Обґрунтування технічних та якісних характеристик
предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі
(відповідно до пункту 4[1] постанови Кабінету Міністрів України від 11 жовтня 2016 № 710 «Про ефективне використання державних коштів»)

1	Назва предмета закупівлі	**Програмна продукція антивірусного захисту**
2	Обґрунтування технічних та якісних характеристик предмета закупівлі	**Програмна продукція антивірусного захисту - за кодом ДК 021:2015: 48760000-3 «Пакети програмного забезпечення для захисту від вірусів»** **Послуги з постачання програмної продукції антивірусного захисту:** поновлення *програмної продукції "ESET Endpoint Security" з централізованим управлінням та встановленням рішень за допомогою консолі "ESET PROTECT" з поновленням на 1 рік для захисту 763 об'єктів.* Програмні продукти, що входять до запропонованого рішення повинні мати діючі позитивні експертні висновки ДССЗЗІ. Запропоноване ПП має бути сумісне з існуючим сервером централізованого керування та активація антивірусного ПП 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. Запропоноване ПП повинно мати на території України центр технічної підтримки, що авторизований виробником. Технічна підтримка повинна відповідати наступним вимогам: • обслуговування 24x7x365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні, цілодобово; • розширені технічні консультації з питань конфігурації та функціонування антивірусного ПП 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 антивірусного ПП. **ПП має відповідати наступним обов'язковим функціональним вимогам:**

№ 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 захисту	- 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 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.
	Операційні системи, які підтримуються	- Microsoft Windows XP Professional (SP3 та вище); - Microsoft Windows Vista (Professional або вище); - Microsoft Windows 7 (Professional або вище); - Microsoft Windows 10; - Microsoft Windows 11.

ПП 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.
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.
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 2003; - Microsoft Windows Server 2008; - Microsoft Windows Server 2008 R2; - Microsoft Windows Server 2012; - Microsoft Windows Server 2016; - Microsoft Windows Server 2019.

Система управління ПП 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; - 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 2003 SP2; Microsoft Windows Server 2003 R2 SP2; Microsoft Windows Server 2008; Microsoft Windows Server 2008 SP2; Microsoft Windows Server 2008 R2 SP1; Microsoft Windows Server 2012; Microsoft Windows Server 2012 R2; Microsoft Windows Server 2016; Microsoft Windows Server 2019. - Ubuntu 12+; RHEL 5+; CentOS 5+; SLED 11+; SLES 11+; OpenSUSE 13; Debian 7+; Fedora 19+.	
3	Обґрунтування очікуваної вартості предмета закупівлі, розмір бюджетного призначення	450 000,00 грн. (чотириста п'ятдесят тисяч грн. 00 коп.) у т.ч. ПДВ.				

Начальник управління інфраструктури
та господарського забезпечення
Головного управління
ДПС в Одеській області

Олег РУДИЙ