Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(відповідно до пункту 4[1] постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, його категорія: Територіальне управління Державної судової адміністрації України в Рівненській області; вул. Симона Петлюри, 10, м. Рівне, 33028; код за ЄДРПОУ - 26259988; державний орган у системі правосуддя.

2. **Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності):** *послуги з постачання антивірусного програмного забезпечення, згідно коду за ДК 021:2015: 48760000-3 «Пакети програмного забезпечення для захисту від вірусів»;*

3. **Ідентифікатор закупівлі**: UA-2026-05-29-007589-a

4. **Обґрунтування технічних та якісних характеристик предмета закупівлі:**

ТЕХНІЧНА СПЕЦИФІКАЦІЯ

Найменування*	**Одиниця виміру**	**Кількість**
Програмна продукція ESET PROTECT Entry On-prem 23 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 31 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 23 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 22 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 27 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 36 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 24 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 34 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 120 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 55 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 23 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 24 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 36 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 26 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 18 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 45 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 24 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 24 obj./1 y. Promo: GOV	одиниця	1
Програмна продукція ESET PROTECT Entry On-prem 18 obj./1 y. Promo: GOV	одиниця	1

Запропоновані ліцензії повинні забезпечувати функціонування програмного забезпечення ESET PROTECT Entry, яке вже використовується Замовником, в обсязі, передбаченому цим додатком до тендерної документації та бути сумісними з існуючим сервером централізованого керування. Строк дії ліцензій – 1 рік з моменту закінчення строку дії відповідних поточних ліцензій. Активація ліцензії має

здійснюватися шляхом додавання ключа до існуючого сервера керування. Ліцензії повинні забезпечувати регулярне оновлення баз загроз та технічну підтримку програмного забезпечення ESET PROTECT Entry в Україні виробником програмного забезпечення або його авторизованим в Україні центром технічної підтримки з наступними умовами:
- обслуговування заявок Замовника в режимі 24x7x365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні;
- розширені технічні консультації з питань конфігурації та функціонування програмного забезпечення ESET PROTECT Entry по телефону (з можливістю зв'язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв'язку) та електронній пошті;
- виїзд інженера на місце розташування Замовника у випадках збоїв роботи програмного забезпечення ESET PROTECT Entry.

Вимоги до програмної продукції ESET PROTECT Entry On-prem

№ п/п	Функціонал захисту робочої станції	Вимоги
1.	Встановлення програмного забезпечення	- окремий інсталяційний пакет, який дозволяє встановлювати клієнта у "ручному" режимі.
2.	Здійснення антивірусного захисту	- перевірка за розкладом і на вимогу за допомогою антивірусних баз даних; - забезпечення захисту в режимі реального часу; - можливість сканування файлів під час запуску системи; - модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду; - сканування комп'ютера у неактивному стані; - сканування в оперативній пам'яті об'єктів, що знаходяться у запакованому стані; - сканування архівів; - евристичний аналізатор; - виявлення шпигунського ПЗ; - виявлення руткитів; - перевірка скриптів; - захист від експлойтів, який забезпечує захист від загроз, здатних використовувати уразливості Java, Flash та інших додатків.
3.	Забезпечення мережевого захист	- наявність персонального брандмауера, який містить в собі майстер для створення правил брандмауера та редактор зон та правил; - можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер; - наявність системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер; - наявність технології, яка забезпечує захист від загроз типу "ботнет"; - захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP тощо.
4.	Забезпечення захисту електронної пошти	- перевірка поштового трафіку (POP3, POP3S, SMTP, IMAP та IMAPS); - перевірка поштових вкладень та захист від спаму; - можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті. - наявність модуля захисту від спаму (власної розробки) з можливістю інтеграції до поштового клієнту. Можливість використовувати білі та чорні списки як користувальницькі, так і глобальні, інформація до яких надходить з серверів оновлення.
5.	Забезпечення захисту у Web	- перевірка HTTP, HTTPS трафіку; - виявлення та блокування доступу до небезпечних сайтів; - формування дозволених\заборонених\ виключених з перевірки переліків сайтів; - наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів. Наявність більше 25 категорій

