ОГОЛОШЕННЯ

про проведення відкритих торгів
UA-2022-11-30-008519-a

Найменування замовника:	ДП "УКРМЕТРТЕСТСТАНДАРТ"
Категорія замовника:	Юридична особа, яка забезпечує потреби держави або територіальної громади
Ідентифікаційний код замовника в ЄДР:	02568182
Місцезнаходження замовника:	03143, Україна, Київська область, Київ, м.Київ, ВУЛИЦЯ МЕТРОЛОГІЧНА, будинок 4
Контактна особа замовника, уповноважена здійснювати зв'язок з учасниками:	Крутов Сергій Леонідович, 380445260116, KRUTOFF@UKRCSM.KIEV.UA
Вид предмета закупівлі:	Товари
Назва предмета закупівлі:	48760000-3 Пакети програмного забезпечення для захисту від вірусів (програмна продукція ESET PROTECT Entry з локальним управлінням на 1 рік для захисту 500 об'єктів (або еквівалент)
Код за Єдиним закупівельним словником:	ДК 021:2015:48760000-3: Пакети програмного забезпечення для захисту від вірусів

Назва номенклатурної позиції предмета закупівлі	**Код згідно з Єдиним закупівельним словником, що найбільше відповідає назві номенклатурної позиції предмета закупівлі**	**Кількість товарів або обсяг виконання робіт чи надання послуг**	**Місце поставки товарів або місце виконання робіт чи надання послуг**	**Строк поставки товарів, виконання робіт чи надання послуг**
48760000-3 Пакети програмного забезпечення для захисту від вірусів (програмна продукція ESET PROTECT Entry з локальним управлінням на 1 рік для захисту 500 об'єктів (або еквівалент)	ДК 021:2015: 48760000-3 — Пакети програмного забезпечення для захисту від вірусів	500 штуки	03143, Україна, Київська область, Київ, м.Київ, ВУЛИЦЯ МЕТРОЛОГІЧНА, будинок 4	до 31 березня 2023

Умови оплати:

Подія	Опис	Тип оплати	Період, (днів)	Тип днів	Розмір оплати, (%)
Дата виставлення рахунку		Аванс	10	Банківські	30
Поставка товару		Післяоплата	10	Банківські	70

Очікувана вартість предмета закупівлі: 340 000,00 UAH

Розмір мінімального кроку пониження ціни: 1 700,00 UAH

Математична формула для розрахунку приведеної ціни (у разі її застосування): відсутня

Кінцевий строк подання тендерних пропозицій: 08 грудня 2022 16:00

Мова тендерної пропозиції: українська

Розмір забезпечення тендерних пропозиції (якщо замовник вимагає його надати): відсутній

Вид забезпечення тендерних пропозиції (якщо замовник вимагає його надати): відсутній

Дата та час розкриття тендерних пропозицій: 08 грудня 2022 16:00

Дата та час проведення електронного аукціону: 09 грудня 2022 12:22

Додаток

Обґрунтування технічних, якісних та кількісних характеристик предмета закупівлі.

Технічні та якісні характеристики:

Вимоги до технічної підтримки
1. Запропонована антивірусна ПП повинна мати авторизований виробником центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог: - обслуговування 24x7x365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні; - розширені технічні консультації з питань конфігурації та функціонування антивірусної ПП по телефону (з можливостю зв'язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв'язку) та електронній пошті;
Вимоги до рішення для захисту робочих станцій під управління несерверних ОС:
2. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ. 3. 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. 4. 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. 5. 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. 6. 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. 7. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі. 8. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. 9. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи. 10. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС. 11. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. 12. Забезпечення антивірусного захисту в режимі реального часу. 13. Використання евристичних технологій власної розробки під час сканування. 14. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 15. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. 16. Можливість сканування файлів під час запуску ОС. 17. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін. 18. Сканування комп'ютера у неактивному стані.

19. 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.

20. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування

21. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.

22. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.

23. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).

24. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.

25. 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.

26. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.

27. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

28. Автоматична антивірусна перевірка змінних носіїв.

29. 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.

30. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.

31. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.

32. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.

33. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.

34. 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.

35. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.

36. 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».

37. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.

38. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

39. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.

40. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.

41. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .

42. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).

43. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.

44. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"

45. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.

46. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE

47. Регламентне оновлення вірусних баз не менше 24 разів за добу.

48. 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.

49. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.

50. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.

51. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.

52. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.

53. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.

54. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.

55. 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.

56. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.

57. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.

58. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.

59. Локальне зберігання журналів на робочих станціях.

60. 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.

61. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.

62. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

63. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.

64. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.

65. 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.

66. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.

67. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.

