Інформація на виконання постанови Кабінету Міністрів України № 1266 від 16 грудня 2020 року

Машини для обробки даних (апаратна частина) (код ДК 021:2015)-30210000-4

09.09.2021 р.

На виконання постанови Кабінету Міністрів України № 1266 від 16 грудня 2020 року, що вносить зміни до постанови КМУ від 11 жовтня 2016 року № 710 «Про ефективне використання державних коштів», ДУ «ГМЦ МВС України» (код ЄДРПОУ 08735882; адреса: вулиця Бердичівська, 1, м. Київ, 04116) надає інформацію про процедуру відкритих міжнародних торгів.

Назва предмету закупівлі: Машини для обробки даних (апаратна частина) (код ДК 021:2015)-30210000-4.

Номер процедури закупівлі у електронній системі закупівель: UA-2021-09-09-011962-c.

Закупівля здійснюється за кошти державного бюджету згідно кошторисних призначень.

Визначення очікуваної вартості закупівлі здійснено згідно проведеного інтернет моніторингу цін за предметом закупівлі, та, враховуючи потребу. Орієнтовна вартість закупівлі становить – 532 000,00 грн з ПДВ.

1. Загальні вимоги

Якість товару повинна відповідати вимогам відповідних діючих нормативних документів та відповідати параметрам та вимогам, зазначеним у цьому технічному завданні.

Товар має бути новим якісним та постачатися в оригінальній упаковці, на якій зазначається: назва товару, логотип фірми-виробника, країна виробника, умови зберігання. Всі основні компоненти товару повинні бути оригінальними, зміна компонентів на неоригінальні забороняється.

Товар повинен мати заводську упаковку та відповідне маркування. Упаковка (тара) має забезпечити захист Товару від пошкодження або псування під час транспортування та зберігання.

Учасник гарантує, що все запропоноване ним обладнання є новим та раніше не використовувалося. Усе обладнання узгоджується з усіма електричними вимогами, що встановлені в Україні (зокрема 220В, 50Гц) та забезпечене посібниками користувача та технічною документацією.

При постачанні товару Постачальник повинен дотримуватись умов «Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», затвердженої постановою Кабінету Міністрів України від 19.10.2016 № 736.

2. Вимоги до Автоматизованого робочого місця у складі: системний блок, монітор, клавіатура та миша:

1.1.Системний блок:

Параметр	**Технічні вимоги**
Живлення	• Не більше ніж 300 Вт
Процесор	• Не гірше AMD Ryzen 5 4600Gабо еквівалент
Кількість ядер процесора	• Не менше 6 ядер CPU
Базова частота процесора	• Не манше 3.7 Ghz
Тип оперативної пам'яті	• Не нижче ніж DDR-4
Об'єм оперативної пам'яті	• Не менше ніж 8 Гб
Тип жорстокого диску	• SSD

Об'єм жорсткого диску	• Не менше ніж 256 Гб
Мережеве підключення	• Наявність порту1 x RJ-45, підтримка швидкості 10/100/1000 Мбіт/с • Wi-Fi IEEE 802.11a/b/g/n/ac dual-band, 2.4 GHz та 5 GHz
Бездротовий інтерфейс (Bluetooth)	• Не нижче версії Bluetooth 5.0
Вимоги до портів	• Не менше 2-х портів USB 2.0 • Не менше 3-х портів USB 3.2 • Не менше 1-х порту USB-C • Не менше 1 x HDMI • Не менше 1 x VGA • Не менше 1 x Audio input port • Не менше 1 x Audio output port • Не менше 1 x Microphone input port • Не менше 1 x Serial port
Операційна система	• Попередньо встановлена ліцензійна ОС Microsoft Windows 10 або еквівалент, що має чинний позитивний експертний висновок щодо відповідності вимогам нормативних документів з технічного захисту інформації, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України
Гарантія	• Обладнання повинно забезпечуватись гарантією від виробника строком не менш ніж на 12 місяців

1.2. Монітор :

Параметр	Технічні вимоги
Діагональ дисплею	• Не менше 19 дюймів
Покриття екрану	• Матове
Роздільна здатність	• Не менше 1600x900 пікселів
Тип матриці	• IPS
Час реакції матриці	• Не більше 5 мс
Яскравість дисплею	• Не менше 250 кд/м^2
Співвідношення сторін	• 16:9
Коефіцієнт яскравості	• Не менше 1000:1
Частота оновлення екрану	• Не менше 60 Гц
Вхідні роз'єми	• Не менше 1 x VGA
Кути огляду по вертикалі та горизонталі	• По вертикалі – не менше 170 ° • По горизонталі – не менше 160 °
Гарантія	• Обладнання повинно забезпечуватись гарантією від виробника строком не менш ніж на 12 місяців

1.3. Клавіатура та «миша»

Вимоги до «миші»	• Провідна • Інтерфейс підключення USB

	• Мінімум дві клавіші • Обов'язково колесо прокрутки • Оптична або лазерна • Сумісність з Microsoft Windows
Вимоги до клавіатури	• Обов'язково українська розкладка • Провідна • Інтерфейс підключення – USB • Сумісність з Microsoft Windows

