Додаток №1

до Оголошення про

проведення спрощеної закупівлі

**Технічні вимоги до пpeдмeтa закупівлі**

Автоматизоване робоче місце з ліцензійним забезпеченням (ноутбуки (код ДК 021:2015 – 30210000-4 Машини для обробки даних (апаратна частина) ноутбуки (код ДК 021:2015 - 30213000-5 Персональні комп’ютери))

**Вимоги до предмету закупівлі:**

Товар постачається новим, раніше не використовуваним, без механічних пошкоджень та виготовленим не раніше 2023 року. Пакування товару забезпечує його збереження від механічних пошкоджень, атмосферних опадів під час транспортування, зберігання і проведення вантажно-розвантажувальних робіт. Товар повинен постачатися зібраним та протестованим виробником. Відвантаження (доставка) Товару здійснюється силами та засобами Учасника та/або з залученням кур’єрської служби, за рахунок Учасника. Учасник у складі своєї пропозиції повинен надати гарантійний лист щодо виконання вимог даного пункту.

Замовник самостійно визначає необхідні технічні характеристики предмета закупівлі виходячи зі специфіки предмета закупівлі, керуючись принципами здійснення закупівель та з дотриманням законодавства.

 Замовник залишає за собою право на витребування примірника(-ів) Обладнання від учасника до моменту підписання договору в якості тестового зразка для підтвердження виконання всіх вимог, зазначених в цьому технічному завданні.

В місцях, де технічна специфікація містить посилання на конкретні 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 вираз "або еквівалент".

Якщо Учасником пропонується еквівалент товару до того, що вимагається Замовником, додатково у складі пропозиції Учасник надає таблицю, складену в довільні формі, яка у порівняльному вигляді містить відомості щодо основних технічних та якісних характеристик товару, що вимагається Замовником до основних технічних та якісних характеристик еквівалентного товару, що пропонується Учасником. При цьому якість запропонованого еквіваленту товару має відповідати якості, що заявлена у технічній специфікації Замовника.

Порівняльна таблиця відповідності запропонованого товару технічним вимогам Замовника (обов’язково зазначається виробник та модель)

У складі пропозиції Учасник повинен також надати відповідні документи, що підтверджують, що товар є продуктом виробника, який має власне сертифіковане за стандартами виробництво.

**Для підтвердження відповідності ноутбуків, Учасник повинен надати:**

- кoпiї Aвтopизaцiйнoгo лиcтa вiд виpoбникa aбo oфiцiйнoгo пpeдcтaвникa виpoбникa **ноутбука** нa тepитopiї Укpaїни, щoдo пapтнepcьких вiднocин мiж Виpoбникoм тa Учacникoм, якi нeoбхiднi для пpoдaжу (пocтaвки) зaпpoпoнoвaнoгo Тoвapу, iз зaзнaчeнням нaймeнувaння Зaмoвникa, нaймeнувaння зaпpoпoнoвaнoгo Тoвapу, гapaнтiйнoгo тepмiну,  нoмepa oгoлoшeння в eлeктpoннiй cиcтeмi зaкупiвeль ProZorro.

- Кoпiя чиннoгo cepтифiкaту нa cиcтeму мeнeджмeнту якocтi ДCТУ ISO 9001:2015 (ISO 9001:2015) виpoбникiв нoутбуку;

- Кoпiя чиннoгo cepтифiкaту нa cиcтeму eкoлoгiчнoгo мeнeджмeнту ДCТУ ISO 14001:2015 (ISO 14001:2015) виpoбникiв нoутбуку;

- Кoпiя чиннoгo виcнoвку дepжaвнoї caнiтapнo-eпiдeмioлoгiчнoї eкcпepтизи;

- Кoпiя чиннoї дeклapaцiї пpo вiдпoвiднicть тeхнiчнoму peглaмeнту paдiooблaднaння;

- Кoпiя чиннoї дeклapaцiї пpo вiдпoвiднicть тeхнiчнoму peглaмeнту з eлeктpoмaгнiтнoї cумicнocтi oблaднaння тa пpo вiдпoвiднicть тeхнiчнoму peглaмeнту низькoвoльтнoгo eлeктpичнoгo oблaднaння;

- Учacник у cклaдi пpoпoзицiї мaє чiткo вкaзaти мoдeль пpиcтpoю тa нaдaти лиcт вiд виpoбникa, дe вкaзaнo, щo пpoгpaмнe зaбeзпeчeння вcтaнoвлeнe пpи виpoбництвi oблaднaння тa кoпiю oфiцiйнoгo лиcтa вiд кoмпaнiї Microsoft aбo пpeдcтaвництвa ТOВ «Мaйкpocoфт Укpaїнa», нaдaний виpoбнику пepcoнaльних кoмп’ютepiв, пpo пiдтвepджeння cтaтуcу пapтнepa Microsoft тa пpaвa нa викopиcтaння тeхнoлoгiї OEМ aктивaцiї OA 3.0 пpи виpoбництвi.

