ОБГРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ ДЛЯ ЗАСТОСУВАННЯ ПРОЦЕДУРИ ЗАКУПІВЛІ – ВІДКРИТІ ТОРГИ З ОСОБЛИВОСТЯМИ

Підстава для публікації обґрунтування: (відповідно до постанови Кабінету Міністрів України від 11.10.2016р. № 710 «Про ефективне використання державних коштів» (із змінами, внесеними згідно з Постановами КМ), зокрема, п. 4^{1}).

Мета проведення закупівлі: З метою виконання поставлених завдань і функцій Головного управління Держпродспоживслужби у Волинській області та забезпечення безперебійної роботи комп'ютерного обладнання, виникла необхідність закупівлі **послуг** за предметом закупівлі **«Пакети антивірусного програмного забезпечення»**.

Назва предмета закупівлі: «Пакети антивірусного програмного забезпечення: програмна продукція 'ESET PROTECT Essential з локальним управлінням» за кодом ДК 021:2015 48760000-3: Пакети програмного забезпечення для захисту від вірусів

Ідентифікатор закупівлі: UA-2024-08-02-002402-a.

Обґрунтування технічних, якісних та кількісних характеристик предмета закупівлі:

У межах закупівлі Замовник планує придбати пакети антивірусного програмного забезпечення (далі – ПЗ), а саме ліцензію, що наведена у **Таблиці № 1**.

3.	Місце постачання ПЗ:	Головне управління Держпродспоживслужби у Волинській області: 43020, м. Луцьк, вул. Поліська Січ, 10
4.	Строк постачання ПЗ:	Учасник повинен передати Замовнику ПЗ до 31.08.2024
5.	Термін дії ліцензії на ПЗ:	Замовник отримує право користування ПЗ протягом 12 місяців з дати надання ПЗ Замовнику
6.	Тип постачання ліцензії на ПЗ:	Цифровий (ПЗ повинно поставлятися в електронній формі у вигляді ключових файлів, цифрових кодів або ідентифікаторів, які забезпечують активацію даного ПЗ)

Таблиця № 1

№ з/п	**Назва продукту***		**Кількість ліцензій, од.**
1.	Пакети антивірусного програмного забезпечення: програмна продукція 'ESET PROTECT Essential з локальним управлінням'		1
1.1.	Тип ліцензії:	Поновлення	
1.2.	Кількість об'єктів для захисту:	230	

**У разі якщо присутнє посилання на конкретну торгівельну марку, фірму, патент, конструкцію, вважати це «або еквівалент».*

Учасник у складі пропозиції повинен надати нижчезазначені підтверджуючі документи:

1. Документальне підтвердження у вигляді авторизаційного листа, партнерського сертифікату або довідки про дилерські повноваження (електронна копія) від компанії-виробника ПЗ або офіційного представника виробника в Україні, що підтверджує право Учасника закупівлі постачати антивірусне ПЗ відповідно до предмету закупівлі та укладати договір про його постачання згідно з цією закупівлею.

2. Дійсний сертифікат Державної служби спеціального зв'язку та захисту інформації України.

3. Документальне підтвердження від Учасника про відповідність (не відповідність) запропонованого ПЗ обов'язковим вимогам у вигляді **Таблиці № 2** «Відповідність технічних, якісних характеристик запропонованого ПЗ обов'язковим вимогам».

Документальне підтвердження про відповідність (не відповідність) запропонованого ПЗ обов'язковим вимогам має бути у вигляді довідки за підписом та відбитком печатки (у разі використання) Учасника.

Таблиця № 2

Відповідність технічних, якісних характеристик запропонованого ПЗ обов'язковим вимогам

№ з/п	Обов'язкові вимоги до пакетів антивірусного програмного забезпечення	Відповідність фактичним параметрам запропонованого програмного забезпечення**
1.	**Вимоги до рішення для захисту робочих станцій під управлінням несерверних ОС:** - надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ; - 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 у поєднанні з компонентом машинного навчання; - 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; - 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; - надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого ПЗ; - надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в ОС; - можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування; - можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення у роботі або впливати на продуктивність системи;	

	- можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання у процес роботи ОС; - можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, у тому числі в інтерфейсі UEFI; - можливість сканування файлів під час запуску ОС; - можливість сканування комп'ютера у неактивному стані; - можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об'єктів та методів сканування, встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень; - можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного ПЗ; - можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру; - можливість додаткової перевірки запущених процесів у хмарному репутаційному сервісі; - можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою; - можливість створювати групи дозволених або заборонених зовнішніх пристроїв; - можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену; - можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв; - можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах; - можливість перевірки дійсності та цілісності сертифікатів SSL-трафіку; - можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим; - можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер; - можливість використання технології, яка забезпечує захист від загроз типу «ботнет»; - можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання; - можливість отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту у закритих ізольованих мережах, що не мають доступу до мережі Інтернет; - можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок; - можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне;	

	- можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею; - можливість відкату оновлень, що дозволяє повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну; - можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень; - можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів ОС, з метою виявлення несанкціонованих та небезпечних змін у ОС; - можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись у системі за визначений час; - можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання; - можливість локального зберігання журналів на робочих станціях; - можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій; - можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску; - можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом; - можливість захисту паролем параметрів рішення для захисту кінцевої точки; - можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача; - можливість крім основного вказати резервні сервери адміністрування; - антивірусне сканування за вимогою користувача або адміністратора та згідно графіку; - забезпечення антивірусного захисту у режимі реального часу; - 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; - 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»; - використання евристичних технологій власної розробки під час сканування; - використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування; - наявність вбудованого інструмента, що об'єднує у собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.; - наявність модулю захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду;	

	- наявність модулю захисту від експлойтів, який забезпечує захист від загроз, здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо; - наявність модулю, який глибоко аналізує запущені процеси та їх діяльність у файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware); - наявність модулю сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами; - наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами у системному реєстрі та захищає комп'ютер від шкідливих програм і небажаної активності; - наявність автоматичної антивірусної перевірки змінних носіїв; - 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; - наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості ПЗ та надання докладнішої інформації про ідентифікатори CVE; - наявність регламентного оновлення вірусних баз не менше 24 разів за добу; - наявність механізму контролю за станом безпеки та актуальністю оновлень ОС; - наявність інструменту для діагностики системи, який має можливість створювати знімки стану ОС для подальшого глибокого аналізу різноманітних аспектів роботи ОС, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання; - 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; - 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; - наявність графічного інтерфейсу, сумісного із сенсорним екраном високої роздільної здатності; - наявність багатомовного інсталятора, який містить у собі у тому числі українську мову; - наявність підтримки ОС: Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10.	
2.	**Вимоги до рішення для захисту робочих станцій під управлінням серверних ОС:**	
	- можливість автоматичного визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної ОС; - можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає	

	можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів; - можливість роботи у кластерах як домена так і робочої групи; - можливість захисту від зміни параметрів антивірусного ПЗ паролем; - можливість налаштовувати швидкодію, вказуючи кількість потоків сканування; - можливість сканування файлів під час запуску ОС; - можливість сканування комп'ютера у неактивному стані; - можливість сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин, без необхідності установки будь-яких агентів на відповідних віртуальних машинах; - 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; - 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; - можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж); - можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій; - можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску; - можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом; - можливість крім основного вказати резервні сервери адміністрування; - антивірусне сканування за вимогою користувача або адміністратора та згідно графіку; - 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; - забезпечення перевірки HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес; - наявність підтримки роботи програм, що працюють у повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ; - наявність додаткового рівня захисту користувачів від програм-вимагачів, який контролює та оцінює всі програми на основі їхньої поведінки та репутації; - наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому; - наявність модулю захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду;	