№ п/п	Функціонал захисту робочої станції	Вимоги
		фільтрації, в яких розподілені більш ніж 100 підкатегорій. Можливість створювати групи з категорій та підкатегорій. Можливість створювати правила фільтрації для різних користувачів та груп ОС Windows; - можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.
6.	Наявність проактивного захисту	- забезпечення захисту від троянського ПЗ; - забезпечення захисту від клавіатурних шпигунів; - забезпечення захисту від рекламного ПЗ; - забезпечення захисту від фішингу; - наявність системи виявлення вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності (наявність функціоналу майстера для створення та редагування правил для контролю запущених процесів, використовуваних файлів та розділів реєстру.
7.	Наявність контролю за використанням зовнішніх пристроїв та змінних носіїв	- автоматична антивірусна перевірка змінних носіїв; - керування доступом до зовнішніх пристроїв; - контроль підключення до робочої станції периферійних пристроїв та змінних носіїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою тощо.
8.	Здійснення оновлень	- часті та невеликі за об'ємом оновлення, відновлення завантаження оновлень після обриву зв'язку; - відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну; - можливість мобільним співробітникам отримати оновлення з серверів виробника он-лайн у разі перебування поза корпоративною мережею; - можливість створення дзеркала оновлень засобами антивірусного ПЗ; - наявність оновлень в центрі антивірусного захисту інформації Державної служби спеціального зв'язку та захисту інформації.
9.	Вимоги до віддаленого управління	- наявність спеціального компоненту для управління антивірусним захистом на віддалених робочих станція без необхідності використання додаткових серверів адміністрування.
10.	Операційні системи, які підтримуються	- Microsoft Windows 7 SP1; Microsoft Windows 8; - Microsoft Windows 10; - Microsoft Windows 11; - macOS Big Sur (11)–macOS Sonoma (14); - Ubuntu Desktop 20.04 LTS; - Ubuntu Desktop 22.04 LTS; - Ubuntu Desktop 24.04 LTS; - Red Hat Enterprise Linux 8; - Red Hat Enterprise Linux 9; - Linux Mint 20; - Linux Mint 21; - Linux Mint 22.

Антивірусне програмне забезпечення для захисту файлових серверів повинно відповідати наступним обов'язковим функціональним вимогам:

№ п/п	Функціонал захисту файлового серверу	Вимоги
1.	Встановлення програмного забезпечення	- окремий інсталяційний пакет, який дозволяє встановлювати клієнта у "ручному" режимі.
2.	Автоматичні виключення	- в залежності від ролей сервера, виключення для специфічних файлів, папок і програм.
3.	Робота в кластерних системах	- можливість роботи в кластерах як домена так і робочої групи.

№ п/п	Функціонал захисту файлового серверу	Вимоги
4.	Робота у режимі серверу терміналів	- можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів.
5.	Сканування Hyper-V	- сканування дисків сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.
6.	Здійснення антивірусного захисту	- перевірка за розкладом і на вимогу за допомогою антивірусних баз даних; - забезпечення захисту в режимі реального часу; - можливість сканування файлів під час запуску системи; - модуль захисту документів; - сканування комп'ютера у неактивному стані; - сканування архівів; - евристичний аналізатор; - виявлення шпигунського ПЗ; - виявлення руткитів; - перевірка скриптів; - захист від ботнетів, технологія яка забезпечує захист від загроз типу "ботнет"; - захист від експлойтів, який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.
7.	Забезпечення захисту електронної пошти	- перевірка поштового трафіку (POP3, POP3S, SMTP, IMAP та IMAPS); - перевірка поштових вкладень; - захист від спаму; - можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
8.	Забезпечення захисту у Web	- перевірка HTTP, HTTPS трафіку; - виявлення та блокування доступу до небезпечних сайтів; - формування дозволених\заборонених\ виключених з перевірки переліків сайтів; - можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.
9.	Наявність проактивного захисту	- забезпечення захисту від троянського ПЗ; - забезпечення захисту від клавіатурних шпигунів; - забезпечення захист від рекламного ПЗ; - забезпечення захисту від фішингу.
10.	Наявність контролю за використанням зовнішніх пристроїв	- автоматична антивірусна перевірка змінних носіїв; - керування доступом до зовнішніх пристроїв; - контроль підключення до сервреру периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою тощо.
11.	Здійснення оновлень	- часті і невеликі за об'ємом оновлення, відновлення завантаження оновлень після обриву зв'язку; - відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну; - можливість мобільним співробітникам отримати оновлення з серверів виробника он-лайн у разі перебування поза корпоративною мережею; - можливість створення дзеркала оновлень засобами антивірусного ПЗ; - наявність оновлень в центрі антивірусного захисту інформації Державної служби спеціального зв’язку та захисту інформації.

