НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ОБҐРУНТУВАННЯ

технічних та якісних характеристик **закупівлі комп'ютерного обладнання,** 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: Національна академія внутрішніх справ;
03035, м. Київ, пл. Солом'янська, 1;
код за ЄДРПОУ – 08751177;

Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі й частин предмета закупівлі (лотів) (за наявності): Комп'ютерне обладнання (Код ДК 021:2015 – 30230000-0 Комп'ютерне обладнання)

Вид та ідентифікатор процедури закупівлі: UA-2023-06-16-012986-a.

Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі: 1 970 000,00 грн. 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 III наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 із змінами.

Розмір бюджетного призначення: 1 970 000,00 грн згідно з розрахунком до кошторису.

Обґрунтування технічних та якісних характеристик предмета закупівлі.

Придбання комп'ютерного обладнання здійснюється відповідно до наявної потреби для забезпечення безперебійної та високошвидкісної роботи освітньої діяльності, а також чіткого та вчасного завершення наукового та освітнього плану Національної академії внутрішніх справ на 2022-2023 роки. Сучасне обладнання дасть можливість модернізувати матеріально-технічну базу академії; створити комфортні умови для якісного виконання наукових та освітніх процесів; підвищити ефективність праці науково-педагогічному складу

Якісні та технічні характеристики заявленої кількості техніки визначені з урахуванням реальних потреб НАВС та оптимального співвідношення ціни та якості для удосконалення навчального процесу.

№ п/п	Характеристика товару	Од. виміру	Кіль-кість
1	**Програмно-апаратний комплекс для відеомонтажу та обробки відеоматеріалів під час навчального процесу:** Колір – сріблястий або сірий або темного кольору; Процесор: Базова частота – не менше 2,3 ГГц; Максимальна частота – не менше 4,3 ГГц; кількість ядер - не менше ніж 6; потоків не менше 12; з продуктивністю не менше ніж 15100 балів в тестуванні багатопотоковості CPU Mark (www.cpubenchmark.net) на сайті PassMark (www.passmark.com). Оперативна пам'ять - Не менше 16 ГБ DDR4 3200 МГц не впаяної пам'яті або краще, з можливістю розширення до 32 GB (наявність додатково слоту SODIMM). Відеокарта - Інтегрований або дискретний відеоадаптер. Жорсткий диск - SSD, Інтерфейс – не гірше PCIe NVMe, Ємність не менше 512 ГБ. Мережева карта - З'єднування RJ-45; швидкість передачі, що підтримується – 10/100/1000 Мб/с. Звукова карта - Інтегрований HD-Audio або еквівалент. Порти вводу/виводу - Не менше ніж 1x USB Type-C (Power Delivery та DisplayPort)/ 3 x USB 3.2 Type-A / HDMI / LAN (RJ-45) / комбінований аудіороз'єм для	шт	40

	наушників/микрофона. Бездротовий інтерфейс (Wi-Fi) - Обов'язково у наявності, 2,4/5 ГГц, не гірше Wi-Fi 6, Bluetooth 5.3 Веб-камера - Обов'язково у наявності, не гірше HD. Інші елементи - Вбудовані динаміки, вбудований мікрофон, комбінований роз'єм для мікрофона/навушників (3,5 мм), Bluetooth версії не гірше 5.X. Блок живлення та батарея - Обов'язково у комплекті. Батарея літій-іонна, ємністю не менше 42 Вт*год, максимальний час роботи батареї не менше 16 годин Пристрої введення - Клавіатура повинна мати Англ./ кириличні символи. Захист від проливу рідини. Тачпад обов'язково у наявності. Розмір дисплея: не менше 15 дюймів з антибліковим покриттям. Технологія матриці дисплея - IPS або аналог. Роздільна здатність дисплея - Не менше 1920x1080 точок (Full HD). Програмне забезпечення - Встановлена виробником операційна система Windows 10 Pro (64Bit) Української редакції з можливістю безкоштовного переходу на Windows 11 Pro. Безпека - Trusted Platform Module або еквівалент; наявність можливості відключення портів USB в BIOS; Наявність сканеру відбитку пальців (FPS). Вага - Не більше 1.8 кг. **<u>Антивірусне програмне забезпечення для захисту робочих станцій під управлінням несерверних ОС (примірні функціональні можливості):</u>** 1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ. 2. 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. 3. 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. 4. 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. 5. 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. 6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в ОС. 7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. 8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи. 9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС. 10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. 11. Забезпечення антивірусного захисту в режимі реального часу. 12. Використання евристичних технологій власної розробки під час сканування. 13. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 14. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. 15. Можливість сканування файлів під час запуску ОС.		

