованих товарів вимогам замовника повинна бути підтверджена учасником шляхом надання у складі тендерної пропозиції довідки, яка має містити порівняльну таблицю технічних, якісних та кількісних характеристик товару, що пропонується учасником, які мають бути не гіршими за наведені в «Технічних, якісних та кількості вимогах (характеристиках) до предмету закупівлі», що викладені у цьому додатку тендерної документації, із обов‘язковим зазначенням типу, марки, моделі, назви товару, що пропонується Учасником.
  6. Учасники процедури закупівлі повинні надати в складі тендерних пропозицій документ/копію документу від виробника/офіційного представника виробника програмного забезпечення (сертифікат/авторизаційний лист/ інший документ) про надання учаснику процедури закупівлі відповідного статусу (дилер/партнер/інший статус) та повноважень на постачання/продаж програмного забезпечення із зазначенням номеру закупівлі у системі Prozorro та найменування Замовника.

**ТЕХНІЧНІ,** **якіснІ та кількісні ВИМОГИ (характеристики) ДО ПРЕДМЕТУ ЗАКУПІВЛІ**

| **№** | **Найменування програмного забезпечення** | **Опис**  **програмного забезпечення** | **Кіл-ть** |
| --- | --- | --- | --- |
| **1** | **Ліцензія на використання програмного забезпечення Fortinet (FC-10-0060E-950-02-12) FortiGate-60E 1 Year Unified Threat Protection (UTP) 24x7** | **Сумістність з FortiGate-60E Ідентифікація та контроль застосувань (AC/ AVC)** Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control)  Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур  **Захист від загроз на основі сигнатурного аналізу (IPS)**  Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system)  Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур  Конфігурація виключень у діях з певними сигнатурами (exemption/override)  **Захист від malware (Antivirus/AMP)**  Anti-Virus / Anti-malware захист  Виявлення та блокування небажаних програм або файлів (grayware)  Захист від зловмисних програм для мобільних пристроїв  **Web та DNS-фільтрація**  Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація)  Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)  Виявлення та блокування DNS запитыв до Botnet мереж  **Захист від невідомих загроз (0-day)**  Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"  Ліцензування має дозволяти аналізувати у cloud sandbox не менше ніж 14 000 файлів на день (24 години)  **Технічна сервісна підтримка**  Обладнання повинно забезпечуватись технічною сервісною підтримкою строком 12 місяців у режимі 24\*7  Постійний доступ (24\*7) до центру технічної підтримки виробника через сайт, електронною поштою та за телефоном для реєстрації сервісних випадків та відкриття звернень  Постійний авторизований доступ (24\*7) до сайту виробника, отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки на протязі дії технічної сервісної підтримки  Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника на протязі дії технічної сервісної підтримки  Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | **2** |
| **2** | **Ліцензія на використання програмного забезпечення Fortinet (FC-10-0060D-950-02-12) FortiGate-60D 1 Year Unified Threat Protection (UTP) 24x7** | **Сумістність з FortiGate-60D Ідентифікація та контроль застосувань (AC/ AVC)** Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control)  Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур  **Захист від загроз на основі сигнатурного аналізу (IPS)**  Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system)  Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур  Конфігурація виключень у діях з певними сигнатурами (exemption/override)  **Захист від malware (Antivirus/AMP)**  Anti-Virus / Anti-malware захист  Виявлення та блокування небажаних програм або файлів (grayware)  Захист від зловмисних програм для мобільних пристроїв  **Web та DNS-фільтрація**  Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація)  Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)  Виявлення та блокування DNS запитыв до Botnet мереж  **Захист від невідомих загроз (0-day)**  Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"  Ліцензування має дозволяти аналізувати у cloud sandbox не менше ніж 14 000 файлів на день (24 години)  **Технічна сервісна підтримка**  Обладнання повинно забезпечуватись технічною сервісною підтримкою строком 12 місяців у режимі 24\*7  Постійний доступ (24\*7) до центру технічної підтримки виробника через сайт, електронною поштою та за телефоном для реєстрації сервісних випадків та відкриття звернень  Постійний авторизований доступ (24\*7) до сайту виробника, отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки на протязі дії технічної сервісної підтримки  Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника на протязі дії технічної сервісної підтримки  Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | **1** |
