В. о. директора СКП «Київтелесервіс»
Чернікову П.О.
Начальника відділу обслуговування програмних та апаратних комплексів
Реут Д.Л.

СЛУЖБОВА ЗАПИСКА

м. Київ

«25» вересня 2023 року

На виконання пункту 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (зі змінами), з метою централізованого придбання антивірусних програмних засобів для забезпечення захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва від зловмисного програмного забезпечення, вважаю за доцільне провести закупівлю послуг згідно переліку:

№	Найменування програмного продукту антивірусного захисту або еквівалент	К-сть ліцензій (одиниці)	Термін дії ліцензії
1	Антивірусне програмне забезпечення (Продовження) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	12440	1 рік
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	500	1 рік

Закупівля здійснюється за кодом CPV за ДК 021:2015 48760000-3 (Пакети програмного забезпечення для захисту від вірусів), орієнтовна вартість якої згідно моніторингу цін становить 5 056 289,48 (п'ять мільйонів п'ятдесят шість тисяч двісті вісімдесят дев'ять) гривень 48 копійок з ПДВ. Фінансування закупівлі здійснюється за рахунок коштів місцевого бюджету (КЕКВ 2610).

У зв'язку із вищезазначеним, надаю детальне обґрунтування даної закупівлі.

Назва предмету закупівлі

Послуги, пов'язані з програмним забезпеченням (48760000-3 Пакети програмного забезпечення для захисту від вірусів)

Обґрунтування доцільності закупівлі

На виконання пункту 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (зі змінами), з метою централізованого придбання антивірусних програмних засобів для забезпечення захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва від зловмисного програмного забезпечення

Обґрунтування обсягів закупівлі

Кількість примірників антивірусного програмного забезпечення сформовано на підставі данних фактичного використання ліцензій станом на 25.09.2023 та надісланих заявок від структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва. Інформація щодо фактичного використання ліцензій наведена в додатку 4.

Обґрунтування якісних характеристик закупівлі

Технічні ті якісні характеристики рекомендовані протоколом № 72 від 23.08.2023 року засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 - 2023 роки. Постачальник повинен поставити Замовнику товар, який відповідає Додатку №1 та чинному законодавству України.

Обґрунтування очікуваної ціни закупівлі

Згідно пункту 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (зі змінами) та за результатами моніторингу цін на підставі отриманих комерційних пропозицій, очікувана вартість закупівлі становить 5 056 289,48 (п'ять мільйонів п'ятдесят шість тисяч двісті вісімдесят дев'ять) гривень 48 копійок з ПДВ. Фінансування закупівлі здійснюється за рахунок коштів бюджету м. Києва (КЕКВ 2610). Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення.

Обґрунтування вибору процедури закупівлі

Відповідно до ст.20 Закону України «Про публічні закупівлі» найбільш прийнятною процедурою для здійснення даної закупівлі є процедура відкритих торгів.

Додатки:

1. Додаток №1. Інформація про необхідні технічні, якісні, кількісні та інші характеристики предмета закупівлі (Технічні вимоги) в 1 прим. на 6 арк.
2. Додаток №2. Кваліфікаційні критерії до учасників в 1 прим. на 2 арк.
3. Додаток №3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) в 1 прим. на 3 арк.
4. Додаток 4. Інформація щодо фактичного використання ліцензій станом на 25.09.2023р.

Відповідальний за розробку технічних вимог
(ініціатор закупівлі) _____ Д. Л. Реут

«ПОГОДЖЕНО»:

Перший заступник директора _____ О.О. Биструшкін

Заступник директора з технічних питань _____ О. Ф. Поліщук

Головний бухгалтер _____ Г. А. Букша

Заступник головного бухгалтера
з економічних питань _____ Ю.В. Волочаєва

Начальник загально-правового
відділу _____ О.М. Тертичний

Додаток 1

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ, КІЛЬКІСНІ ТА ІНШІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ)

Найменування закупівлі: Антивірусне програмне забезпечення (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)

На виконання пункту 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 №5824/5865).

Учасник має право запропонувати еквівалент конкретної торговельної марки чи фірми, патенту, або типу предмета закупівлі, джерела його походження або виробника, які можливо вживаються в тендерній документації, за умови, що такий еквівалент відповідатиме вимогам, встановленим у документації.

№	Найменування програмного продукту антивірусного захисту або еквівалент	К-сть ліцензій (одиниці)	Термін дії ліцензії
1	Антивірусне програмне забезпечення (Продовження) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	12440	1 рік
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	500	1 рік

Технічні вимоги ESET PROTECT Entry

1. **Рішення для захисту робочих станцій під управління серверних та несерверних ОС.**

Вимоги щодо підтримки програмного забезпечення (далі ПЗ):

- Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог викладених нижче), зареєстрованих в Адміністрації Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.

