ОБҐРУНТУВАННЯ

технічних та якісних характеристик предмета закупівлі, очікуваної вартості предмета закупівлі

Пункт Кошторису замовника	Предмет закупівлі	Очікувана вартість предмета закупівлі згідно Річного плану закупівель, грн	Очікувана вартість предмета закупівлі згідно ОГОЛОШЕННЯ про проведення відкритих торгів	Ідентифікатор процедури закупівлі
51.06 (2022)	**Пакети антивірусного програмного забезпечення (поновлення),** код ДК 021:2015 - 48760000-3 - Пакети програмного забезпечення для захисту від вірусів	702 190,00 грн. без ПДВ	702 190,00 грн. без ПДВ	**UA-2022-08-29-005132-a**

Визначення потреби в закупівлі: Закупівля зумовлена необхідністю забезпечення антивірусним захистом серверів та комп'ютерів підприємства з метою автоматичного виявлення, видалення шкідливого, небезпечного програмного забезпечення та зниження ймовірності ураження шкідливим програмним забезпеченням комп'ютерної та серверної інфраструктури підприємства. Підвищення рівня безпеки шляхом організації двофакторної автентифікації в корпоративній мережі.

Обґрунтування очікуваної вартості предмета закупівлі: Визначення очікуваної вартості предмета закупівлі обумовлено статистичним аналізом загальнодоступної інформації про ціну предмета закупівлі на підставі затвердженої центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері публічних закупівель, примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275. Очікувана вартість предмета закупівлі визначена методом порівняння ринкових цін на підставі отриманих комерційних пропозицій від компаній партнерів поточного Виробника антивірусного ПЗ. Для розрахунку використано середньоарифметичне значення отриманих даних.

Обґрунтування обсягів закупівлі: Обсяги визначено відповідно до очікуваної потреби та обсягу фінансування.

Обґрунтування технічних та якісних характеристик предмета закупівлі: Якісні та технічні характеристики предмета закупівлі визначені з урахуванням реальних потреб підприємства та оптимального співвідношення ціни та якості.

Враховуючи зазначене, замовник прийняв рішення стосовно застосування таких технічних та якісних характеристик предмета закупівлі:

№ п/п	Найменування Товару	Одиниці виміру	Кількість	Технічні та інші характеристики (технічна специфікація)
1	Програмна продукція антивірусного захисту	шт.	1	**Загальні вимоги:** – загальна кількість об’єктів захисту **450 од.**; – забезпечення антивірусного захисту комп’ютерів (робочих станцій) та серверів; – забезпечення централізованого управління, що дозволить управляти захистом і контролювати стан антивірусної безпеки в корпоративній мережі; – наявність інтерфейсу та документації програмної продукції українською та англійською мовами; – забезпечення можливості оновлення антивірусних баз програмного продукту з вебсайту Центру антивірусного захисту інформації Держспецзв’язку України (http://cazi.gov.ua); – забезпечення регулярного, щоденного надання оновлень антивірусних баз 12 місяців. **1. Вимоги до антивірусного захисту серверів:** 1.1 Підтримка ОС: Microsoft Windows Server 2019 (Server Core and Desktop Experience), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1, RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 1.2 Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи. 1.3 Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 1.4 Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду. 1.5 Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. 1.6 Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням. 1.7 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. 1.8 Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж). 1.9 Можливість крім основного вказати резервні сервери адміністрування. 1.10 Наявність механізму контролю за актуальністю оновлень ОС. 1.11 Забезпечення захисту в режимі реального часу. 1.12 Використання евристичних технологій під час сканування. 1.13 Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків. 1.14 Можливість інтеграції захисту серверів з хмарною пісочницею (при наявності додаткової ліцензії), без необхідності встановлення додаткових програмних продуктів. 1.15 Сканування інтерфейсу UEFI - перевірка на наявність шкідливого програмного забезпечення в головному завантажувальному записі.