| **3** | **Ліцензія на використання програмного забезпечення Fortinet (FC-10-00116-950-02-12) FortiGate-100D 1 Year Unified Threat Protection (UTP) 24x7** | **Сумістність з FortiGate-100D Ідентифікація та контроль застосувань (AC/ AVC)** Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control)  Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур  **Захист від загроз на основі сигнатурного аналізу (IPS)**  Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system)  Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур  Конфігурація виключень у діях з певними сигнатурами (exemption/override)  **Захист від malware (Antivirus/AMP)**  Anti-Virus / Anti-malware захист  Виявлення та блокування небажаних програм або файлів (grayware)  Захист від зловмисних програм для мобільних пристроїв  **Web та DNS-фільтрація**  Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фільтрація)  Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)  Виявлення та блокування DNS запитів до Botnet мереж  **Захист від невідомих загроз (0-day)**  Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"  Ліцензування має дозволяти аналізувати у cloud sandbox не менше ніж 14 000 файлів на день (24 години)  **Технічна сервісна підтримка**  Обладнання повинно забезпечуватись технічною сервісною підтримкою строком 12 місяців у режимі 24\*7  Постійний доступ (24\*7) до центру технічної підтримки виробника через сайт, електронною поштою та за телефоном для реєстрації сервісних випадків та відкриття звернень  Постійний авторизований доступ (24\*7) до сайту виробника, отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки на протязі дії технічної сервісної підтримки  Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника на протязі дії технічної сервісної підтримки  Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | **1** |
| **4** | **Ліцензія на використання програмного забезпечення Fortinet (FC-10-00305-950-02-12) FortiGate-300D 1 Year Unified Threat Protection (UTP) 24x7** | **Сумістність з FortiGate-300D Ідентифікація та контроль застосувань (AC/ AVC)** Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control)  Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур  **Захист від загроз на основі сигнатурного аналізу (IPS)**  Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system)  Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур  Конфігурація виключень у діях з певними сигнатурами (exemption/override)  **Захист від malware (Antivirus/AMP)**  Anti-Virus / Anti-malware захист  Виявлення та блокування небажаних програм або файлів (grayware)  Захист від зловмисних програм для мобільних пристроїв  **Web та DNS-фільтрація**  Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фільтрація)  Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)  Виявлення та блокування DNS запитів до Botnet мереж  **Захист від невідомих загроз (0-day)**  Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"  Ліцензування має дозволяти аналізувати у cloud sandbox не менше ніж 14 000 файлів на день (24 години)  **Технічна сервісна підтримка**  Обладнання повинно забезпечуватись технічною сервісною підтримкою строком 12 місяців у режимі 24\*7  Постійний доступ (24\*7) до центру технічної підтримки виробника через сайт, електронною поштою та за телефоном для реєстрації сервісних випадків та відкриття звернень  Постійний авторизований доступ (24\*7) до сайту виробника, отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки на протязі дії технічної сервісної підтримки  Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника на протязі дії технічної сервісної підтримки  Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника). | **1** |
| **5** | **Ліцензія на використання програмного забезпечення Fortinet (FC-10-L0401-247-02-12) FortiAnalyzer-400E 1 Year 24x7 FortiCare Contract** | **Сумістність з FortiAnalyzer-400E**  **Технічна сервісна підтримка**  Обладнання повинно забезпечуватись технічною сервісною підтримкою строком 12 місяців у режимі 24\*7  Постійний доступ (24\*7) до центру технічної підтримки виробника через сайт, електронною поштою та за телефоном для реєстрації сервісних випадків та відкриття звернень  Постійний авторизований доступ (24\*7) до сайту виробника, отримання актуальних репутаційних баз, сигнатур захисту веб-додатків та всіх необхідних оновлень для сервісів безпеки на протязі дії технічної сервісної підтримки  Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника на протязі дії технічної сервісної підтримки  Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | **1** |
| **6** | **Ліцензія на використання програмного забезпечення HPE Aruba ClearPass Cx000V VM Appl E-LTUw\NL EY 100 CE E-LTUw \ 1Y FC 24x7 SVC Support** | Сумістність з HPE Aruba 7030 (RW) 64 AP Branch Cntlr (JW686A)  Загальні характеристики та архітектура  • Система управління політиками повинна мати можливість контролю доступу до дротової та бездротової мережі на основі ідентифікаційних даних користувача, типу та характеристик пристрою, стану програмного забезпечення на пристрої користувача;  • Система повинна підтримувати розгортання в віртуалізованому середовищі VMware ESX/i та Microsoft Hyper-V і має опцію поставки у вигляді образу віртуальної машини підготовленої для розгортання у відповідному середовищі.  