Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі: "ДК 021:2015 "Єдиний закупівельний словник": 48760000-3 Пакети програмного забезпечення для захисту від вірусів (Послуги у сфері інформатизації (Постачання програмної продукції для антивірусного захисту (поновлення)))"

Технічні вимоги

на закупівлю: "ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів (Послуги у сфері інформатизації (Постачання програмної продукції для антивірусного захисту (поновлення)))"

Загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, визначені Правилами забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затвердженими постановою Кабінету Міністрів України від 23.03.2006 № 373, та включають необхідність забезпечення захисту інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 № 463.

Учасник повинен поновити ліцензію на право користування програмною продукцією для антивірусного захисту робочих станцій та серверів ESET PROTECT Entry з локальним управлінням, яке буде використовуватися у корпоративній мережі Замовника, з експертним висновком Державної служби спеціального зв'язку та захисту інформації, дійсним не менш ніж період використання ліцензії.

Програмні продукти, які входять до складу комплексного рішення ESET PROTECT Entry з локальним управлінням:

ESET Endpoint Security для Windows 6.X
ESET Endpoint Security для Windows 7.X
ESET Endpoint Security для Windows 8.X
ESET Endpoint Security для Windows 9.X
ESET Endpoint Antivirus для Windows 6.X
ESET Endpoint Antivirus для Windows 7.X
ESET Endpoint Antivirus для Windows 8.X
ESET Endpoint Antivirus для Windows 9.X
ESET Endpoint Security для Android 2.X
ESET Endpoint Antivirus для Linux 7.X
ESET File Security для Microsoft Windows Server 6.X
ESET File Security для Microsoft Windows Server 7.X
ESET Server Security для Microsoft Windows Server 8.X
ESET Server Security для Microsoft Windows Server 9.X
ESET Server Security для Linux 8.X
ESET File Security для Linux 7.X
ESET File Security для Linux/FreeBSD 4.X

Ліцензійні ключові файли повинні мати можливість відстрочки активації. Термін дії ліцензії – 1 рік, починаючи з моменту активації ліцензійного ключа.

Учасник гарантує високий рівень підтримки програмної продукції виробником впродовж строку дії ліцензії і наявність на території України авторизованого виробником українського центру технічної підтримки та надання технічної підтримки відповідно до наступних вимог:

– 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 антивірусної програмної продукції 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 антивірусної програмної продукції.

Термін дії технічної підтримки – 1 рік, починаючи з моменту активації ліцензійного ключа

Приймання програмної продукції здійснюється за адресою Держстату (01601, м. Київ, вул. Шота Руставелі, 3) шляхом підписання Акту приймання-передачі.

Кількість об’єктів захисту та найменування програмної продукції наведена у таблиці 1:

Таблиця 1

№	Найменування *	Кількість, од.
1.	Програмна продукція ESET Protect Entry з локальним управлінням, поновлення, на 1 рік, для захисту 5380 об'єктів (робочі станції та сервери)	1

*****посилання на конкретну торгівельну марку пов’язане з необхідністю поновлення ліцензії наявної у Замовника програмної продукції**.**

Загальні вимоги:

– загальна кількість об’єктів захисту 5380 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 протягом 1 року.

Запропоноване рішення має відповідати наступним обов'язковим функціональним вимогам:

№ з/п	Функціонал захисту робочої станції	Вимоги
1.	Встановлення програмної продукції	- 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; - можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI; - використання технологій машинного навчання під час первинного аналізу відправлених файлів; - захист від програм-вимагачів;

№ з/п	Функціонал захисту робочої станції	Вимоги
		- 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; - можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах; - перевірка дійсності та цілісності сертифікатів SSL-трафіку та можливість керувати списками довірених сертифікатів та сертифікатів, виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.
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.

№ з/п	Функціонал захисту робочої станції	Вимоги
5.	Веб-контроль	- 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 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.
9.	Вимоги до віддаленого управління	- наявність спеціального компоненту для управління антивірусним захистом на віддалених

№ з/п	Функціонал захисту робочої станції	Вимоги
		робочих станція без необхідності використання додаткових серверів адміністрування.
10.	Операційні системи, які підтримуються	– Microsoft Windows 11, 10, 8.1, 8, 7 SP1 – macOS 10.12 та вище – Ubuntu Desktop 20.04 LTS та 18.04 LTS 64-біт – Red Hat Enterprise Linux 7, 8 64-біт із встановленим підтримуваним середовищем робочого столу – SUSE Linux Enterprise Desktop 15 64-біт Microsoft Windows 10.

Програмна продукція для антивірусного захисту файлових серверів має відповідати наступним обов'язковим функціональним вимогам:

№ з/п	Функціонал захисту файлового серверу	Вимоги
1.	Встановлення програмної продукції	- окремий інсталяційний пакет, який дозволяє встановлювати клієнта у "ручному" режимі (помодульна інсталяція).
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; - вбудована підтримка кластерів.
4.	Контроль швидкодії	- можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
5.	Робота у режимі серверу терміналів	- можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів.
6.	Сканування Hyper-V	- сканування дисків сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.
7.	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; - захист від програм-вимагачів; - виявлення руткитів; - перевірка скриптів; - захист від експлойтів, який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків;