				1.16 Можливість сканування файлів під час запуску операційної системи. 1.17 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. 1.18 Сканування серверу у неактивному стані. 1.19 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. 1.20 Автоматична антивірусна перевірка змінних носіїв. 1.21 Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою. 1.22 Наявність інструменту, який зможе здійснювати контроль підключення до серверу 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. 1.23 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. 1.24 Забезпечення захисту поштового клієнту на сервері з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS. 1.25 Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті. 1.26 Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес. 1.27 Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер. 1.28 Можливість використання технології, яка забезпечує захист від загроз типу "ботнет". 1.29 Захист вразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д. 1.30 Отримання оновлення клієнтів з локального дзеркала на сервері. 1.31 Можливість створення дзеркала оновлень засобами антивірусного ПЗ. 1.32 Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне. 1.33 Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну. 1.34 Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. 1.35 Наявність інструменту віддаленого управління. 1.36 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. 1.37 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. 1.38 Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 1.39 Можливість роботи в кластерах як домена так і робочої групи 1.40 Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування. 1.41 Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів. 1.42 Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом. 1.43 Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ. 1.44 Можливість захисту паролем від зміни параметрів та видалення антивірусного ПЗ. 1.45 Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому. 1.46 Можливість віддаленого встановлення на файловий сервер. 1.47 Можливість предвстановлення на окремих файлових серверах за допомогою комплексного інсталятору, що дасть можливість з'єднуватись з сервером управління одразу після підключення до мережі. **2. Вимоги до антивірусного захисту комп'ютерів (робочих станцій)** 2.1 Надання захисту від різних видів загроз, мережевих атак та спаму. Захист від загроз типу "ботнет, IP та MAC спуфінгу, "нульового" дня". Захист уразливостей мережевого протоколу що покращує виявлення загроз, які використовують недоліки мережевих протоколів SMB. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків. 2.2 Використання розширеного машинного навчання із застосуванням нейронних мереж і групи з шести алгоритмів класифікації для покращення виявлення, що працює навіть без підключення до мережі Інтернет. 2.3 Програмний продукт повинен мати низькі показники споживання ресурсів комп'ютеру актуальними антивірусними версіями продукту (сукупно з усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору. 2.4 Використання евристичних технологій під час сканування та забезпечення захисту в режимі реального часу. 2.5 Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 2.6 Сканування комп'ютера у неактивному стані. 2.7 Перевірка завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. 2.8 Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. 2.9 Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи. 2.10 Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.

				2.11 Наявність модуля захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. 2.12 Можливість сканування файлів під час запуску ОС. 2.13 Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз. 2.14 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. 2.15 Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування. 2.16 Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. 2.17 Наявність інструмент Antimalware Scan Interface (AMSI) для захисту від сценаріїв у Powershell (wscript.exe, а також cscript.exe). 2.18 Автоматична антивірусна перевірка змінних носіїв. 2.19 Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою. 2.20 Наявність інструменту, який може здійснювати контроль підключення до робочої станції зовнішніх пристроїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження. 2.21 Можливість створювати групи дозволених або заборонених зовнішніх пристроїв. 2.22 Можливість застосовувати правила контролю зовнішніх пристроїв протягом певного часового проміжку (планування на основі дня\часу). 2.23 Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену. 2.24 Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль повинен містити в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру. 2.25 Забезпечення додаткового рівня захисту Інтернет трафіку шляхом перевірки HTTP, HTTPS трафіку, що надасть можливість блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware». 2.26 Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес. 2.27 Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі. 2.28 Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP–об'єктів (IP– адресів, діапазонів IP–адресів, підмереж). 2.29 Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах. 2.30 Перевірка дійсності та цілісності сертифікатів SSL трафіку. 2.31 Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим. 2.32 Відкат оновлень з можливістю повернутися до попередніх версій баз антивірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.