68. Можливість віддаленого встановлення на клієнтську робочу станцію

69. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.

70. Можливість крім основного вказати резервні сервери адміністрування.

71. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.

72. 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; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit, Ubuntu Desktop 20.04 LTS, Red Hat Enterprise Linux 7 та 8, SUSE Linux Enterprise Desktop 15.

73. Наявність експертного висновку Державної служби спеціального зв'язку та захисту інформації, що засвідчує відповідність програмного продукту (продукції) захисту інформації, вимогам нормативних документів з технічного захисту інформації (дійсний не менше ніж період використання ліцензії на програмну продукцію).

Вимоги до рішення для захисту робочих станцій під управління серверних ОС:

74. Підтримка ОС: Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; Linux Kernel версії 2.6.x та вище; FreeBSD версії 9.x (x86).

75. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.

76. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.

77. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.

78. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.

79. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.

80. Можливість сканування файлів під час запуску ОС.

81. Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.

82. Сканування комп'ютера у неактивному стані.

83. 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.

84. Автоматична антивірусна перевірка змінних носіїв.

85. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.

86. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows.

87. Наявність системи виявлення вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру.

88. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень.

89. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.

90. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.

91. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).

92. Регламентне оновлення вірусних баз не менше 24 разів за добу.

93. Можливість крім основного вказати резервні сервери адміністрування.

94. Наявність механізму контролю за актуальністю оновлень ОС.

95. 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. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання.

96. 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 та за умови виникнення конкретних подій.

97. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

98. Можливість роботи в кластерах як домена так і робочої групи.

99. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.

100. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.

101. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.

102. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.

103. Можливість захисту від зміни параметрів антивірусного ПЗ паролем.

104. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.

Вимоги до інструменту віддаленого управління антивірусними рішеннями:

105. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.

106. 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.

107. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.

108. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.

109. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.

110. Віддалена інсталяція користувальницького програмного забезпечення.

111. Можливість віддаленого видалення встановленого користувальницького ПЗ.

112. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac

113. 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.

114. 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.

115. 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.

116. Можливість аутентифікувати адміністраторів ERA за допомогою груп безпеки AD.

117. Можливість використовувати двохфакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.

118. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.

119. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів.

120. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.

121. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.

122. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.

123. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.

124. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.

125. 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.

126. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.

127. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.

128. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.

129. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.

130. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.

131. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом.

132. 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.

133. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.

134. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях

135. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту.

136. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.

137. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування).

138. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу

139. Можливість встановлення серверу адміністрування на ОС Windows та Linux.

140. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).

141. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+.

142. Можливість обирати варіанти обробки ідентифікаторів клонованих комп'ютерів, такі як зіставляння з наявними комп'ютерами або створення нових комп'ютерів.

143. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.

144. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну ідентифікацію клонованих машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.

145. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.

146. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.

147. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.

148. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

149. Можливість встановлення агенту управління на ARM64 процесорах.

Кількісні характеристики:

Надання захисту робочих місць та серверів загальною кількістю 500 од.

Обгрунтування:

Закупівля необхідна для забезпечення якісного антивірусного захисту робочих місць структурних підрозділів підприємства , серверів доступу до мережі ІНТЕРНЕТ, сервісу електронної пошти, за адресами м. Київ, вул. Метрологічна, 4 та вул. Краснова, 7/1.

Начальник відділу № 16 _____ Андрій КАТАШ

(підпис)

Обгрунтування очікуваної вартості предмету закупівлі

код ДК 021:2015 - 48760000-3

Пакети програмного забезпечення для захисту від вірусів

(***Програмна продукція 'ESET PROTECT Entry з локальним управлінням'. На 1 рік. Для захисту 500 об'єктів.*** *(або еквівалент)*)

Для розрахунку очікуваної вартості використаємо метод порівняння ринкових цін. Ціни на послуги візьмемо з запитів постачальників аналогічних послуг.

Маємо 3 комерційні пропозиції:

	НАЙМЕНУВАННЯ	ВАРТІСТЬ, грн з ПДВ
1.	ТОВ «ДАТАСТРІМ»	340 000,00
2.	ПрАТ «АРКАДА»	340 000,00
3.	ТОВ ««Ай Ті Про»	340 000,00

Ціни актуальні станом на 11.02.2022р

Визначимо очікувану вартість предмету закупівлі за формулою:

$$Цод = (Ц1+Ц2+ Ц3)/3$$

Очікувана вартість предмету закупівлі складає:

$$Цод = (340\,000{,}00 + 340\,000{,}00 + 340\,000{,}00)/3$$

$$= 340\,000{,}00 \text{ грн, з ПДВ}$$

Начальник відділу №16 Андрій КАТАШ