

То К-Етими
до Котенки
сррр

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

СЛУЖБОВА ЗАПИСКА

м. Київ

«28» травня 2021 року

На виконання пункту 16.20. «Закупівля антивірусного програмного забезпечення» та заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 18.12.2018 № 461/6512, 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) від зловмисного програмного забезпечення з ліцензією на право їх використання, вважаю за доцільне провести закупівлю ліцензій: Пакети програмного забезпечення для захисту від вірусів – за кодом CPV за ДК 021:2015 – 48760000-3 (закупівля антивірусного програмного забезпечення) за процедурою відкритих торгів з публікацією англійською мовою, орієнтовна вартість якої згідно моніторингу цін становить 3 460 000 (три мільйони чотириста шістьдесят тисяч) гривень 00 копійок без ПДВ. Фінансування закупівлі здійснюється за рахунок коштів місцевого бюджету (КЕКВ 2610).

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

Назва предмету закупівлі

Код за ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів (Закупівля антивірусного програмного забезпечення)

Обґрунтування доцільності закупівлі

На виконання пункту 16.20. «Закупівля антивірусного програмного забезпечення» та заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 18.12.2018 № 461/6512, з метою централізованого придбання антивірусного програмного забезпечення для захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації) від зловмисного програмного забезпечення з ліцензією на право їх використання.

Обґрунтування обсягів закупівлі

Станом на 01.01.2021 р. загальна кількість робочих станцій, що належать установам, підприємствам, структурним підрозділам виконавчого органу Київської міської ради (Київської міської державної адміністрації) та захищена антивірусним програмним забезпеченням ESET Endpoint Protection Advanced становить 12 440 одиниць.

Враховуючи вище наведене, для забезпечення захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації) від зловмисного програмного забезпечення, та діючи в рамках існуючих бюджетних призначень, вважаю за необхідне здійснити закупівлю (продовження дії)

наступної кількості ліцензій Антивірусного програмного забезпечення ESET Endpoint Protection Advanced у кількості 12 440 одиниць.

Обґрунтування якісних характеристик закупівлі

Постачальник повинен поставити Замовнику програмне забезпечення, яке відповідає Додатку №1 та чинному законодавству України.

Обґрунтування очікуваної ціни закупівлі

Згідно пункту 16.20 Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки, затвердженої рішенням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 18.12.2018 № 461/6512 та за результатами моніторингу цін на аналогічні послуги, очікувана вартість закупівлі становить 3 460 000 (три мільйони чотириста шістьдесят тисяч) **грн 00 коп. без ПДВ**. Фінансування закупівлі здійснюється за рахунок коштів бюджету м. Києва (КЕКВ 2610).

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 4 арк.
2. Додаток №2. Кваліфікаційні критерії до учасників в 1 прим. на 1 арк.
3. Додаток №3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) в 1 прим. на 3 арк.
4. Додаток №4. Протокол № 10 від 13 травня 2021 року в 1 прим. на 9 арк.

Відповідальний за розробку ТВ
(ініціатор закупівлі) Начальник відділу
обслуговування програмних
та апаратних комплексів

Д.Л. Реут

«ПОГОДЖЕНО»:

Головний бухгалтер

Г.А. Букша

Начальник загально-правового відділу

В. В. Тихонов

Заступник директора з технічних
питань

О.Ф. Поліщук

Заступник директора з впровадження
та інформаційного супроводу ІТ рішень

В. С. Іцкович

Заступник директора
з загальних питань

О.Л. Опарін

Місце поставки товару - 04071, м. Київ, вул. Сролівська, 1/б.
Строк поставки товарів - по 05 вересня 2021 року.