	16. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін. 17. Сканування комп'ютера у неактивному стані. 18. 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. 19. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування 20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення. 21. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо. 22. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware). 23. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами. 24. 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. 25. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру. 26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. 27. Автоматична антивірусна перевірка змінних носіїв. 28. 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. 29. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою. 30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв. 31. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену. 32. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв. 33. 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. 34. 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». 35. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах. 36. Перевірка дійсності та цілісності сертифікатів SSL-трафіку. 37. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим. 38. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер. 39. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет" 40. Наявність упроваджених методів виявлення різноманітних атак, що		

	намагаються використовувати вразливості ПЗ та надання докладнішої інформації про ідентифікатори CVE. 41. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання. 42. Регламентне оновлення вірусних баз не менше 24 разів за добу. 43. 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. 44. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок. 45. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне. 46. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею. 47. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну. 48. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. 49. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС. 50. 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. 51. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі. 52. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час. 53. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання. 54. Локальне зберігання журналів на робочих станціях. 55. 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. 56. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій. 57. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 58. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом. 59. Можливість захисту паролем параметрів рішення для захисту кінцевої точки. 60. 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. 61. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності. 62. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача. 63. Можливість крім основного вказати резервні сервери адміністрування. 64. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову. 65. Підтримка ОС: Microsoft Win 11, Win 10, 8.1, 8, 7 (SP1+KB). <u>Вимоги до інструменту віддаленого управління антивірусними рішеннями:</u> 1. Можливість централізованого управління антивірусним захистом всієї		

	мережевої інфраструктури. 2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати централізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам. 3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно. 6. Віддалена інсталяція користувальницького програмного забезпечення. 7. Можливість віддаленого видалення встановленого користувальницького ПЗ. 8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac 9. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера. 10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування. 11. Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захисту. 12. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління. 13. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування. 14. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів. 15. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань. 16. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю. 17. Можливість використовувати як вбудовані, так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик. 18. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування. 19. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів. 20. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту. 21. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL. 22. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.		

	23. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів. 24. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу. 25. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів. 26. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом. 27. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи. 28. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором. 29. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях 30. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту. 31. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів. 32. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування). 33. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу 34. Можливість встановлення серверу адміністрування на ОС Windows та Linux. 35. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії. 36. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому. 37. Можливість встановлення агенту управління на ARM64 процесорах. 38. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям. 39. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії. Термін підписки антивірусної програми: не менше 12 місяців Гарантійний термін: не менше 12 місяців.		
2	**<u>Багатофункціональний пристрій формату А4:</u>** Тип - Монохромний лазерний багатофункціональний пристрій. Функціонал - друк, копіювання, сканування. Максимальний формат друку - А4. Швидкість друку - не менше ніж 18 сторінок за хвилину формату А4. Роздільна здатність друку - не менше ніж 600х400 точок на дюйм. Якість друку - не менше ніж 1200 х 600 точок на дюйм. Час виходу першої сторінки - не більше 8 секунд. Загальна ємність лотка (або лотків) подачі паперу не менше 150 аркушів А4 80 г/м2; Тип паперу: А4, А5, щільністю 60–163 г/м2. Роздільна здатність сканування (оптична) - не менше ніж 600х600 точок на дюйм. Швидкість копіювання (А4): не менше ніж 18 сторінок за хвилину. Операційні системи які підтримуються - обов’язково: Windows 10 та 11. Інтерфейс - не менше: USB 2.0 Hi-Speed. Витратні матеріали - обов’язково: оригінальний картридж (або комплект картриджів) загальним обсягом не менш ніж 3,900 аркушів (5% покриття, А4) у комплекті; Гарантійний термін: не менше 24 місяці від виробника.	шт	20
3	**<u>Принтер:</u>** Технологія друку: лазерний, монохромний; Формат друку: А4; Загальна ємність лотка (або лотків) подачі паперу не менше 350 аркушів А4 80 г/м2ж; Швидкість друку: не менша ніж 38 стор./хв. (А4); не менше ніж 31 стор./хв (А4, duplex); Розширені функції друку: дуплексний друк;	шт	10

	Роздільна здатність під час друку: не менша ніж 1200×1200 dpi Час друку першої сторінки: не більше 5,5 сек.; Прямий друк документів із USB-накопичувача (JPEG/TIFF/PDF) Інтерфейс і підключення: USB 2.0 High-Speed, 10Base-T/100Base-TX/1000Base-T, бездротове підключення 802.11b/g/n, підключення Wireless Direct; Оперативна пам'ять: не менше 1 ГБ; Рекомендований щомісячний обсяг друку: 750-4000 сторінок на місяць; Максимальний щомісячний обсяг друку: не менше 80000 сторінок на місяць; Друк із захистом PIN-кодом – так Витратні матеріали: - повинен бути укомплектований оригінальним картриджем ємністю не менш ніж 1500 сторінок; Гарантійний термін: не менше 24 місяці від виробника.		