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 (продовження дії ліцензій (поновлення) програмного забезпечення для комплексного антивірусного та антиспамового захисту інформаційних ресурсів)"

Технічні вимоги

на продовження дії ліцензій (поновлення) програмного забезпечення для комплексного антивірусного та антиспамового захисту інформаційних ресурсів

Відповідно до Технічного завдання на створення комплексної системи захисту інформації (далі - КСЗІ) в інформаційно-телекомунікаційній системі органів державної статистики України (центральний рівень) (далі - ІТС ОДС), нова редакція на заміну ЄААД.468244.276 ТЗ.01, погодженого Адміністрацією Державної служби спеціального зв'язку та захисту інформації України від 10.07.2020, відповідних технічних проєктів, проєктної та експлуатаційної документації на КСЗІ в ІТС ОДС, а також Атестатів відповідності КСЗІ на складові ІТС ОДС, а саме: підсистеми електронної звітності ІТС ОДС (зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 22 грудня 2020 року за № 22359) та програмно-апаратного комплексу автоматизованої системи збору даних статистичної звітності "Кабінет респондента" підсистеми електронної звітності ІТС ОДС (зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 22 грудня 2020 року за № 22360), програмне забезпечення ІТС ОДС складається з системного та функціонального.

До системного програмного забезпечення ІТС ОДС відноситься програмне забезпечення антивірусного захисту. Відповідно до відомостей щодо структури та складу КСЗІ, а також щодо переліку технічних, організаційних, фізичних та інших заходів захисту, які у сукупності складають КСЗІ, до складу комплексу засобів захисту ІТС ОДС входить програмне забезпечення антивірусного захисту ESET (Endpoint Protection Advanced (EES, EFS), ESET File Security для Windows, ESET File Security для Linux, ESET Mail Security).

Учасник повинен надати ліцензії на право користування антивірусним програмним забезпеченням для робочих станцій та серверів, для поштових серверів та поштових скриньок, 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.

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

Замовник самостійно здійснює інсталяцію (активацію) та відновлення програмного забезпечення.

Учасник гарантує високий рівень підтримки програмного забезпечення 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 антивірусного ПЗ 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 ПЗ.

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

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

Кількість об’єктів захисту та назва антивірусного програмного забезпечення наведена у таблиці 1:

Таблиця 1

№	Найменування	Кількість, шт.
1.	Програмне забезпечення як завантажні файли на правах користування ESET Endpoint Protection Advanced (EES, EFS)*. Продовження дії ліцензії (поновлення). Для захисту 7500 об'єктів (робочі станції та сервери) на період 12 місяців, відповідна ліцензія, програмна та експлуатаційна документація на електронному носії інформації та у паперовому вигляді	1
2.	Програмне забезпечення як завантажні файли на правах користування ESET Mail Security*. Продовження дії ліцензії (поновлення). Для захисту 350 об'єктів (поштові сервери та поштові скриньки) на період 12 місяців, відповідна ліцензія, програмна та експлуатаційна документація на електронному носії інформації та у паперовому вигляді	1

***Обґрунтування: посилання на конкретну торгівельну марку пов’язане з необхідністю продовження дії ліцензій (поновлення) наявного у Замовника програмного забезпечення з урахуванням складу комплексу засобів захисту КСЗІ ІТС ОДС.**

Запропоноване рішення має відповідати наступним обов'язковим функціональним вимогам:

№ з/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; - 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; - 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;

№ з/п	Функціонал захисту робочої станції	Вимоги
		- 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.
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.

№ з/п	Функціонал захисту робочої станції	Вимоги
		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 робочих станція без необхідності використання додаткових серверів адміністрування.
10.	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.

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

№ з/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.	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; - виявлення руткитів; - перевірка скриптів; - захист від експлойтів, який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.
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.	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.
10.	Наявність проактивного захисту	- забезпечення захисту від троянського ПЗ; - забезпечення захисту від клавіатурних шпигунів; - забезпечення захист від рекламного ПЗ; - забезпечення захисту від фішингу.

№ з/п	Функціонал захисту файлового серверу	Вимоги
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 антивірусного ПЗ; - 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 2003; - Microsoft Windows Server 2008; - Microsoft Windows Server 2008 R2; - Microsoft Windows Server 2012; - Microsoft Windows Server 2016.

Система управління антивірусним програмним забезпеченням 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

№ з/п	Функціонал системи управління	Вимоги
		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 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;

№ з/п	Функціонал системи управління	Вимоги
		- 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.	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 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; - Ubuntu 12+; RHEL 5+; CentOS 5+; SLED 11+; SLES 11+; OpenSUSE 13; Debian 7+; Fedora 19+.