№ п/п	Функціонал захисту файлового серверу	Вимоги
12.	Захист віртуальних робочих станцій	- наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.
13.	Операційні системи, які підтримуються	- Microsoft Windows Server 2008 R2; - Microsoft Windows Server 2012; - Microsoft Windows Server 2016. - Microsoft Windows Server 2019; - Microsoft Windows Server 2022; - Microsoft Windows Server 2025; - RedHat Enterprise Linux (RHEL) 8; - RedHat Enterprise Linux (RHEL) 9; - Ubuntu Server 20.04 LTS; - Ubuntu Server 22.04 LTS; - Ubuntu Server 24.04 LTS; - Debian 11; - Debian 12; - SUSE Linux Enterprise Server (SLES) 15; - Alma Linux 8; - Alma Linux 9; - Rocky Linux 8; - Rocky Linux 9; - Oracle Linux 8.

Система управління антивірусним програмним забезпеченням повинна відповідати наступним обов’язковим функціональним вимогам:

№ п/п	Функціонал системи управління	Вимоги
1.	Виявлення комп'ютерів у корпоративній мережі та здійснення управління комп'ютерами	- можливість імпорту з Active Directory, після якого створюється аналогічне дерево груп з користувачами; - можливість виконувати періодичну синхронізацію з Active Directory; - "ручний" імпорт облікових записів в систему; - автоматичне та ручне групування комп'ютерів; - можливість створення багаторівневої структури груп; - можливість виконувати додаткові мережеві дії, такі як: перевірка зв'язку, пробудження віддаленого комп'ютера, перегляд спільних ресурсів, завершення роботи та перезавантаження тощо.
2.	Встановлення клієнтського програмного забезпечення	- віддалена інсталяція/видалення антивірусного програмного забезпечення; - можливість конфігурації інсталяційного пакету; - можливість встановлення інсталяційних пакетів за допомогою системи управління; - можливість "ручного" встановлення клієнта; - автоматичне встановлення клієнта на нові комп'ютери; - віддалена активація/деактивація модулів захисту на окремо взятому клієнті; - можливість здійснювати віддалене встановлення та видалення стороннього ПЗ.
3.	Управління конфігурацією клієнтів	- можливість здійснення централізованого управління конфігурацією клієнтів; - наявність інструменту для створення та редагування інсталяційних пакетів з попередньо встановленими настройками конфігурації; - можливість наслідування політик/конфігурації клієнтів.
4.	Управління інфраструктурою серверів	- наявність можливості встановлення додаткових серверів;

№ п/п	Функціонал системи управління	Вимоги
		- наявність можливості здійснення централізованого управління інфраструктурою серверів; - 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.
5.	Інформування про стан системи антивірусного захисту	- наявність можливості моніторингу антивірусного захисту корпоративної мережі та надання актуальної інформації про стан безпеки; - наявність набору звітів щодо стану системи; - наявність можливості коригування вигляду та налаштування параметрів звітів; - наявність можливості фільтрації інформації у звітах по одному комп'ютеру, групах комп'ютерів тощо; - наявність можливості експорту звітів в інші формати; - наявність можливості сповіщення адміністратора про небезпечні події; - спеціальний компонент, що спрощує виявлення незахищених робочих станцій.
6.	Управління обліковими записами адміністраторів	- 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; - можливість автентифікувати адміністраторів за допомогою груп безпеки Active Directory; - наявність журналу аудиту, у якому відстежуються і реєструються всі зміни в конфігурації та всі дії, які виконують користувачі сервера адміністрування.
7.	Захист з’єднань з сервером управління	- використання сертифікатів для з’єднання з сервером управління, в тому числі і самостійно випущених сертифікатів; - можливість використовувати двофакторну автентифікацію для облікових записів адміністраторів.
8.	Постачання сервера адміністрування	- комплексний інсталяційний пакет, що містить всі необхідні компоненти; - окремі інсталяційні пакети для покомпонентного встановлення; - можливість встановлення серверу адміністрування на ОС Windows та Linux. - образ віртуальної машини з сервером, готовим до використання, для таких віртуальних середовищ, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
9.	Операційні системи, які підтримуються сервером віддаленого управління	- Microsoft Windows Server 2012; Microsoft Windows Server 2012 R2; Microsoft Windows Server 2016; Microsoft Windows Server 2019; Microsoft Windows Server 2022, Microsoft Windows Server 2025. - Ubuntu 20.04 LTS x64;RHEL Server 8 x64;Debian 10 x64;Debian 11 x64;Rocky Linux 9.