• Запропоноване ПЗ забезпечується в Україні технічною підтримкою через українську службу технічної підтримки, яка працює в режимі 24×7×365 - цілодобово, з можливістю зв'язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку), на підтвердження чого у складі своєї тендерної пропозиції надається лист від виробника або його ексклюзивного дистриб'ютора щодо наявності в Україні авторизованого центру технічної підтримки.
• Можливість отримувати розширені технічні консультації з питань конфігурації та функціонування антивірусного програмного забезпечення по телефону та електронній пошті.
• Можливість розподілу захисту між робочими місцями та файловими серверами в будь-якій пропорції в межах кількості об'єктів, на яку придбаний антивірусний захист.
• Доступність всієї функціональності в рамках зазначеного програмного забезпечення, без додаткових придбань.
• Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.

ПЗ забезпечує:

• Надання захисту від: шкідливих програм, шпигунського, троянського та рекламного програмного забезпечення, клавіатурних шпигунів, фішингу, руткітів, скриптів, потенційного небажаного та небезпечного програмного забезпечення, мережевих атак, спаму.
• Можливість використання технології, яка забезпечує захист від загроз типу ботнет.
• Захист від експлойтів, який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.
• Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
• Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі в інтерфейсі UEFI.
• Захист вразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
• Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.
• Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
• Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
• Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, що дасть можливість більш ефективно перевіряти POP3, POP3S, SMTP, IMAP та IMAPS та забезпечити перевірку поштових вкладень.
• Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті
• Модуль захисту документів, який перевіряє макроси на наявність зловмисного коду.
• Наявність модуля захисту від спаму з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мереж.
• Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх так і локальних мережевих атак.
• Можливість створювати для персонального брандмауеру різні профілі, які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
• Забезпечення захисту в режимі реального часу, можливість сканування файлів під час запуску системи та сканування комп'ютера у неактивному стані.
• Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій

сайтів.
• Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
• Наявність додаткового модуля, який дає можливість запускати браузери у захищеному режимі з метою блокування спроб втручання в область пам'яті браузера та вмісту його вікон, а також додаткового захисту критичних інтернет з'єднань таких як інтернет-платежі та інтернет-банкінг тощо.
• Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
• Наявність системи запобігання вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру для більш гнучкого налаштування правил для не популярних процесів.
• 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.
• Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
• Можливість отримання оновлення вірусних баз з локального дзеркала на сервері, з загальної мережевої папки або з носія інформації та можливість створення дзеркала оновлень засобами антивірусного ПЗ та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
• Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника онлайн, у разі перебування поза корпоративною мережею.
• Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом для перевірки ПК в ізольованих мережах різних класів захищеності
• Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
• Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи;
• Можливість роботи в кластерах як домена так і робочої групи.
• Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування цим самим регулювати навантаження в серверних системах для оптимального використання серверних ресурсів.
• Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
• Можливість встановлення агенту управління на ARM64 процесорах.
• Наявність функціональності створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
• Наявність функціональності визначення адміністратора площадки або філії з відповідною частиною ліцензії.
• Можливість використання ПЗ за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту. 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.

- Захист ОС під управлінням:
  - Microsoft Windows 11, 10, 8.1, 8, 7 (SP1);
  - Microsoft Windows Server 2022, 2019, 2016, 2012, 2008 (R2 SP1);
  - Microsoft Windows Storage Server 2016, 2012, 2008 (R2 SP1);
  - Microsoft Windows MultiPoint Server 2012, 2011, 2010;
  - Microsoft Windows Small Business Server 2011, 2008;

  - MacOS 10.9 та вище;
  - iOS 9 та вище;
  - Android 5 (Lollipop) та вище;

- Ubuntu Desktop 18.04 LTS 64-bit и RedHat Enterprise Linux (RHEL) Desktop 7 64-bit
- Ubuntu Server 16.04 LTS 64-bit, 18.04 LTS 64-bit
- RedHat Enterprise Linux (RHEL) 7, 8;
- CentOS 7, 8;
- Debian 9, 10;
- SUSE Linux Enterprise Server (SLES) 12 64-bit, 15 64-bit;
- Oracle Linux 8;
- Amazon Linux 2;

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

1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати ценралізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам.
3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
5. Віддалена інсталяція антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac на кілька кінцевих точок одночасно.
6. Віддалена інсталяція користувальницького програмного забезпечення.
7. Можливість віддаленого видалення встановленого користувальницького програмного забезпечення.
8. Віддалене видалення антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac
9. 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 операційної системи клієнтського комп'ютера.
10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac 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.
11. 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 захиту.

12. Можливість аутентифікувати адміністраторів консолі керування за допомогою груп безпеки Active Directory.
13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.
14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.
15. Можливість віддалено активувати та деактивувати модулі захисту, такі як персональний брандмауер, захист в режимі реального часу, захист поштового клієнта, захист доступу до Інтернету, контроль пристроїв, веб-контроль, антиспам на окремо взятому клієнті.
16. Можливість створювати та редагувати статичні групи та можливість імпорту з Active Directory дерева комп'ютерів.
17. Можливість налаштування автоматичного розподілу клієнтів по динамічних группах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
18. Можливість імпорту користувачів та груп з Active Directory, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
19. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.
20. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
21. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
22. 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.
23. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
24. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM
25. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.
26. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
27. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
28. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шлягом з'єднання, захищеного сертифікатом.
29. 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 операційної системи.
30. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
31. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях
32. Спецільний компонент, який здійснює виявлення в мережі незахищенних робочих станцій для подальшого розгортання антивірусного захисту.
33. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.
34. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування.

35. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу
36. Можливість встановлення серверу адміністрування на ОС Windows та Linux
37. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
38. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+
39. Можливість визначати, яка віртуальна машина буде джерелом для копіювання або клонування у системах VDI.
40. Наявність майстра налаштування для визначення детальних параметрів для інтеграції з системами VDI
41. Можливість обирати варіанти обробки ідентифікаторів клонованих комп'ютерів, такі як зіставляння з наявними комп'ютерами або створення нових комп'ютерів.
42. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.
43. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну індентифікацію клонованнних машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.
44. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
45. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
46. Можливість встановлення агенту управління на ARM64 процесорах.
47. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензції окремим філіям.
48. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, з метою встановлення джерела постачання та наявності гарантій виробника на програмне забезпечення, що пропонується Учасником до постачання, учасником у складі тендерної пропозиції надається:

авторизаційний та/або інформаційний лист від виробника або його офіційного представника на території України відповідного ліцензійного програмного забезпечення, яке пропонується Учасником до постачання, що адресований на ім'я Замовника із посиланням на цю процедуру закупівлі.

**У разі використання в даному документі посилань на конкретні торговельну марку, фірму, назву або тип предмета закупівлі, джерело його походження або виробника, після такого посилання слід вважати в наявності вираз "або еквівалент". При цьому відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 №287/2015, еквівалентне ліцензійне програмне забезпечення не повинно бути розробленим у Російській Федерації.*

Начальник відділу обслуговування програмних та апаратних комплексів **Реут Д.Л.**

Додаток №2

Кваліфікаційні критерії, вимоги та документи, які вимагаються для підтвердження відповідності пропозиції учасника кваліфікаційним критеріям та іншим вимогам замовника

Для участі у процедурі закупівлі учасники повинні відповідати кваліфікаційним критеріям та іншим вимогам, наведеним у таблиці.

Вимога	**Підтвердження відповідності (перелік документів, що вимагаються від учасника)**
1. Кваліфікаційні критерії до учасника та спосіб їх документального підтвердження	
Кваліфікаційні критерії, встановлені відповідно до статті 16 Закону	**Документальне підтвердження наявності кваліфікаційних критеріїв**
1. Наявність документально підтвердженого досвіду виконання аналогічного договору *В цій тендерній документації під аналогічним договором слід розуміти договір на поставку з аналогічного предмету закупівлі, який зазначено в даній документації	1.1. Довідка у довільній формі про наявність досвіду виконання аналогічного договору за період з 2014 року по теперішній час із зазначенням найменування контрагента, предмету договору, строку дії договору. Разом з довідкою учасник повинен надати копію договору, зазначеного у довідці з усіма наявними додатками, зазначеними у договорі, на який надано лист-відгук (рекомендацію тощо), від контрагента (контрагентів), зазначеного у довідці із зазначенням в ньому дати укладання і номеру договору, на який надано лист-відгук (рекомендацію тощо).

Начальника відділу обслуговування програмних та апаратних комплексів **Реут Д.Л.**

Постачальник:
ТОВ «СПАН»
Україна, 04070 м. Київ,
вул. Набережно-Хрещатицька, буд. 9
Телефон +380 44 362 22 11

Покупець:
Київтелесервіс

Комерційна пропозиція №071_20230920_IS

від 20.09.2023 року

№	Назва продукту	Кількість	Ціна, грн, з ПДВ	Сума, грн, з ПДВ
1	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік. Поновлення. Для захисту 12440 об'єктів.	1	4 812 787,20	4 812 787,20
2	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік. Пільгова. Понад 12440. Для захисту 500 об'єктів	1	193 440,00	193 440,00
			Всього сума грн, з ПДВ	5 006 227,20

Ціни та ПДВ

Ціни вказані в ГРН з ПДВ

Умови оплати

Оплата здійснюється не пізніше 10 календарних днів після поставки

Строк постачання

10 календарних днів з дати підписання договору

Комерційну пропозицію підготував
Ігор Смірнов
Менеджер з рішень – IT Безпека
Igor.smirnov@span.eu| M +380 67 467 3473

SOFTNET GROUP

Вих. №52/09-13092024

від 14 вересня 2023 року

СПЕЦІАЛІЗОВАНЕ КОМУНАЛЬНЕ ПІДПРИЄМСТВО «КИЇВТЕЛЕСЕРВІС»

щодо надання комерційної пропозиції' на антивірусне програмне забезпечення (Продовження дії) ESET

Комерційна пропозиція ТОВ «СОФТНЕТ ГРУП» від 14 вересня 2023 року

На Ваше звернення щодо отримання комерційної пропозиції від нашої компанії, **ТОВ «СОФТНЕТ ГРУП»** після детального аналізу запиту надаємо комерційну пропозицію за специфікацією послуг.