2. Ноутбук

Параметр	**Технічні вимоги**
Діагональ дисплею	• Не менше ніж 15 дюймів
Тип екрану	• IPS
Роздільна здатність	• Не менше 1920x1080 пікселів
Частота оновлення екрану	• Не нижче 60 Гц
Процесор	• Intel Core i3-10110U або еквівалент
Кількість ядер процесора	• Не менше ніж 2 ядра
Тип оперативної пам'яті	• Не нижче ніж DDR-4
Об'єм оперативної пам'яті	• Не менше ніж 8 Гб
Тип жорстокого диску	• SSD
Об'єм жорсткого диску	• Не менше ніж 256 Гб
Бездротовий інтерфейс (Bluetooth)	• Не нижче версії Bluetooth 5.0
Мережеве підключення	• Wi-Fi: IEEE 802.11a/b/g/n/ac, 2.4GHz та 5GHz
Вбудована відеокамера	• Так, розширення не нижче 1280x720 піскелів
Сканер відбитку пальців	• Обов'язково
Тачпад	• Обов'язково
Акумулятор (енергетична ємність), Втг	• Не менше ніж 42 Втг
Операційна система	• Попередньо встановлена ліцензійна ОС Microsoft Windows 10 або еквівалент, що має чинний позитивний експертний висновок щодо відповідності вимогам нормативних документів з технічного захисту інформації, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України
Вага	• Не більше ніж 1.53 кг
Наявність портів	• Не менше 1 - USB Type-C • Не менше 1 – USB 3.0 • Не менше 2 – USB 2.0 • Не менше 1 – HDMI • Не менше 1 – комбінований аудіороз'єм 3.5 мм jack

Гарантія	• Обладнання повинно забезпечуватись гарантією від виробника строком не менш ніж на 12 місяців

Вимоги до антивірусного програмного забезпечення

- Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
- Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп'ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
- Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.
- Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
- Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
- Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
- Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
- Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
- Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
- Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
- Забезпечення антивірусного захисту в режимі реального часу.
- Використання евристичних технологій власної розробки під час сканування.
- Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
- Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.
- Можливість сканування файлів під час запуску ОС.
- Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
- Сканування комп'ютера у неактивному стані.
- Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об'єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.
- Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
- Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.

- Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.
- Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).
- Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
- Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп'ютер від шкідливих програм і небажаної активності.
- Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.
- Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
- Автоматична антивірусна перевірка змінних носіїв.
- Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження.
- Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
- Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.
- Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
- Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
- Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
- Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
- Можливість використовувати білі та чорні списки спам-адресатів як користувальницькі (гнучка персоналізація інтелектуального спам-модулю), так і глобальні, інформація до яких надходить з серверів оновлення.
- Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».
- Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
- Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
- Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
- Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
- Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
- Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
- Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.
- Наявність у персональному брандмауеру інтерактивного режиму, що надає детальну інформацію про нове невідоме мережеве з'єднання та дає можливість не тільки створювати

на ПК нове правило мережевої фільтрації для виявленого з'єднання, а й вказувати детальні налаштування для нього.

- Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.
- Наявність редактора правил, що дає можливість не тільки редагувати створені правила, а й керувати вбудованими правилами, яких достатньо для первинного ретельного захисту від несанкціонованих мережевих з'єднань та локальних мережевих атак.
- Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.
- Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
- Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.
- Наявність додаткового функціоналу персонального брандмауеру, що дозволяє переглядати всю детальну інформацію по всіх наявних мережевих з'єднаннях, а також попереджати користувача про підключення до незахищеної мережі Wi-Fi.
- Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.
- Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
- Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
- Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE
- Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
- Наявність додаткового функціоналу персонального брандмауеру, що дає можливість переглядати на ПК перелік заблокованих IP-адрес, надає інформацію про причини потрапляння до чорного списку, та дозволяє зробити виключення для конкретних безпечних адрес.
- Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.
- Фільтрація інтернет-трафіку.
- Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
- 27 категорій фільтрації інтернет-трафіку, в яких розподілені більш ніж 100 підкатегорій, а також можливість створювати групи з категорій та підкатегорій.
- Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.
- Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.
- Регламентне оновлення вірусних баз не менше 24 разів за добу.
- Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет.
- Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
- Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
- Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.

- Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
- Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
- Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
- Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
- Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
- Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
- Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
- Локальне зберігання журналів на робочих станціях.
- Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів програми.
- Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
- Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
- Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
- Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
- Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.
- Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
- Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
- Можливість віддаленого встановлення на клієнтську робочу станцію
- Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
- Можливість крім основного вказати резервні сервери адміністрування.
- Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
- Підтримка ОС: Microsoft Windows XP Professional; Microsoft Windows Vista (Professional або вище); Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10.
- Запропоноване ПЗ повинне забезпечуватись в Україні технічною підтримкою, яка працює в режимі 24x7x365, з можливістю зв'язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку).

Строк поставки товару – до 25.12.2021 року.

Місце поставки: вулиця Бердичівська, 1, м. Київ, 04116.

Уповноважена особа **Юлія СТЕЛЬНИКОВИЧ**