				2.33 Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. 2.34 Оновлення програмного продукту та антивірусних сигнатур в локальній мережі (без підключення до мережі Інтернет). 2.35 Наявність механізму контролю за актуальністю оновлень операційної системи. 2.36 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 (вміння порівнювати різні знімки стану системи для виявлення змін, які відбулись в системі, створення та виконання скриптів, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання). 2.37 Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі. 2.38 Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час. 2.39 Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання. 2.40 Локальне зберігання журналів на робочих станціях. 2.41 Наявність планувальника завдань, з можливістю 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. 2.42 Можливість захисту від зміни параметрів антивірусного ПЗ паролем. 2.43 Наявність розширеного сканер пам'яті, який дозволяє знешкоджувати загрози, що містяться в оперативній пам'яті у зашифрованому вигляді. 2.44 Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак. 2.45 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. 2.46 Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання. 2.47 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. 2.48 Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер. 2.49 Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж. 2.50 Наявність додаткового функціоналу персонального брандмауеру, що дозволить переглядати всю детальну інформацію у всіх наявних мережевих з'єднаннях, переглядати автоматично заблоковані мережеві з'єднання з метою корегування правил, а також контролювати зміни у мережевих додатках.

				2.51 Наявність модуль захисту від спаму з можливістю інтеграції до поштового клієнту. Можливість використовувати білі та чорні списки як користувальницькі, так і глобальні, інформація до яких надходить з серверів оновлення. 2.52 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. 2.53 Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті. 2.54 Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE 2.55 Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання. 2.56 Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання. 2.57 Налаштування додаткових параметрів модуля системи виявлення вторгнень з метою виявлення різних типів можливих мережевих атак на комп'ютер. 2.58 Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів. 2.59 Наявність у достатній кількості категорій фільтрації інтернет-трафіку, з розподіленням на підкатегорії, а також можливість створювати групи з категорій та підкатегорій. 2.60 Можливість створювати правила фільтрації інтернет трафіку для різних користувачів та груп ОС Windows або домену. 2.61 Можливість задавати часові інтервали, що дозволить більш гнучко налаштовувати правила веб-фільтрації. 2.62 Регламентне оновлення вірусних баз не менше 24 разів за добу. 2.63 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. 2.64 Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок. 2.65 Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне. 2.66 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. 2.67 Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача. 2.68 Можливість віддаленого встановлення на клієнтську робочу станцію 2.69 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. 2.70 Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ. 2.71 Можливість крім основного вказати резервні сервери адміністрування. 2.72 Наявність інструменту віддаленого управління. 2.73 Підтримка ОС: Microsoft Windows 11, Windows 10, Windows 8, Windows 7 SP1, macOS 10.12 і вище. **3. Функціональні вимоги до централізованого керування антивірусним захистом (інструменту віддаленого**

				управління): 1.1 Централізоване управління антивірусним ПЗ (програмним продуктом). 1.2 Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених об'єктів, а також стану самого сервера адміністрування. 1.3 Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 1.4 Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 1.5 Віддалена інсталяція антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac на кілька кінцевих точок одночасно. 1.6 Віддалена інсталяція користувальницького програмного забезпечення. 1.7 Можливість віддаленого видалення встановленого користувальницького програмного забезпечення. 1.8 Віддалене видалення антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac. 1.9 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. 1.10 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. 1.11 Можливість аутентифікувати адміністраторів за допомогою груп безпеки Active Directory. 1.12 Можливість віддалено активувати та деактивувати модулі захисту, такі як персональний брандмауер, захист в режимі реального часу, захист поштового клієнта, захист доступу до Інтернету, контроль пристроїв, веб-контроль, антиспам на окремо взятому клієнті. 1.13 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. 1.14 Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів сервера адміністрування. Можливість обраному користувачеві сервера адміністрування додати одну або кілька груп автентифікації Windows або домену. 1.15 Наявність журналу аудиту, у якому відстежуються і реєструються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування. 1.16 Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту. 1.17 Збереження на локальному диску або відправлення на електронну пошту звітів у форматах PDF, PS, CSV. 1.18 Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом. 1.19 Проведення за розкладом антивірусної перевірки комп'ютерів і серверів та оновлень антивірусних сигнатур засобу антивірусного захисту.

