Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі (Послуги з подовження ліцензій на право використання антивірусного програмного забезпечення (Пакети антивірусного програмного забезпечення)).

Замовник: Головне управління Держпродспоживслужби у Вінницькій області
Предмет Закупівлі: Послуги з подовження ліцензій на право використання антивірусного програмного забезпечення (Пакети антивірусного програмного забезпечення).
Очікувана вартість предмета закупівлі: 251 500,00 грн. з ПДВ.
Ідентифікатор закупівлі: UA-2023-09-05-004447-a.
На виконання вимог постанови Кабінету Міністрів України від 11 жовтня 2016 р. № 710 (зі змінами) розпорядником бюджетних коштів з метою прозорого, ефективного та раціонального використання коштів забезпечено:

- обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі;
- оприлюднення обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі шляхом розміщення на власному веб-сайті протягом п’яти робочих днів з дня оприлюднення оголошення про проведення конкурентної процедури закупівель або повідомлення про намір укласти договір про закупівлю за результатами переговорної процедури закупівель.

Обґрунтування технічних та якісних характеристик предмета закупівлі

З метою забезпечення антивірусного захисту робочих станцій Головного управління Держпродспоживслужби у Вінницькій області до предмету закупівлі висуваються наступні вимоги:

1. Місце поставки послуг: м.Вінниця, вул.Праведників світу, 19.

Технічні вимоги до антивірусного програмного забезпечення для захисту робочих станцій під керуванням ОС Microsoft Windows

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 операційній системі.
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. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
35. Наявність модуля захисту від спаму власної розробки з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
36. 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.
37. 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».
38. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
39. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
40. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
41. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
42. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
43. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
44. Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.
45. 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.
46. Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.
47. 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.
48. Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.
49. Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
50. Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.
51. 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.
52. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.
53. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
54. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
55. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE

56. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
57. 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.
58. Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.
59. Фільтрація інтернет-трафіку.
60. Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
61. 27 категорій фільтрації інтернет-трафіку, в яких розподілені більш ніж 100 підкатегорій, а також можливість створювати групи з категорій та підкатегорій.
62. Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.
63. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.
64. Регламентне оновлення вірусних баз не менше 24 разів за добу.
65. 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.
66. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
67. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
68. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.
69. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
70. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
71. Інструменти моніторингу, оцінки стану безпеки та реагування:
72. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
73. 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.
74. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
75. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
76. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
77. Локальне зберігання журналів на робочих станціях.
78. 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.
79. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
80. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

81. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
82. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
83. 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.
84. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
85. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
86. Можливість віддаленого встановлення на клієнтську робочу станцію
87. Можливість предвстановлення на окремих ПК або у образі VDI за допомогою комплексного інсталятору, що дасть можливість з'єднуватись з сервером управління одразу після підключення до мережі або запуску у середовищі VDI.
88. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
89. Можливість крім основного вказати резервні сервери адміністрування.
90. Наявність інструменту віддаленого управління.
91. Низьке споживання ресурсів ПК актуальними антивірусними продуктами (сукупно усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору.
92. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
93. Підтримка ОС: Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10.

Технічні вимоги до антивірусного програмного забезпечення для захисту файлових серверів під керуванням ОС Microsoft Windows Server

1. Підтримка ОС: Microsoft Windows Server 2022, 2019, 2016, 2012R2, 2012, 2008R2, Microsoft Windows Server Core 2022, 2019, 2016, 2012R2, 2012, 2008R2; RedHat Enterprise Linux (RHEL) 7, 8, 9; CentOS 7; Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS; Debian 10, 11; SUSE Linux Enterprise Server (SLES) 12, 15; Oracle Linux 8; Amazon Linux 2.
2. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
3. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
4. 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.
5. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
6. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.
7. Можливість сканування файлів під час запуску ОС.
8. 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.
9. Сканування комп'ютера у неактивному стані.
10. 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.
11. Автоматична антивірусна перевірка змінних носіїв.

12. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.
13. 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.
14. 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.
15. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
16. 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.
17. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
18. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
19. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.
20. 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.
21. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
22. Регламентне оновлення вірусних баз не менше 24 разів за добу.
23. Можливість крім основного вказати резервні сервери адміністрування.
24. Наявність механізму контролю за актуальністю оновлень ОС.
25. 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.
26. 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.
27. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
28. Можливість роботи в кластерах як домена так і робочої групи.
29. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
30. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.
31. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
32. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
33. Можливість захисту від зміни параметрів антивірусного ПЗ паролем.
34. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.

Технічні вимоги до інструменту віддаленого управління антивірусними рішеннями

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 аутентифікувати адміністраторів ERA за допомогою груп безпеки AD.
13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.
14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.
15. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів.
16. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
17. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
18. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.
19. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
20. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
21. 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.

22. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
23. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.
24. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.
25. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
26. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
27. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом.
28. 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.
29. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
30. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях
31. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту.
32. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.
33. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування).
34. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу
35. Можливість встановлення серверу адміністрування на ОС Windows та Linux.
36. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
37. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
38. Можливість встановлення агенту управління на ARM64 процесорах.
39. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
40. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

Обґрунтування очікуваної вартості та/або розміру бюджетного призначення предмета закупівлі

Необхідність проведення закупівлі зумовлена потребою забезпечення антивірусного захисту робочих станцій Головного управління Держпродспоживслужби у Вінницькій області.

Очікувана вартість предмета закупівлі: 251 500,00 грн., визначалась на підставі обсягу закупівлі товару, цін на послуги за результатами вивчення постачальників такого товару - офіційних представництв та офіційних дистриб'юторів фірм-виробників антивірусного програмного забезпечення в Україні.

Обґрунтування розміру бюджетного призначення: розмір бюджетного призначення до кошторису на 2023 рік (згідно внесених змін), враховуючи очікувану вартість.

ДЕРЖАВНА СЛУЖБА УКРАЇНИ
З ПИТАНЬ БЕЗПЕЧНОСТІ ХАРЧОВИХ ПРОДУКТІВ ТА ЗАХИСТУ СПОЖИВАЧІВ
ГОЛОВНЕ УПРАВЛІННЯ ДЕРЖПРОДСПОЖИВСЛУЖБИ У ВІННИЦЬКІЙ ОБЛАСТІ
СЕКТОР ПІДТРИМКИ КОРИСТУВАЧІВ ТА ІНЖЕНЕРНОЇ ІНФРАСТРУКТУРИ

вул. Праведників світу, 19, м. Вінниця, 21036, тел. (0432) 65-88-00, факс (0432) 66-03-03
web: www.vingudpss.gov.ua, e-mail: info@vingudpss.gov.ua, код ЄДРПОУ 40310643

_____ № _____ на № _____

Начальнику Головного управління
Держпродспоживслужби у Вінницькій області
Сидоруку Григорію Павловичу

СЛУЖБОВА ЗАПИСКА

З метою забезпечення антивірусного захисту робочих станцій Головного управління, прошу розглянути питання, щодо проведення тендерної процедури із закупівлі послуг з подовження ліцензій на право використання антивірусного програмного забезпечення (код за ДК 021:2015: 48761000-0 – Пакети антивірусного програмного забезпечення).

Орієнтовна вартість – 251 500 грн.

Завідувач сектору підтримки
користувачів та інженерної інфраструктури Андрій РУДЗЕВИЧ

UB
Головне управління Держпродспоживслужби у Вінницькій області
№СЗ-15/990/23 від 28.08.2023
КЕП: Рудзевич А. В. 28.08.2023 10:43
3FAA9288358EC0030400000015462A000657BB00
Сертифікат дійсний з 16.06.2023 09:52 до 16.06.2025 09:52