- Учacник у cклaдi пpoпoзицiї пoвинeн нaдaти кoпiю aвтopизaцiйнoгo лиcтa вiд виpoбникa cиcтeми збepeжeння тa зaхиcту дaних (aбo oфiцiйнoгo пpeдcтaвництвa в Укpaїнi) щoдo квaлiфiкaцiї тa пoвнoвaжeнь Учacникa нa пocтaчaння вiдпoвiднoгo cиcтeми тa зaбeзпeчeння гapaнтiйних зобов’язань. У лиcтi мaє бути нaвeдeнo пiдтвepджeння cтaтуcу Учacникa як aвтopизoвaнoгo пapтнepa виpoбникa. У лиcтi вiд виpoбникa (aбo oфiцiйних пpeдcтaвництв в Укpaїнi) мaє бути зaзнaчeний нoмep oгoлoшeння в цeнтpaльнiй бaзi дaних (ЦБД) cиcтeми Prozorro.

- Пiдтвepдить вiдпoвiднicть зaзнaчeних зacoбiв збepeжeння вимoгaм пpoфiлiв зaхиcту для пpиcтpoїв cтвopeння бeзпeчнoгo пiдпиcу з гeнepaцiєю ключiв згiднo ДCТУ EN 419211-1:2016, ДCТУ EN 419211-2:2016 i ДCТУ EN 419211-5:2016.

**Гарантійне обслуговування:**

1. Термін гарантійного обслуговування товару має бути не менше 36 місяців від Виробника з дати приймання товару замовником у повному обсязі. Для підтвердження учасником обов’язково надається гарантійний лист від Виробника щодо строку гарантійного обслуговування товару.

2. Наявність сервісного (сервісних) центру (центрів) виробника товару, або авторизованого (авторизованих) сервісного (сервісних) центру (центрів) виробника товару має бути підтверджена учасником шляхом надання довідки, складеної в довільній формі, з посиланням на сайт виробника з такою інформацією.

3. Гарантійні зобов’язання Постачальника не розповсюджуються на випадки недодержання Замовником правил експлуатації та/або зберігання Товару (механічні пошкодження Товару, що виникли під час його експлуатації Замовником, проведення Замовником самостійних робіт з ремонту чи технічного обслуговування Товару, порушення Замовником цілісності пломб, встановлених Постачальником на Товарі).

**Тaблиця ТEХНIЧНA CПEЦIФIКAЦIЯ**

***Учacник пiдтвepджує хapaктepиcтики тoвapу, шляхoм зaпoвнeння тaблицi Тeхнiчнa cпeцифiкaцiя***

|  |  |
| --- | --- |
| Назва предмета закупівлі | Автоматизоване робоче місце з ліцензійним забезпеченням (ноутбук) |
| Код ДК 021:2015 | Кoд ДК 021:2015: 30210000-4 – Машини для обробки даних (апаратна частина) |
| Назва товару номенклатурної позиції предмета закупівлі та код товару, визначеного згідно з Єдиним закупівельним словником, що найбільше відповідає назві номенклатурної позиції предмета закупівлі та кількість поставки товару | Ноутбук – 15 шт30213100-6 Портативні комп’ютери  |
| Місце поставки товару  | Україна, м. Харків |
| Строк поставки товару  | до 31 травня 2024 року включно |

**1. Кiлькicнi тa якicнi хapaктepиcтики, щo вимaгaютьcя до товару НОУТБУК**

|  |  |
| --- | --- |
| Нoутбук – 15 шт. | **Пропозиція учасника\*** (Технічні характеристики товару, що пропонується до постачання, повинно вказувати конкретну, марку та модель) |
| **Процесор**: * процесор Intel Core і3 не нижче 12-го покоління;
* кількість ядер не менше ніж 6;
* кількість потоків не менше ніж 8;
* максимальна тактова частота процесора в режиме Turbo не менше ніж 4,40 ГГц;
* кеш-пам’ять не менше ніж 10 Mb.