№	Товар	Кількість		Ціна без ПДВ	Сума з ПДВ
1	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік. Поновлення. Для захисту 12440 об'єктів.	1	шт	**4 010 656,00**	**4 812 787,20**
2	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік. Для захисту 500 об'єктів.	1	шт	**161 200,00**	**193 440,00**
Загальна вартість ліцензій на 12 місяців, грн, з ПДВ					**5 006 227, 20**

Загальна вартість послуг за цією комерційною пропозицією становить **5 006 227 грн. 20** коп. (п'ять мільйонів шість тисяч двісті двадцять сім грн) 20 коп. **з ПДВ.**

Умови цієї комерційної пропозиції можуть бути деталізовані та уточнені після ознайомлення із вимогами відповідної тендерної документації планової закупівлі.

З повагою та надією на співробітництво,

Директор ТОВ «СОФТНЕТ ГРУП» **М. В. Тихонов**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 209/09-2023
Від 14 09 2023 р.

ТОВ "СОФТНЕТ ГРУП"
ЄДРПОУ 42952398,
П/р № 33305299000026004036703983
у АТ КБ «Приватбанк», МФО 380775

ЮРИДИЧНА АДРЕСА:
м.Київ, вул. О. Пироговського, буд. 19/4.
Тел. +38 044 393 93 23

ФАКТИЧНА АДРЕСА:
м.Київ, вул. О. Пироговського, буд. 19/4.
Тел. +38 044 393 93 23

ТОВ «АЛЕСТА»
ЄДРПОУ 42232756 **ІПН** 422327526530
www.alesta.net.ua | info@alesta.net.ua | +380 44 377 73 11
01135, Україна, Київ, вул. Дмитрівська №66а, офіс 65

В.о. Директора
СКП "КИЇВТЕЛЕСЕРВІС"
Павлу ЧЕРНІКОВУ

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

На ваш запит від 13.09.2023 року за № 292-09/2023 ТОВ «АЛЕСТА» надає інформацію щодо орієнтовної вартості ліцензійного антивірусного програмного забезпечення по закупівлі **«48760000-3 «Закупівля антивірусного програмного забезпечення» за ДК 021:2015 Єдиного закупівельного словника»**.

Повідомляємо, що орієнтовна вартість запропонованого програмного забезпечення складає **5 156 414,04** грн (п'ять мільйонів сто п'ятдесят шість тисяч чотириста чотирнадцять гривень 04 копійки) в тому числі з ПДВ **859 402,34** (вісімсот п'ятдесят дев'ять тисяч чотириста дві гривні 34 копійки).

Специфікація та вартість програмного забезпечення наведена у таблиці:

№	Найменування програмного продукту антивірусного захисту	К-сть ліцензій (одиниці)	Термін дії ліцензії	Вартість без ПДВ, грн.
1	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік. Поновлення.	12 440	1 рік	4 130 975,70
2	Програмна продукція 'ESET PROTECT Entry з локальним управлінням' (К). На 1 рік.	500	1 рік	166 036,00
			Всього без ПДВ, грн:	**4 297 011,70**
			ПДВ, грн:	**859 402,34**
			Всього з ПДВ, грн:	**5 156 414,04**