№ з/п	Функціонал захисту файлового серверу	Вимоги
		- захист від ботнетів; - захист від мережевих атак.
8.	Забезпечення захисту електронної пошти	- перевірка поштового трафіку (POP3, POP3S, SMTP, IMAP та IMAPS); - перевірка поштових вкладень; - можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
9.	Веб-контроль	- 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.
10.	Наявність проактивного захисту	- забезпечення захисту від троянського ПЗ; - забезпечення захисту від клавіатурних шпигунів; - забезпечення захист від рекламного ПЗ; - забезпечення захисту від фішингу; - система запобігання вторгненням (HIPS)
11.	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.
12.	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 антивірусної програмнрої продукції; - наявність оновлень в Центрі антивірусного захисту інформації Державної служби спеціального зв’язку та захисту інформації.
13.	Захист віртуальних робочих станцій	- наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.
14.	Операційні системи, які підтримуються	– Microsoft Windows Server 2022, 2019, 2016, 2012, 2008 R2 SP1

№ з/п	Функціонал захисту файлового серверу	Вимоги
		– Microsoft Windows Storage Server 2012, 2008 R2 – Microsoft Windows Small Business Server 2011 – RedHat Enterprise Linux (RHEL) 7, 8 – CentOS 7, 8 – Ubuntu Server 16.04 LTS, 18.04 LTS, 20.04 LTS – Debian 9, 10, 11 – SUSE Linux Enterprise Server (SLES) 12, 15 – Oracle Linux 8 – Amazon Linux 2

Система управління антивірусною програмною продукцією повинна відповідати наступним обов’язковим функціональним вимогам:

№ з/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 клієнтської програмної продукції	- віддалена інсталяція/видалення антивірусної програмної продукції; - 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; - можливість проведення інвентаризації апаратного та програмного забезпечення.
3.	Управління конфігурацією клієнтів	- можливість здійснення централізованого управління конфігурацією клієнтів;

№ з/п	Функціонал системи управління	Вимоги
		- 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 з декількох серверів, розташованих в різних мережах та віддалених географічно.
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;

№ з/п	Функціонал системи управління	Вимоги
		- 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.	Додаткові вимоги	- можливість використання антивірусних продуктів за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту.
10.	Операційні системи, які підтримуються сервером віддаленого управління	- Microsoft Windows Server 2022, 2019, 2016, 2012, 2008 R2 SP1; - Ubuntu 12+; RHEL 5+; CentOS 5+; SLED 11+; SLES 11+; OpenSUSE 13; Debian 7+; Fedora 19+.

Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених для Державної служби статистики Кошторисом на 2023 рік для апарату Держстату за бюджетною програмою КПКВК 0414010 "Керівництво та управління у сфері статистики" по КЕКВ 2240 "Оплата послуг (крім комунальних)".

З метою визначення очікуваної вартості закупівлі послуг з постачання програмної продукції ESET Protect Entry з локальним управлінням (поновлення) проведено аналіз відповідних закупівель, розміщених на порталі електронної системи закупівель https://prozorro.gov.ua/.

Процедури закупівлі аналогічних послуг у 2023 році завершили такі замовники:

- Державне підприємство "Українські спеціальні системи" в інтересах Головне управління ДПС у м. Києві: ДК 021:2015 48760000-3 Пакети програмного забезпечення для захисту від вірусів (послуги з продовження дії ліцензії на програмне забезпечення ESET PROTECT Entry (пакети програмного забезпечення для захисту від вірусів) (https://prozorro.gov.ua/tender/UA-2023-07-13-002553-a) – 1298880,00 грн. Кількість об'єктів захисту відповідно до укладеного договору – 3200 од.;

- Державне спеціалізоване підприємство "Чорнобильська АЕС": ДК 021:2015 код 72260000-5 Послуги, пов`язані з програмним забезпеченням (Послуги щодо надання ліцензій на право річного користування антивірусним програмним продуктом: ESET PROTECT Entry з локальним управлінням (G) (поновлення 590 ліцензій)) (https://prozorro.gov.ua/tender/UA-2023-07-06-007111-a) – 248390,00 грн. Кількість об'єктів захисту відповідно до укладеного договору – 590 од.;

- Територіальне управління Державної судової адміністрації України в Чернівецькій області: ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів (Послуги з постачання антивірусного програмного продукту) (https://prozorro.gov.ua/tender/UA-2023-02-16-010304-a) – 209671,20 грн. Кількість об'єктів захисту відповідно до укладеного договору – 571 од.

Очікувана вартість предмета закупівлі розрахована та уточнена відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275, за методом порівняння ринкових цін на закупівлі, що розміщені на порталі електронної системи закупівель https://prozorro.gov.ua/.

Так, було визначено вартість захисту одного об'єкта, виходячи з ціни договору та кількості об'єктів захисту, та визначено очікувану вартість закупівлі, що розраховується за такою формулою:

Цод = (Ц1 / О1+… + Цк / Ок) / К*З,

де: Цод - очікувана ціна аналогічних послуг;
Ц1, Цк- ціни договорів на надання аналогічних послуг;
О1, Ок- кількість об'єктів захисту, передбачених договорами;
К - кількість цін, отриманих з відкритих джерел інформації;
З - кількість об'єктів захисту в Держстаті

2 142 000 грн ≈ 2 141 418,7 грн = (1298880/3200грн + 248390/590грн + 209671/571грн) / 3 * 5380

Директор департаменту
інформаційних технологій
Держстату Олена ПУЗАНОВА