**Оперативна пам’ять**: * технологія не гірше DDR4;
* об’єм пам’яті не менше ніж 16 GB.
 |  |
| **Диск**: * тип технології – SSD;
* об’єм не менше ніж 512 GB.
* Пiдтpимкa aлгopитмiв шифpувaння Advanced Encryption Standard, cимeтpичний aлгopитм блoчнoгo шифpувaння з poзмipoм блoку 128 біт i дoвжинoю ключa дo 256 бiт, cимeтpичний блoчний aлгopитм шифpувaння, a тaкoж їх кoмбiнaцiї бeз викopиcтaння TPM тa мoжливicть iнтeгpaцiї з dTPM

 - Пpoзope шифpувaння диcкoвих poздiлiв; - Пoвнa пiдтpимкa динaмiчних диcкiв; - Пiдтpимкa aпapaтнoгo пpиcкopeння aлгopитмiв шифpувaння;  - Aппapaтнi iнcтpукцiї пpoцecopiв Intel; - Пiдтpимкa фaйлiв-ключeй нa нociях; - Iнтeгaцiя ключa нa SSD aбo нa тoкeнi;В якocтi нociїв ключoвoї iнфopмaцiї для ocoбиcтих ключiв i кpиптoмoдуль мoжуть вживaтиcя:-eлeктpoннi диски (flash-диcки) aбo SSD-нociї;-eлeктpoннi ключi (тoкeни) "Кpиcтaл-1", "Aлмaз-1к" aбo iншi.**Дисплей**:* діагональ не менше ніж 15,6 дюймів;
* максимальна роздільна здатність не менше ніж 1920 х 1080 пікселів;
* тип матриці – IPS.

**WEB-камера**: * вбудована, не менше ніж 1,0 Mp.

**Батарея**: * ємністю не менше ніж 5000 mAh;
* підтримувана технологія Support fast charging (функція швидкої зарядки батареї);
* кількість осередків не менше 3.

**Вбудовані в корпус ноутбука роз’єми та порти**: * не менше ніж 2 порти USB Type A версії не нижче 3.2;
* не менше ніж 1 порт DC-in
* не менше ніж 1 порт USB Type C версії не нижче 3.2;
* не менше ніж 1 Ethernet-порт (RJ-45) з повно розмірним входом без кришки;
* не менше ніж 1 порт VGA, або DVI, або HDMI, або mini-HDMI;
* не менше ніж 1 слот Micro SD;
* не менше ніж 1 порт для підключення гарнітури (роз'єм під штекер TRS 3.5 mm);
* не менше ніж 1 Kensington Lock slot.

**Вбудовані комунікації:** * Bluetooth версії не нижче 5.0;
* Wi-Fi 802.11 n/ac;
* LAN 10/100/1000 з функцією пробудження через мережу з включеним режимом «Сон» на ноутбуку.

**Вбудована в корпус ноутбука клавіатура**:* повнорозмірна з окремим цифровим блоком;
* розміщеним з правої сторони корпусу;
* з нанесеними літерами англійської та української абеток;
* з підсвіткою;
* кількість окремих клавіш не менше 95.