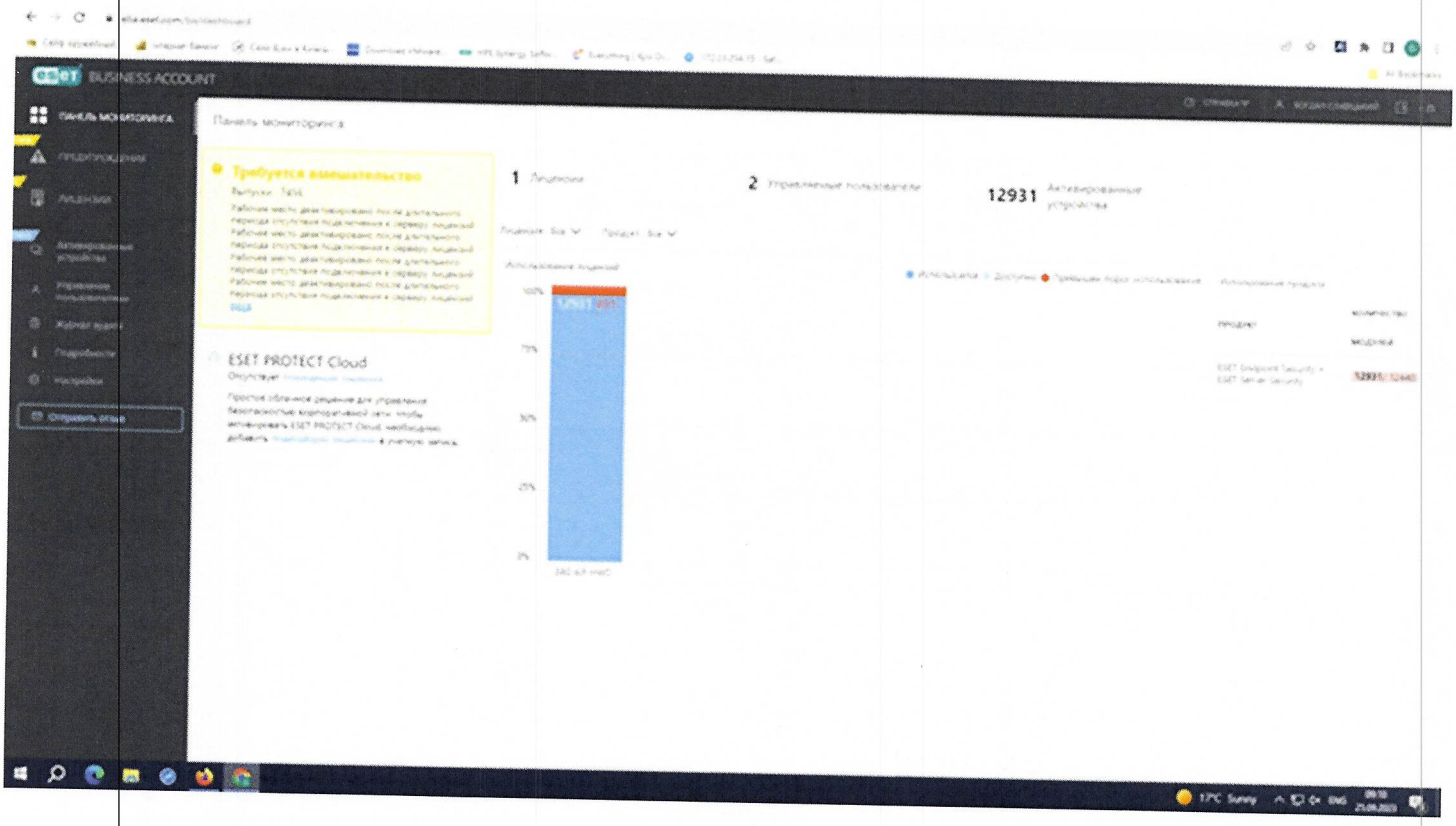
14.09.2023 року
Директор ТОВ «АЛЕСТА» **Анатолій БЛІНОВ**

Україна * Товариство з обмеженою відповідальністю * м. Київ
«АЛЕСТА»
ідентифікаційний код 42232756

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 208/09-2023
Від 14 09 2023 р.

Додаток 4.

Інформація щодо фактичного використання ліцензій станом на 25.09.2023 р.



ПРОТОКОЛ № 72

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 - 2023 роки

м. Київ «23» серпня 2023 року

ПРИСУТНІ:

Члени робочої групи:

А. Вовнюк
М. Журбенко
В. Жучков
В. Іцкович
С. Осіпов
О. Поліщук
Д. Рябіченко
Т. Самойленко
М. Спічка
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019–2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (зі змінами) (далі – Програма), у 2023 році, а саме:

1.1 проєкт технічних вимог до закупівлі «Обладнання для розвитку комплексної системи відеоспостереження та системи забезпечення безпеки» (пункт 11.1 «Розвиток, супровід та технічна підтримка комплексної системи відеоспостереження та систем забезпечення безпеки у м. Києві із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми)

1.2 проєкт технічних вимог до закупівлі «Послуга по встановленню спеціальних засобів зв'язку (засоби відеозв'язку/відеофіксації) для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 11.1 «Розвиток, супровід та технічна підтримка комплексної системи відеоспостереження та систем забезпечення безпеки у м. Києві із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.3 проєкт технічних вимог до закупівлі «Антивірусне програмне забезпечення» (пункт 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Програми).

2. Обговорення питання щодо рекомендацій Департаменту внутрішнього фінансового контролю та аудиту виконавчого органу Київської міської ради (Київської міської державної адміністрації) підвищення професійної компетенції працівників, що здійснюють погодження та контроль закупівель у межах виконання завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки.

По пункту 1.1 – 1.2 питання 1

СЛУХАЛИ:

М. Спічку, який поінформував, що з метою розвитку комплексної системи відеоспостереження міста Києва та облаштування відеонаглядом нових локацій на території міста Києва необхідно придбати обладнання та послугу із встановлення спеціальних засобів зв'язку (засоби відеозв'язку/відеофіксації) та представив проєкти технічних вимог до відповідних закупівель «Обладнання для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуга по встановленню спеціальних засобів зв'язку (засоби відеозв'язку/відеофіксації) для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 11.1 переліку завдань і заходів Програми).