Система повинна підтримувати можливість кластерізації для забезпечення відмовостійкого впровадження та масштабованості;  Система управління політиками по контролю доступу до дротової та бездротової мережі повинна підтримувати наступні основні функціональні можливості в запропонованій конфігурації:  • Підтримку сервісів автентифікації, авторизації та обліку дій користувачів (ААА) за протоколами RADIUS, Kerberos;  • Підтримка використання в якості зовнішнього джерела даних автентифікації та авторизації Microsoft Active Directory, із можливістю роботи в декількох AD доменах;  • Підтримка використання в якості зовнішнього джерела даних автентифікації та авторизації будь-якого LDAP-сумісного каталогу;  • Підтримка використання в якості зовнішнього джерела даних автентифікації та авторизації будь-якої ODBC-сумісної SQL бази даних;  • Підтримка використання в якості джерела даних автентифікації та авторизації вбудованої SQL бази даних;  • Підтримка 802.1X ;  • Підтримка протоколів PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);  • Підтримка протоколів EAP-TLS;  • Підтримка протоколів EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);  • Підтримка протоколів TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP);  • Підтримка протоколів PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-MD5;  • Підтримка MAC автентифікації для неінтелектуальних пристроїв;  • Підтримка веб-автентифікації;  • Підтримка профілювання та класифікації кінцевих пристроїв на основі MAC OUI, DHCP fingerprint, TCP, SNMP та інших методів;  • Можливість розгортання гостьового порталу для веб-автентифікації та авторизації гостьових користувачів і надання їм тимчасових облікових записів та контрольованого доступу до мережі відповідно до встановлених політик. Наявна можливість організації різних сценаріїв реєстрації гостьових користувачів в мережі, в тому числі:  • створення гостьових облікових записів авторизованим нетехнічним персоналом із використанням спеціалізованого інтерфейсу системи;  • самореєстрація гостьового користувача на порталі із автоматичним сповіщенням відповідального співробітника і активацією гостьового запису тільки після підтвердження з боку співробітника;  • самореєстрація гостей через гостьовий портал із наступним відправленням згенерованих облікових даних на вказаний при реєстрації мобільний номер за допомогою SMS повідомлення;  • Підтримка сервисів Apple Bonjour: AirPlay, AirPrint, mDNS;  • Вбудована система аналітики і генерації звітів, з використанням системних та створених користувачем шаблонів, можливість запуску за розкладом та автоматичного відправлення звітів по електронній пошті.  • Підтримка роботи із обладнанням різних виробників (мультивендорність), підтримка широкого переліку моделей дротового та бездротового обладнання (комутатори, контролери бездротового доступу та ін.) в якості NAS/NAD пристроїв.  • Забезпечується підтримка обладнання в пропозиції, а також обладнання, що використовується в мережі Замовника  Система управління політиками по контролю доступу до дротової та бездротової мережі повинна підтримувати наступні розширені функціональності системи (за умови придбання додаткових ліцензій):  • Вбудований центр сертифікації з можливістю його використання як в режимі автономного або підлеглого центру сертифікатів в корпоративній інфраструктурі;  • Створення умов для безпечного доступу допоміжних мобільних робочих пристроїв співробітників (планшети, смартфони), яким за політиками дозволений такий доступ, до корпоративної мережі шляхом автоматизації процесів настроювання допоміжних пристроїв для використання стійких методів автентифікації і доставки на них атрибутів доступу (сертифікатів з внутрішньої або зовнішньої PKI), без безпосередньої участі адміністратора. Підтримуються засоби автоматизованого настроювання та доставки атрибутів для мобільних пристроїв під управлінням Apple iOS, Android, Windows.  Підтримка контролю стану кінцевого пристрою (версія операційної системи, наявність критичних оновлень, наявність антивірусу із оновленою базою сигнатур) в процесі авторизації при доступі до мережі, для операційних систем сімейства Microsoft Windows з використанням технології Microsoft NAP;  • Підтримка контролю стану кінцевого пристрою (версія операційної системи, наявність критичних оновлень, наявність антивірусу із оновленою базою сигнатур) для операційних систем сімейства Microsoft Windows, операційних систем сімейства MacOS X, операційних систем на базі Linux з використанням агентів, що завантажуються;  Сервісна підтримка:  • Термін 12 місяців  • Включає доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника в режимі 24 х 7 з боку центру технічної підтримки виробника. | **1** |

**Технічні, якісні характеристики предмета закупівлі, повинні передбачати необхідність застосування заходів із захисту довкілля,** відповідати вимогам Законів України «Про охорону навколишнього природного середовища», «Про забезпечення санітарного та епідеміологічного благополуччя населення» та інших чинних нормативно-правових актів України з питань екологічної безпеки, охорони навколишнього природного середовища, пожежної та техногенної безпеки, охорони праці та виробничої санітарії.