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

№ з/п.	Вимога	Параметри
1.	Перевірка трафіку	Перевірка вхідного та вихідного поштового трафіку на рівні транспортного протоколу
2.	Вимоги до захисту	Захист бази даних поштових скриньок. Сканування листів в базі даних під час відкриття листа користувачем, в фоновому режимі. Сканування бази даних поштових скриньок за розкладом.

№ з/п.	Вимога	Параметри
		Можливість виявлення реального типу файлу, що дозволяє застосовувати політики для певного типу вмісту електронних листів. Захист від спаму що оснований на використанні комплексу технологій: "чорні" списки реального часу, "чорні" списки серверів на основі DNS, використання цифрових відбитків, перевірка репутації, аналіз вмісту листа, фільтр Байеса, користувальницькі правила, користувальницькі "чорні" та "білі" списки. Робота з "сірими" списками що, основана на специфікації RFC 821. Управління карантином пошти, можливість видаляти або відновлювати листи що потрапили в карантин після сканування. Веб-інтерфейс для управління карантином пошти. Менеджер користувальницьких правил, що дозволяє створювати умови фільтрації електронної пошти та дії, що необхідно виконати з відфільтрованими повідомленнями. Можливість роботи в кластерах як домена так і робочої групи. Комплексний захист сервера, включаючи резидентний захист і сканування на вимогу
3.	Планувальник завдань	Наявність планувальника завдань, який надає можливість створювати на сервері заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів, що виконуються під час запуску системи, створення знімка стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів, оновлення ядра захисту від спаму, оновлення правил ядра захисту від спаму, фонове сканування поштового серверу. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій. Можливість створення на сервері у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску
4.	Оновлення	Можливість створення дзеркала оновлень засобами антивірусного ПЗ
5.	Додаткові вимоги	Наявність eShell рядка, що дозволяє запускати скрипти для виконання дій, а також створювати/змінювати налаштування. Автоматичне створення виключень для критично важливих файлів операційної системи, що забезпечує мінімальний вплив на продуктивність роботи серверу. Можливість віддалено розгорнути, управляти та оновлювати антивірусні продукти для забезпечення безпеки в мережі.

№ з/п.	Вимога	Параметри
		Можливість крім основного вказати резервний сервер адміністрування. Застосування політик, моніторинг виявлень і налаштування програми мають здійснюватися з єдиної консолі. Наявність веб-панелі, що забезпечує повний контроль над корпоративною мережею в режимі реального часу. Можливість створювати докладні та повні журнали і статистику про стан безпеки. Наявність журналу спаму з відображенням відправника, одержувача, оцінку спаму, причину класифікації, а також виконані дії. Наявність журналу «сірих» списків — відображає «сірого» відправника, одержувача, виконані дії та статус. Моніторинг продуктивності сервера в режимі реального часу.

Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених для Державної служби статистики Кошторисом на 2021 рік для апарату Держстату за бюджетною програмою КПКВК 0414010 "Керівництво та управління у сфері статистики" по КЕКВ 2240 "Оплата послуг (крім комунальних)" відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року № 275.

З метою уточнення очікуваної вартості закупівлі послуг із продовження дії ліцензій (поновлення) програмного забезпечення для комплексного антивірусного та антиспамового захисту інформаційних ресурсів на базі програмного забезпечення ESET Endpoint Protection Advanced були підготовлені та надіслані листи-запити цінових пропозицій до Компанії ESET (від 21.05.2021 № 12.3-04/60-21) ТОВ "АМ Інтегратор Груп" (від 24.05.2021 № 12.3-04/61-21), ТОВ "СМАРТЛІНК" (від 24.05.2021 № 12.3-04/61-21).

Відповідь від Компанії ADEON SK, s.r.o. – ексклюзивного дистриб'ютора Компанії ESET на території України (від 02.06.2021 № 2106/1) містить всю необхідну інформацію для визначення очікуваної вартості предмета закупівлі, відповідно до якої рекомендована вартість подовження дії ліцензій становить:

- ESET Endpoint Protection Advanced, строком використання 1 рік, для захисту 7500 об'єктів – 305,90 за 1 шт. без ПДВ;
- ESET Mail Security, строком використання 1 рік, для захисту 350 об'єктів – 228,80 за 1 шт. без ПДВ.

Ураховуючи рекомендації ексклюзивного дистриб'ютора Компанії ESET на території України та можливі коливання курсу валют, розраховано очікувану вартість подовження дії ліцензій (поновлення) програмного забезпечення для комплексного антивірусного та антиспамового захисту інформаційних ресурсів на базі програмного забезпечення ESET Endpoint Protection Advanced в обсязі 2 375 000,00 гривень (7500*305,90+350*228,80=2 374 330,00).

Директор департаменту
інформаційних технологій
Держстату Олена ПУЗАНОВА