В обговоренні брали участь: О. Поліщук.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівель «Обладнання для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуга по встановленню спеціальних засобів зв'язку (засоби відеозв'язку/відеофіксації) для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки»» (пункт 11.1 переліку завдань і заходів Програми) використовувати проєкти технічних вимог, розглянуті на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 10, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По пункту 1.3 питання 1

СЛУХАЛИ:

М. Журбенка, який поінформував, що у зв'язку із закінченням терміну дії ліцензій антивірусного програмного забезпечення для забезпечення антивірусним захистом автоматизованих робочих місць користувачів структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних

адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, необхідно централізовано закупити антивірусне програмне забезпечення та представив проєкт технічних вимог до закупівлі «Антивірусне програмне забезпечення» (пункт 16.20 переліку завдань і заходів Програми).

В обговоренні брали участь: Д. Рябіченко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Антивірусне програмне забезпечення» (пункт 16.20 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 10, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По питанню 2

СЛУХАЛИ:

В. Іцкович, яка поінформувала, що за результатами планового аудиту з оцінки діяльності спеціалізованого комунального підприємства «Київтелесервіс» щодо ефективності виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки в частині закупівлі антивірусного програмного забезпечення Департамент внутрішнього фінансового контролю та аудиту виконавчого органу Київської міської ради (Київської міської державної адміністрації) листом від 21.07.2023 № 070-6-08/1187 надав план заходів із рекомендаціями.

Виконання рекомендованого заходу № 12 відноситься до повноважень Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) як головного виконавця Програми. Для уникнення ризику неефективного, нераціонального використання бюджетних коштів на антивірусне програмне забезпечення через неналежне планування потреби в його кількості рекомендовано посилити внутрішній контроль за процесом закупівлі антивірусного програмного забезпечення та його подальшим використанням, а також підвищити професійну компетенцію працівників, що здійснюють погодження та контроль закупівель.

Ураховуючи зазначене, з метою забезпечення ефективного виконання заходів Програми необхідно посилити у комунальних підприємствах контроль за проведенням усіх закупівель у межах реалізації відповідних проєктів, відповідально ставитися до розробки технічних вимог до закупівель, звертати увагу на використання програмного забезпечення надійних та перевірених виробників, щоб мати впевненість у застосуванні програмних засобів протягом усього терміну дії ліцензії, а також залучати до розробки та погодження технічних вимог до закупівель найбільш фахових працівників Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської

ради (Київської міської державної адміністрації) та комунальних підприємств, провести відповідні навчання/підвищення кваліфікації.

В обговоренні брали участь: О. Поліщук, Т. Самойленко.

УХВАЛИЛИ:

Посилити контроль за процесом розробки та погодження технічних вимог до закупівель у межах реалізації завдань і заходів Програми, залучати під час розробки та погодження технічних вимог найбільш фахових працівників Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) та комунальних підприємств.

ГОЛОСУВАЛИ: «ЗА» - 10, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1851
Дата реєстрації 23.08.2023
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 23.08.2023 (Протокол № 72 від 23.08.2023)

Кількість файлів: 4
Кількість ЕП: 42

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
23.08.2023 № 075-1851

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Жучков Василь Анатолійович **Кількість ЕП:** 4	24.08.2023 12:01:31 ; 24.08.2023 12:01:31 ; 24.08.2023 12:01:32 ; 24.08.2023 12:01:33 ;	24.08.2023 12:01:33 Погодив;	24.08.2023 12:01:33 Погодив
Спічка Максим Олегович **Кількість ЕП:** 4	24.08.2023 10:15:15 ; 24.08.2023 10:15:16 ; 24.08.2023 10:15:16 ; 24.08.2023 10:15:17 ;	24.08.2023 10:15:17 Погодив;	24.08.2023 10:15:17 Погодив
ВОВНЮК АНАТОЛІЙ ВІТАЛІЙОВИЧ **Кількість ЕП:** 4	24.08.2023 09:15:47 ; 24.08.2023 09:15:48 ; 24.08.2023 09:15:48 ; 24.08.2023 09:15:49 ;	24.08.2023 09:15:49 Погодив;	24.08.2023 09:15:49 Погодив
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 4	23.08.2023 18:28:09 ; 23.08.2023 18:28:09 ; 23.08.2023 18:28:10 ; 23.08.2023 18:28:11 ;	23.08.2023 18:28:11 Погодив;	23.08.2023 18:28:11 Погодив

ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 4	23.08.2023 17:46:21 ; 23.08.2023 17:46:22 ; 23.08.2023 17:46:22 ; 23.08.2023 17:46:23 ;	23.08.2023 17:46:23 Погодив;	23.08.2023 17:46:23 Погодив
РЯБІЧЕНКО ДМИТРО ВОЛОДИМИРОВИЧ **Кількість ЕП:** 4	23.08.2023 17:35:39 ; 23.08.2023 17:35:49 ; 23.08.2023 17:36:00 ; 23.08.2023 17:36:11 ;	23.08.2023 17:36:12 Погодив;	23.08.2023 17:36:11
Самойленко Тамара Анатоліївна **Кількість ЕП:** 4	23.08.2023 16:48:47 ; 23.08.2023 16:49:06 ; 23.08.2023 16:49:13 ; 23.08.2023 16:49:17 ;		23.08.2023 16:49:17
Журбенко Максим Анатолійович **Кількість ЕП:** 4	23.08.2023 16:21:29 ; 23.08.2023 16:21:29 ; 23.08.2023 16:21:30 ; 23.08.2023 16:21:30 ;	23.08.2023 16:21:30 Погодив;	23.08.2023 16:21:30 Погодив
Журбенко Максим Анатолійович **Кількість ЕП:** 4	23.08.2023 16:21:29 ; 23.08.2023 16:21:29 ; 23.08.2023 16:21:30 ; 23.08.2023 16:21:30 ;	23.08.2023 16:21:30 Погодив;	23.08.2023 16:21:30 Погодив