	- наявність розширеного сканеру пам'яті, який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами; - наявність системи виявлення вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності. Також, цей модуль містить у собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру; - наявність автоматичної антивірусної перевірки змінних носіїв; - наявність контролю змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою; - 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; - наявність регламентного оновлення вірусних баз не менше 24 разів за добу; - наявність механізму контролю за станом безпеки та актуальністю оновлень ОС; - наявність інструменту для діагностики системи, який має можливість створювати знімки стану ОС для подальшого глибокого аналізу різноманітних аспектів роботи ОС, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись у системі. Також, він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання; - 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; - підтримка ОС: Microsoft Windows Server 2008, 2008R2, 2012, 2012R2, 2016, 2019, 2022; Microsoft Windows Server Core 2008, 2008R2, 2012, 2012R2; Linux Kernel версії 2.6.x та вище; FreeBSD версії 9.x (x86).	
3.	**Вимоги до інструменту віддаленого управління антивірусними рішеннями:**	
	- можливість постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation); - можливість обирати варіанти обробки ідентифікаторів клонованих комп'ютерів, такі як зіставляння з наявними комп'ютерами або створення нових комп'ютерів; - можливість встановлення серверу адміністрування на ОС Windows та Linux; - можливість встановлення агенту управління на ARM64 процесорах;	

	- можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури; - 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; - можливість аутентифікувати адміністраторів за допомогою груп безпеки Active Directory (AD); - можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів; - можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю; - можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик; - можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань; - можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління; - можливість здійснення інвентаризації обладнання, що встановлено на робочих станціях та серверах під управлінням ОС Windows, Linux та macOS; - можливість здійснення інвентаризації ПЗ, що встановлено на робочих станціях та серверах під управлінням ОС Windows, Linux та macOS; - можливість віддаленої інсталяції антивірусного ПЗ для ОС Windows, Linux та macOS на кілька кінцевих точок одночасно; - можливість віддаленої інсталяції користувальницького ПЗ; - можливість віддаленого видалення встановленого антивірусного ПЗ для ОС Windows, Linux та macOS; - можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станціях, до яких немає фізичного або віддаленого доступу; - можливість віддаленого видалення встановленого користувальницького ПЗ; - можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором; - 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 ОС клієнтського комп'ютера; - можливість 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 ОС;	

	- 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; - можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин; - можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів; - можливість експортувати журнали в syslog для подальшої інтеграції з SIEM; - можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу; - можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів; - наявність підтримки систем віртуалізації таких як: VMware Horizon 8.x або Citrix XenCenter/XenServer 8+; - наявність веб-орієнтованого інтерфейсу, який дає можливість керувати сервером через будь-який браузер шляхом з'єднання, захищеного сертифікатом; - наявність захисту з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів; - наявність додаткового компоненту, що дозволяє керувати антивірусним захистом на мобільних пристроях; - наявність інструменту для керування станом ліцензій (навіть без використання сервера адміністрування); - наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям; - наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії; - наявність спеціального компоненту, який здійснює виявлення у мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту; - наявність підтримки інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL; - наявність інструменту для створення та редагування інсталяційних пакетів для ОС Windows, Linux та macOS 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; - 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; - наявність журналу аудиту, у якому реєструються і відстежуються всі зміни у конфігурації і всі дії, які виконують користувачі сервера адміністрування; - наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану	

	захищених кінцевих точок, а також стану самого сервера адміністрування; - наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів; - наявність передвстановлених шаблонів у системі сповіщень для інформування про некоректну ідентифікацію клонованих машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію з системами VDI; - наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії; - наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери у цілому.	
4.	**Вимоги до технічної підтримки:** Запропоноване антивірусне ПЗ повинно мати центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог: - обслуговування 24 х 7 х 365 – 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 антивірусного ПЗ по телефону (з можливістю зв'язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв'язку) та електронній пошті.	

Кількість послуг: 1 послуга.

Місце поставки предмета закупівлі: 43020, Волинська обл., м. Луцьк, вул. Поліська Січ, 10.

Строк поставки предмета закупівлі: до 31 серпня 2024 року.

Обґрунтування розміру бюджетного призначення та очікуваної вартості предмета закупівлі: Очікувана вартість предмета закупівлі була визначена із застосуванням Примірної методики визначення очікуваної вартості предмета закупівлі затвердженої наказом МЕРТУ від 18.02.2020 № 275 (із змінами) методом порівняння ринкових цін очікуваної вартості на підставі даних ринку, а саме загальнодоступної відкритої інформації про ціни, що міститься в мережі Інтернет у відкритому доступі, а також аналізу обсягів робіт та інформації про аналогічні закупівлі розміщені на сайті https://prozorro.gov.ua ".

Очікувана вартість предмета закупівлі: 120 088,00 грн., з ПДВ.