Для підтвердження надання послуг у відповідності з вимогами замовника, учасник у складі своєї пропозиції надає:

- гарантійний лист в довільній формі, в якому зазначає інформацію щодо можливості надання послуг відповідно до вимог, передбачених Додатком 2 до тендерної документації замовника, а також інформацію щодо наявності в Україні центру технічної підтримки (виробника програмного

забезпечення або його авторизованого представника) із зазначенням телефонного номеру такого центру;

- документ (оригінал або копію) який підтверджує, що під час надання послуг, що є предметом закупівлі, учасник не порушує законодавство України у сфері авторського права і суміжного права (таким документом може бути копія свідоцтва про реєстрацію авторського права, відповідний ліцензійний/субліцензійний договір або ліцензія (в тому числі невиключна) від компанії **ESET, spol. s r. o.**, якій належать права на програмне забезпечення ESET PROTECT Entry, партнерський сертифікат від компанії **ESET, spol. s r. o.** або її офіційного представництва в Україні,, дійсний протягом 2026 року, що підтверджує статус учасника як офіційного партнера компанії **ESET, spol. s r. o.** та підтверджує його право розповсюджувати програмне забезпечення та/або ліцензії на нього на території України, або відповідний авторизаційний лист від компанії **ESET, spol. s r. o.** чи її офіційного представництва в Україні).

ПЗ має бути сумісне з існуючим сервером централізованого керування та активація антивірусного ПЗ має здійснюватися шляхом додавання ключа до існуючого сервера керування. На підтвердження відповідності пропозиції учасника цій характеристиці на вимогу замовника учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.

Програмні продукти, що входять до запропонованого рішення повинні мати діючі позитивні експертні висновки (сертифіковані) Державною службою спеціального зв'язку та захисту інформації України (далі ДССЗЗІ). На підтвердження учасник надає сканкопію експертного висновку (або інший документ який підтвердить відповідність продуктової лінійки програмного продукту нормативним документам, які регламентують вимоги до засобів технічного захисту інформації, які встановлено законодавством України.

5. **Розмір бюджетного призначення, очікуваної вартості предмета закупівлі**.

Закупівля проводиться на очікувану вартість, яка визначена на основі примірної методики визначення очікуваної вартості предмета закупівлі Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 ««Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі» методом порівняння ринкових цін, шляхом порівняння цінових пропозицій потенційних постачальників товару. Основними джерелами інформації для визначення очікуваної вартості закупівлі товарів брались до уваги: Прайс-листи на сайтах інтернет магазинів постачальників; Інтернет ресурси. Система Prozorro зробила відкритим доступ до публічних закупівель, що дозволяє аналізувати реальні угоди купівлі-продажу інших Замовників, та встановлено наступне:

Відповідно комерційної пропозиції від 05.05.26, ТОВ "Кубіт", Код ЄДРПОУ 38389872, вартість ПЗ на 633 об'єкти буде становити 454240,80 грн (ціна за один 717,60 грн)

Відповідно відповіді на запит від 23.02.2026 Центр інформаційної та технічної підтримки продуктів ESET і рішень технологічного альянсу в Україні, вартість ПЗ 560 об'єктів буде становити 492576,00 грн (ціна за один 879,60 грн).

Відповідно інформації на сайті Softkey вартість ПЗ з ціною за одиницю 2284,80 грн.

Відповідно інформації на сайті Most IT, вартість ПЗ з ціною за одиницю 2277,00 грн.

Одночасно з тим відкриття електронної системи закупівель майданчика прозоро дає змогу відслідковувати реальні пропозиції потенційних надавачів послуг, та встановлено

Відповідно до Тендерна пропозиція/пропозиція UA-2026-05-20-009527-a ФОП Савляк Ганна Василівна, пропонує ПЗ з вартістю за об'єкт 1 220,00 UAH без ПДВ.

Відповідно до Тендерна пропозиція/пропозиція UA-2026-01-23-007688-a ТОВ ""МОСТ АЙ ТІ"" пропонує ПЗ з вартістю за об'єкт (870,97 грн з ПДВ) 725,81 UAH без ПДВ.

Враховуючи вище викладене найнижчу вартість ціну за одиницю з урахуванням кількісної потреби судів, необхідно провести закупівлю **послуги з постачання антивірусного програмного забезпечення**, згідно коду за ДК 021:2015: **48760000-3 «Пакети програмного забезпечення для захисту від вірусів»** у кількості 19 ПОСЛУГ НА 633 об'єкти на суму454240,80 грн.

Розмір бюджетного призначення та/або очікувана вартість предмета закупівлі: Державний бюджет України, **454240,80 грн** з ПДВ