Поліщук Олег Федорович **Кількість ЕП:** 5	23.08.2023 16:19:49 ; 23.08.2023 16:19:51 ; 23.08.2023 16:19:52 ; 23.08.2023 16:19:53 ; 23.08.2023 16:20:40 ;	23.08.2023 16:19:53 Погодив;	23.08.2023 16:20:40
Іцкович Вікторія Євгенівна **Кількість ЕП:** 4	23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ;	23.08.2023 15:52:35 Погодив;	23.08.2023 15:52:35 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 4	23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ;	23.08.2023 15:52:35 Погодив;	23.08.2023 15:52:35 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 4	23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ;	23.08.2023 15:52:35 Погодив;	23.08.2023 15:52:35 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 4	23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ; 23.08.2023 15:52:35 ;	23.08.2023 15:52:35 Погодив;	23.08.2023 15:52:35 Погодив

Лисик Ганна Миколаївна **Кількість ЕП:** 1	23.08.2023 15:51:57 ;	23.08.2023 15:51:57 Погодив;	23.08.2023 15:51:57 Погодив

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ, КІЛЬКІСНІ ТА ІНШІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ)

Найменування закупівлі: Антивірусне програмне забезпечення (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)

На виконання пункту 16.20 «Закупівля антивірусного програмного забезпечення» переліку завдань і заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 №5824/5865).

Учасник має право запропонувати еквівалент конкретної торговельної марки чи фірми, патенту, або типу предмета закупівлі, джерела його походження або виробника, які можливо вживаються в тендерній документації, за умови, що такий еквівалент відповідатиме вимогам, встановленим у документації.

№	Найменування програмного продукту антивірусного захисту або еквівалент	К-сть ліцензій (одиниці)	Термін дії ліцензії
1	Антивірусне програмне забезпечення (Продовження) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	12440	1 рік
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	500	1 рік

Технічні вимоги ESET PROTECT Entry

1. **<u>Рішення для захисту робочих станцій під управління серверних та несерверних ОС.</u>**

Вимоги щодо підтримки програмного забезпечення (далі ПЗ):

- Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог викладених нижче), зареєстрованих в Адміністрації Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.
- Запропоноване ПЗ забезпечується в Україні технічною підтримкою через українську службу технічної підтримки, яка працює в режимі 24×7×365 - цілодобово, з можливістю

зв'язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку), на підтвердження чого у складі своєї тендерної пропозиції надається лист від виробника або його ексклюзивного дистриб'ютора щодо наявності в Україні авторизованого центру технічної підтримки.

• Можливість отримувати розширені технічні консультації з питань конфігурації та функціонування антивірусного програмного забезпечення по телефону та електронній пошті.

• Можливість розподілу захисту між робочими місцями та файловими серверами в будь-якій пропорції в межах кількості об'єктів, на яку придбаний антивірусний захист.

• Доступність всієї функціональності в рамках зазначеного програмного забезпечення, без додаткових придбань.

• Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.

ПЗ забезпечує:

• Надання захисту від: шкідливих програм, шпигунського, троянського та рекламного програмного забезпечення, клавіатурних шпигунів, фішингу, руткітів, скриптів, потенційного небажаного та небезпечного програмного забезпечення, мережевих атак, спаму.

• Можливість використання технології, яка забезпечує захист від загроз типу ботнет.

• Захист від експлойтів, який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.

• Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.

• Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі в інтерфейсі UEFI.

• Захист вразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.

• Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.

• Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.

• Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування

• Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, що дасть можливість більш ефективно перевіряти POP3, POP3S, SMTP, IMAP та IMAPS та забезпечити перевірку поштових вкладень.

• Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті

• Модуль захисту документів, який перевіряє макроси на наявність зловмисного коду.

• Наявність модуля захисту від спаму з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мереж.

• Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх так і локальних мережевих атак.

• Можливість створювати для персонального брандмауеру різні профілі, які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.