				1.20 Створення правил для оповіщення на вірусні події, виконання завдань за розкладом та роботи засобу антивірусного захисту. 1.21 Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу. 1.22 Можливість генерації для захисту облікових записів адміністраторів додаткових паролів для запобігання несанкціонованому вимкненню або переналаштуванню антивірусного захисту корпоративної інфраструктури. 1.23 Можливість використовувати двофакторну автентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління. 1.24 Можливість створювати та редагувати статичні групи та можливість імпорту з Active Directory дерева комп'ютерів. 1.25 Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань. 1.26 Можливість імпорту користувачів та груп з Active Directory, для подальшого використання їх для персоналізації правил контролю пристроїв та вебконтролю. 1.27 Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик. 1.28 Наявність передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів. 1.29 Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL. 1.30 Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM. 1.31 Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/ клієнтів. 1.32 Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу. 1.33 Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів. 1.34 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. 1.35 Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях. 1.36 Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів. 1.37 Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування. 1.38 Можливість встановлення серверу адміністрування на ОС Windows та Linux 1.39 Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation). 1.40 Забезпечення централізованим управління в єдиній консолі адміністрування програмних продуктів, що закупляються відповідно п.1, п.2 та п.3 специфікації.
2	Програмна продукція антивірусного захисту	шт.	1	**Загальні вимоги:** – загальна кількість об’єктів захисту **600 од.**; – забезпечення антивірусного захисту комп’ютерів (робочих станцій) та серверів; – забезпечення централізованого управління, що дозволить управляти захистом і контролювати стан антивірусної

				безпеки в корпоративній мережі; – наявність інтерфейсу та документації програмної продукції українською та англійською мовами; – забезпечення можливості оновлення антивірусних баз програмного продукту з вебсайту Центру антивірусного захисту інформації Держспецзв'язку України (http://cazi.gov.ua); – забезпечення регулярного, щоденного надання оновлень антивірусних баз 12 місяців. **Вимоги до антивірусного захисту серверів, Вимоги до антивірусного захисту комп'ютерів (робочих станцій), Функціональні вимоги до централізованого керування антивірусним захистом (інструменту віддаленого управління) аналогічні до п.1 специфікації.** **Програмна продукція згідно специфікації п.1 та п.2 повинна бути повністю ідентична та забезпечуватись централізованим управління в єдиній консолі адміністрування програмних продуктів, що закупляються відповідно п.1, п.2 та п.3 специфікації.**
3	Програмна продукція ESET Endpoint Security (поновлення)	шт.	1	**Загальні вимоги:** – кількість об'єктів захисту 200 од.; – поновлення функціональних можливостей; – забезпечення регулярного, щоденного надання оновлень антивірусних баз 12 місяців для існуючого у Замовника програмного продукту ESET Endpoint Security інв.№694 захист ПК на 200 ключів.
4	Програмна продукція контролю доступу	шт.	1	**Загальні вимоги:** – кількість об'єктів захисту 400 од.; – забезпечення віддаленого централізованого управління, що дозволяє управляти захистом і контролювати стан двофакторної автентифікації в корпоративній мережі; – термін дії активації на програмну продукцію – 12 місяців. **Склад програмної продукції з наступними компоненти:** – плагін для забезпечення двофакторної автентифікації для різних додатків Microsoft Web Applications; – плагін для забезпечення двофакторної автентифікації для Remote Desktop Protocol; – плагін для забезпечення двофакторної автентифікації для комп'ютерів Windows; – компонент RADIUS Server додає функцію двофакторної автентифікації до автентифікації VPN. **Функціональні вимоги:** – наявність функції двофакторної автентифікації (2FA) в домени Microsoft Active Directory або локальну мережу; – передбачена генерація одноразового пароля (OTP) та його застосування додатково до облікових даних; – двофакторна автентифікація з можливістю передбаченням створення push-сповіщення, яке необхідно прийняти на мобільному телефоні користувача з ОС Android, iOS або Windows після успішної автентифікації користувача за допомогою облікових даних; – можливість додання 2FA для безпечного доступу входу в як локальний обліковий запис, так і доменний обліковий запис системи під управлінням: Miscrosoft Windows, Linux або MAC OS X; – можливість отримання паролів 2FA за допомогою смс-повідомлень, push-повідомлень, OTP;

