ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з предметом закупівлі: ДК 021:2015 код 72260000-5 “Послуги, пов’язані з програмним забезпеченням” (Послуга у сфері інформатизації з постачання програмного забезпечення ESET Security для Microsoft Sharepoint Server. Пільгова. Для захисту трьох об’єктів на 1 рік на виконання п. 4.4. завдань регіональної програми інформатизації “Дніпропетровщина: цифрова трансформація” на 2023–2025 роки)

1. Замовник

Департамент цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської облдержадміністрації.

2. Підстави закупівлі

Закупівля здійснюється відповідно до пункту 4.4. завдань регіональної програми інформатизації “Дніпропетровщина: цифрова трансформація” на 2023–2025 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 14 жовтня 2022 року № 216-13/VIII.

Метою закупівлі є забезпечення антивірусним захистом серверного обладнання електронного комунікаційного центру області, поштових шлюзів, автоматизованих робочих місць користувачів корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації відповідно до вимог комплексної системи захисту інформації.

Одним із головних компонентів комплексної системи захисту інформації є програмне забезпечення антивірусного захисту.

На даний час система інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації функціонує на базі захищеного електронного комунікаційного центру (далі – ЕКЦ) області комунального підприємства “Головний інформаційно-комунікаційний і науково-виробничий центр” Дніпропетровської обласної ради”, який об’єднує 47 серверів, 6 технологічних систем, 4 сховища даних та має близько 2000 користувачів корпоративної мережі, до якої входять: працівники апарату та структурних підрозділів облдержадміністрації, обласної ради, райдержадміністрацій, відповідних органів місцевого самоврядування області, у т.ч. територіальних громад.

На базі захищеного ЕКЦ області активно функціонують та розвиваються корпоративні хмарні сервіси (система електронного документообігу, реєстр територіальних громад, віртуальний офіс електронних послуг, платформа створення веб-сайтів тощо).

Відповідно до вимог комплексної системи захисту інформації необхідно проводити заходи щодо захисту автоматизованих робочих місць від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп’ютерного обладнання та захисту інформації на них.

З метою виконання доручення Прем’єр-міністра України від 29.04.2022 № 9178/1/1-22 виникла необхідність придбання додаткового програмного забезпечення, а саме: для забезпечення захисту програмно-технічного комплексу "Регіональний віртуальний офіс адміністративних послуг" (Е-СЕРВІС) на рівні середовища виконання додатків, що дозволить посилити рівень безпеки від шкідливих завантажень будь-яких файлів в систему, при роботі її користувачів (реєстратори ЦНАП, суб’єкти надання адміністративних послуг), у тому числі з урахуванням рекомендацій CERT-UA (https://cert.gov.ua/recommendation/11388).

3. Очікувана вартість предмета закупівлі: 390000,00 грн з ПДВ (обласний бюджет).

Очікувана вартість сформована з використанням примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Мінекономіки від

18.02.2020 №275, на підставі запиту безпосередньо до представника виробника програмної продукції, самостійного аналізу цін на аналогічні за технічними характеристиками типи програмної продукції через мережу Інтернет та в електронній системі закупівель Prozorro, а також з урахуванням необхідності забезпечення економії бюджетних коштів в умовах дії правового режиму воєнного стану в Україні.

4. Технічні та якісні характеристики предмета закупівлі

ТЕХНІЧНА СПЕЦИФІКАЦІЯ

Найменування програмного забезпечення	Кількість, од.
Послуга у сфері інформатизації з постачання програмного забезпечення ESET Security для Microsoft Sharepoint Server. Пільгова. Для захисту 3 об"єктів. 1 рік	1

Вимоги захисту Microsoft Sharepoint Server

1. Автоматичне визначення ролей сервера для створення автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
2. Надання захисту від: шкідливих програм, троянського ПЗ, клавіатурних шпіонів, рекламного ПЗ, фішингу, шпигунського ПЗ, руткітів, скриптів, потенційного небажаного та небезпечного ПЗ.
3. Забезпечення захисту в режимі реального часу.
4. Використання евристичних технологій під час сканування.
5. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
6. 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.
7. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
8. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків
9. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.
10. Сканування інтерфейсу UEFI - перевірка на наявність шкідливого програмного забезпечення в головному завантажувальному записі.
11. Можливість сканування файлів під час запуску операційної системи.
12. 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.
13. Сканування комп'ютера у неактивному стані.
14. 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.
15. Автоматична антивірусна перевірка змінних носіїв.
16. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.
17. 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.

18. 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.

19. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

20. 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.

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

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

23. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.

24. 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 .

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

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

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

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

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

30. Отримання оновлення клієнтів з локального дзеркала на сервері.

31. Можливість створення дзеркала оновлень засобами антивірусного ПЗ.

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

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

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

35. Наявність інструменту віддаленого управління.

36. Можливість крім основного вказати резервні сервери адміністрування.

37. Наявність механізму контролю за актуальністю оновлень операційної системи.

38. 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.

39. 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.

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

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

42. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.

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

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

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

46. Можливість захисту паролем від зміни параметрів та видалення антивірусного ПЗ.

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

48. Можливість віддаленого встановлення на файловий сервер.

49. Можливість предвстановлення на окремих файлових серверах за допомогою комплексного інсталятору, що дасть можливість з'єднуватись з сервером управління одразу після підключення до мережі.

50. Можливість вносити виключення для процесів для забезпечення сумісності зі стороннім програмним забезпеченням.

51. Використання 64-бітового ядра задля оптимізації процесів сканування.

52. Можливість контролювати ефективність процесу сканування за допомогою лічильники продуктивності.

53. Наявність віддаленого моніторингу та управління (RMM) для нагляду та контролю за програмними системами (настільні комп’ютери, сервери та мобільні пристрої).

54. Можливість використання прямого доступу до бази даних SQL.

55. Можливість інтеграції з системою EDR (Endpoint Detection and Response)

56. Можливість вибору веб-сайтів SharePoint, які потрібно сканувати.

57. Швидке сканування бази даних SharePoint завдяки паралельному завантаженню та скануванню файлів.

58. Можливість багато потокового сканування у фермі SharePoint

59. Сканування документів як під час завантаження на сервер SharePoint, так і під час завантаження з серверу SharePoint.

60. Можливість очищення заражених документів від зловмисних вкладень.

61. Автоматичне сканування зображень та файлів, пов’язаних з документами.

62. Можливість сканування, при наявності, всіх версій файлу, починаючи з самої старої.

63. Можливість використовувати правила сканування за вибраними критеріями (ім’я, розмір, тип, URL файлу, дата зміни файлу користувачем, наявність захищеного паролем архіву, наявність пошкодженого архіву, час змін).

Додаткові вимоги:

1. Запропоноване ПЗ повинне забезпечуватись в Україні технічною підтримкою, яка працює в режимі 24x7x365, з можливістю зв’язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку).
2. Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог, викладених вище), зареєстрованих в Адміністрації Державної служби спеціального зв’язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.