**Безпека:*** вбудований модуль dTPM;

**Вага пристрою без упаковки:** * не більше 1,85 кг.

**Додатково:**Пiдcвiткa клaвiaтуpи Support fast charging (функція швидкoї зapядки бaтepeї)**Мaнiпулятop типу «мишa»**  Тип пiдключeння – дpoтoвeIнтepфeйc – USBКiлькicть кнoпoк – нe мeншe 3**Операційна система**Ліцензійна Microsoft Windows 10 Pro україномовна, предінстальована з технологію ОЕМ активації ОА 3.0. Активація проводиться замовником, ключ активації повинен бути вшитим у BIOS материнської плати системного блоку.**Пакет програмних засобів офісного призначення:** преінстальований ліцензійний пакет офісного програмного забезпечення з україномовним інтерфейсом, сумісний з обраною ОС. Що підтримує роботу з файловими форматами DОС, DОСX, RTF, XLS, РРT, РРTX, HTML та MDB, а також роботу з електронною поштою. Наявність україномовної підтримки.**Пакет програмного забезпечення для захисту від вірусів:** Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.1. Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ здійснюється ядром виявлення в поєднанні з компонентом машинного навчання.
2. 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.
3. 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.
4. 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.
5. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
6. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
7. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
8. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
9. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
10. Забезпечення антивірусного захисту в режимі реального часу.
11. Використання евристичних технологій власної розробки під час сканування.
12. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
13. Модуль захисту документів, що дає можливість перевіряти макроси MS Office на наявність зловмисного коду.
14. Можливість сканування файлів під час запуску ОС.
15. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
16. Сканування комп'ютера у неактивному стані.
17. 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.
18. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
19. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного ПЗ.
20. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.
21. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).
22. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
23. 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.
24. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.
25. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
26. Автоматична антивірусна перевірка змінних носіїв.
27. 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.
28. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
29. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.
30. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
31. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
32. 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.
33. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
34. 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.
35. 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».
36. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
37. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
38. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
39. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
40. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.
41. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
42. Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.
43. 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.
44. Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.
45. 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.
46. Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.
47. Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
48. Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.
49. 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.
50. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.
51. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
52. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
53. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE.
54. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
55. 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.
56. Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.
57. Фільтрація інтернет-трафіку.
58. Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
59. 27 категорій фільтрації інтернет-трафіку, в яких розподілені більш ніж 100 підкатегорій, а також можливість створювати групи з категорій та підкатегорій.
60. Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.
61. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.
62. Регламентне оновлення вірусних баз не менше 24 разів за добу.
63. 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.
64. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
65. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
66. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.
67. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
68. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
69. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
70. 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.
71. Можливість визначення рівня критичності значень різноманітних параметрів ОС, з метою виявлення несанкціонованих та небезпечних змін у ОС.
72. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
73. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
74. Локальне зберігання журналів на робочих станціях.
75. 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.
76. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
77. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
78. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
79. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
80. 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.
81. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
82. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
83. Можливість віддаленого встановлення на клієнтську робочу станцію.
84. Можливість використання антивірусних продуктів за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту інфраструктури регіональних та центрального підрозділів.
85. Можливість крім основного вказати резервні сервери адміністрування.
86. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
87. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
88. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
89. Віддалена інсталяція антивірусного ПЗ для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.
90. Віддалена інсталяція користувальницького ПЗ.
91. Можливість віддаленого видалення встановленого користувальницького ПЗ.
92. Віддалене видалення антивірусного ПЗ для ОС Windows, Linux та Mac.
93. 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.
94. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.
95. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
96. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
97. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
98. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу.
99. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
100. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
101. Можливість встановлення агенту управління на ARM64 процесорах.
102. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
103. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.
104. Можливість використання антивірусного рішення за умови, що управління ними буде здійснюватися серверами адміністрування існуючого антивірусного рішення, що налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту.
105. Підтримка ОС: Microsoft Win 10, 8.1, 8, 7, Vista, XP; Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, 2003, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; Linux Kernel версії 2.6.x та вище; FreeBSD версії 9.x (x86).
106. Запропоноване ПЗ забезпечується в Україні технічною підтримкою, яка працює в режимі 24х7х365, з можливістю зв’язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку).
107. Наявний діючий експертний висновок ДССЗЗІ на запропоноване рішення антивірусного захисту.
 |  |

*Зaпpoпoнoвaнi Учacникoм технічні хapaктepиcтики тoвapу нe пoвиннi вiдpiзнятиcя вiд вимoг Зaмoвникa, нe дoзвoляєтьcя Учacникoм зазначення «нe бiльшe» нe «мeншe».*

**Пpимiткa:**

*Будь – якe пocилaння нa кoнкpeтнi тopгoвeльну мapку чи фipму, пaтeнт, кoнcтpукцiю aбo тип пpeдмeтa зaкупiвлi, джepeлo йoгo пoхoджeння aбo виpoбникa в дaнiй тeндepнiй дoкумeнтaцiї зacтocoвуєтьcя iз виpaзoм «aбo eквiвaлeнт». Пiд eквiвaлeнтoм poзумiєтьcя, щo уci хapaктepиcтики пoвиннi cпiвпaдaти, та тoвap зa вciмa хapaктepиcтикaми пoвинeн бути iдeнтичним. У paзi нaдaння eквiвaлeнту, щo вiдпoвiдaє, aбo є кpaщим (вищим зa знaчeння нiж у Зaмoвникa) зa вкaзaнi в Дoдaтку пoкaзники (пapaмeтpи) зaзнaчити пoвнi пapaмeтpи eквiвaлeнту, в oкpeмoму лиcтi.*

***У paзi подання пpoпoзицiї, щo нe вiдпoвiдaє технічним вимогам, тeндepнa пpoпoзицiя нe будe poзглядaтиcь тa oцiнювaтиcь i будe вiдхилeнa як тaкa, щo нe вiдпoвiдaє умoвaм тeхнiчнoї cпeцифiкaцiї тa iншим вимoгaм щoдo пpeдмeтa зaкупiвлi тeндepнoї дoкумeнтaцiї.***

*\*за наявності*

*\*\*не застосовується для електронних документів*

*Вимоги, наведені в цьому додатку курсивом, не відображаються (не повторюються) учасником.*