				– підтримка апаратних токенів, які працюють по стандартам OATH, HOTP, TOTP, FIDO, FIDO2; – можливість додання 2FA для веб-додатків Microsoft: Microsoft Outlook Web App, Microsoft Exchange, Microsoft SharePoint, Microsoft Exchange Mailbox Server Role, Microsoft SharePoint Foundation, Microsoft Dynamics CRM, Microsoft Remote Desktop - Web Access, Microsoft Remote Desktop Gateway, Microsoft Terminal Services Web Access, Microsoft Exchange Admin Center; – наявність API, яка дозволяє додавати двофакторну аутентифікацію в наявні додатки; – наявність пакету SDK, що надає доступ до функцій керування користувачами та їх аутентифікаціями; – захист VPN ТА VDI систем, таких як: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC,Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall,Netasq, VMware Horizon View и Citrix XenApp, Cyberoam; – можливість захисту RADIUS PAM для Linux, Mac; – наявність Identity Provider Connector для забезпечення 2FA хмарних служб (постачальником послуг) і постачальником ідентифікаційних даних, таких як: OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence; – захист через SSO та Microsoft Active Directory Federation Services для входу до Office 365 або Azure; – можливість захисту мобільного додатку за допомогою біометрики на базі операційних систем IOS та Android; – інформування користувача про спробу авторизації з можливістю підтвердити або відхилити подальшу автентифікацію; – наявність системи звітності, що можуть використовуватися як для панелі моніторингу, так і для формування звітів; – наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації, запуск та зупинки служби двофакторної автентифікації; – можливість інтеграції з SIEM та іншими системами моніторингу, аналітики та реагування; – можливість для адміністратора надавати альтернативний одноразовий пароль OTP у разі, якщо коли користувач немає доступу до токену або до мобільного додатку; – можливість імпортувати користувачів у спеціальні області за допомогою файлу CSV або LDF; – можливість використання 2FA для безпечного режиму, блокуванні облікового запису Windows, використання UAC; – можливість налаштування використання 2FA для користувачів, які не мають підключення до серверу 2FA; – можливість обмеження кількості використання одноразових паролів для комп'ютерів, які не мають підключення до серверу 2FA; – наявність захисту від підбору одноразового паролю шляхом блокування користувача; – наявність системи сповіщень про вибрані типи дій; – можливість виключення з 2FA для списку IP-адрес; – можливість налаштування користувацького способу доставлення паролів OTP.

Додаткова інформація:

Обґрунтування необхідності закупівлі даного виду товару по позиціям 1-2, 4 – замовник здійснює закупівлю даного виду товару, оскільки він за своїми якісними та технічними характеристиками найбільше відповідатиме вимогам та потребам замовника.

Обґрунтування необхідності закупівлі даного виду товару по позиції 3 специфікації - предмет закупівлі буде використовуватися для вже існуючої програмної продукції, яка потребує поновлення, а тому дуже важливо, для сумісності з вже існуючою програмною продукцією, чітко дотримуватись зазначених технічних вимог.

Для дотримання принципів Закону, а саме максимальної економії та ефективності, замовником було прийнято рішення провести закупівлю саме даної програмної продукції.

У місцях, де технічна специфікація містить посилання на стандартні характеристики, технічні регламенти та умови, вимоги, умовні позначення та термінологію, пов'язані з товарами, роботами чи послугами, що закуповуються, біля кожного такого посилання вважається наявним вираз «або еквівалент».

У місцях, де технічна специфікація містить посилання на конкретну 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». Таким чином, вважається, що до кожного посилання додається вираз «або еквівалент» *(таке посилання обумовлено наданням Учасникам загального уявлення про технічні та інші характеристики чи складові Товару).*

Під **«еквівалентом»** розуміється це щось рівноцінне, рівнозначне, рівносильне, таке що повністю відповідає встановленим вимогам Замовника (технічні та інші характеристики запропонованого «еквіваленту» повинні відповідати встановленим технічним та іншим характеристикам).