• Забезпечення захисту в режимі реального часу, можливість сканування файлів під час запуску системи та сканування комп'ютера у неактивному стані.
• Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
• Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
• Наявність додаткового модуля, який дає можливість запускати браузери у захищеному режимі з метою блокування спроб втручання в область пам'яті браузера та вмісту його вікон, а також додаткового захисту критичних інтернет з'єднань таких як інтернет-платежі та інтернет-банкінг тощо.
• Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
• Наявність системи запобігання вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру для більш гнучкого налаштування правил для не популярних процесів.
• 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.
• Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
• Можливість отримання оновлення вірусних баз з локального дзеркала на сервері, з загальної мережевої папки або з носія інформації та можливість створення дзеркала оновлень засобами антивірусного ПЗ та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
• Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника онлайн, у разі перебування поза корпоративною мережею.
• Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом для перевірки ПК в ізольованих мережах різних класів захищеності
• Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
• Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи;
• Можливість роботи в кластерах як домена так і робочої групи.
• Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування цим самим регулювати навантаження в серверних системах для оптимального використання серверних ресурсів.
• Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
• Можливість встановлення агенту управління на ARM64 процесорах.
• Наявність функціональності створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
• Наявність функціональності визначення адміністратора площадки або філії з

відповідною частиною ліцензії.

• Можливість використання ПЗ за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту. 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.

• Захист ОС під управлінням:
- Microsoft Windows 11, 10, 8.1, 8, 7 (SP1);
- Microsoft Windows Server 2022, 2019, 2016, 2012, 2008 (R2 SP1);
- Microsoft Windows Storage Server 2016, 2012, 2008 (R2 SP1);
- Microsoft Windows MultiPoint Server 2012, 2011, 2010;
- Microsoft Windows Small Business Server 2011, 2008;

- MacOS 10.9 та вище;
- iOS 9 та вище;
- Android 5 (Lollipop) та вище;

- Ubuntu Desktop 18.04 LTS 64-bit и RedHat Enterprise Linux (RHEL) Desktop 7 64-bit
- Ubuntu Server 16.04 LTS 64-bit, 18.04 LTS 64-bit
- RedHat Enterprise Linux (RHEL) 7, 8;
- CentOS 7, 8;
- Debian 9, 10;
- SUSE Linux Enterprise Server (SLES) 12 64-bit, 15 64-bit;
- Oracle Linux 8;
- Amazon Linux 2;

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

1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати ценралізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам.
3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
5. Віддалена інсталяція антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac на кілька кінцевих точок одночасно.
6. Віддалена інсталяція користувальницького програмного забезпечення.
7. Можливість віддаленого видалення встановленого користувальницького програмного забезпечення.
8. Віддалене видалення антивірусного програмного забезпечення для операційних систем Windows, Linux та Mac
9. 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 операційної системи клієнтського комп'ютера.

10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac 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.
11. 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 захиту.
12. Можливість аутентифікувати адміністраторів консолі керування за допомогою груп безпеки Active Directory.
13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.
14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.
15. Можливість віддалено активувати та деактивувати модулі захисту, такі як персональний брандмауер, захист в режимі реального часу, захист поштового клієнта, захист доступу до Інтернету, контроль пристроїв, веб-контроль, антиспам на окремо взятому клієнті.
16. Можливість створювати та редагувати статичні групи та можливість імпорту з Active Directory дерева комп'ютерів.
17. Можливість налаштування автоматичного розподілу клієнтів по динамічних группах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
18. Можливість імпорту користувачів та груп з Active Directory, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
19. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.
20. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
21. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
22. 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.
23. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
24. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM
25. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50

шаблонів для різних систем/клієнтів.

26. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
27. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
28. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шлягом з'єднання, захищеного сертифікатом.
29. 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 операційної системи.
30. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
31. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях
32. Спецільний компонент, який здійснює виявлення в мережі незахищенних робочих станцій для подальшого розгортання антивірусного захисту.
33. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.
34. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування.
35. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу
36. Можливість встановлення серверу адміністрування на ОС Windows та Linux
37. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
38. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+
39. Можливість визначати, яка віртуальна машина буде джерелом для копіювання або клонування у системах VDI.
40. Наявність майстра налаштування для визначення детальних параметрів для інтеграції з системами VDI
41. Можливість обирати варіанти обробки ідентифікаторів клонованих комп'ютерів, такі як зіставляння з наявними комп'ютерами або створення нових комп'ютерів.
42. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.
43. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну індентифікацію клонованнних машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.
44. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
45. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
46. Можливість встановлення агенту управління на ARM64 процесорах.
47. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензції окремим філіям.
48. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, з метою встановлення джерела постачання та наявності гарантій виробника на програмне забезпечення, що пропонується Учасником до постачання, учасником у складі тендерної пропозиції надається:

авторизаційний та/або інформаційний лист від виробника або його офіційного представника на території України відповідного ліцензійного програмного забезпечення, яке пропонується Учасником до постачання, що адресований на ім'я Замовника із посиланням на цю процедуру закупівлі.

**У разі використання в даному документі посилань на конкретні торговельну марку, фірму, назву або тип предмета закупівлі, джерело його походження або виробника, після такого посилання слід вважати в наявності вираз "або еквівалент". При цьому відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 №287/2015, еквівалентне ліцензійне програмне забезпечення не повинно бути розробленим у Російській Федерації.*