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

**На виконання пункту 16.20. «Закупівля антивірусного програмного забезпечення»
напрямів та заходів Комплексної міської цільової програми «Електронна столиця» на
2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512.**

**Найменування закупівлі: за код ДК 021:2015 (CPV) «Єдиний закупівельний
словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів
(Закупівля антивірусного програмного забезпечення)**

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 дії) 'ESET Endpoint Protection Advanced (EES, EFS)' (К). На 1 рік.)*	12 440	1 рік

1. Рішення для захисту робочих станцій під управління серверних та несерверних ОС - ESET ENDPOINT PROTECTION ADVANCED,

Вимоги щодо підтримки програмного забезпечення (далі ПЗ):

- Наявність експертного висновку Державної служби спеціального зв'язку та захисту інформації, що підтверджується наданням у складі тендерної пропозиції копії документа, завіреного відповідним чином.
- Запропоноване ПЗ забезпечується в Україні технічною підтримкою через українську службу технічної підтримки, яка працює в режимі 24x7x365 - 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 усього функціоналу в рамках зазначеного програмного забезпечення, без додаткових придбань.
- Наявність багатомовного інсталлятора, 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, мережесих 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 мережесих протоколів, таких як SMB, RPC, RDP і т.д.
- Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережесих атак на комп'ютер.
- Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
- 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 мережесих атак.
- Можливість створювати для персонального брандмауера 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.
- Наявність системи виявлення 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 ізолюваних мережах різних

класів захищеності

- Наявність інструменту віддаленого управління з можливістю віддаленої інсталяції користувальницького ПЗ.

Наявність журналу аудиту, у якому відстежуються і реєструються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.

- Можливість відслідковувати все встановлене на робочій станції програмне забезпечення, а також видаляти встановлене програмне забезпечення за вибором, що дозволяє не тільки виявити несанкціоноване встановлене програмне забезпечення та реагувати на подібні інциденти інформаційної безпеки шляхом видалення
 - Можливість налаштування автоматичного розподілу клієнтів по групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань для автоматизації більшості процесів, пов'язаних з реагуванням на інциденти інформаційної безпеки.
 - Інструмент віддаленого управління повинен мати веб-орієнтований інтерфейс.
 - Можливість встановлення сервера адміністрування на ОС Windows та Linux що значно заощадити на ліцензіях для серверів, а також надає більше можливостей під час вибору серверної платформи.
 - Двофакторна аутентифікація для захисту облікових записів адміністраторів.
 - Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станціях до яких немає фізичного або віддаленого доступу.
 - 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 створення 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 глибокого аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
 - 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 10, 8.1, 8, 7, Vista;
 - Microsoft Windows Server 2019, 2016, 2012, 2008;
 - Microsoft Windows Storage Server 2016, 2012, 2008;
 - Microsoft Windows MultiPoint Server 2012, 2011, 2010;
 - Microsoft Windows Small Business Server 2011, 2008;
 - MacOS 10.9 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 64-bit

- CentOS 7 64-bit
- Debian 9 64-bit
- SUSE Linux Enterprise Server (SLES) 12 64-bit, 15 64-bit

- VMware vSphere 6.0, 6.5+, 6.7+ (vCenter Single Sign-On, vSphere Client/Web Client, vCenter Server, vCenter Inventory Service)
- VMware NSX Manager 6.3+, 6.4.0, 6.4.1, 6.4.2
- VMware Guest Introspection 6.2.4+, 6.3+, 6.4+

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.

**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.*

**Начальника відділу обслуговування
програмних та апаратних комплексів**




Реут Д.Л.

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)
<i>1. Кваліфікаційні критерії до учасника та спосіб їх документального підтвердження</i>	
Кваліфікаційні критерії, встановлені відповідно до статті 16 Закону	Документальне підтвердження наявності кваліфікаційних критеріїв
1. Наявність обладнання, матеріально-технічної бази та технологій	1.1. Довідка у довільній формі про наявність обладнання та матеріально-технічної бази, необхідних для постачання програмного забезпечення, що є предметом закупівлі.
2. 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	2.1. 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.



Вих. №195/05-27052021

від 27 травня 2021 р.

щодо надання
комерційної пропозиції
на антивірусне програмне забезпечення
(Продовження дії) ESET
Endpoint Protection Advanced



СПЕЦІАЛІЗОВАНЕ КУМУНАЛЬНЕ
ПІДПРИЄМСТВО «КИЇВТЕЛЕСЕРВІС»

**Комерційна пропозиція ТОВ «СОФТНЕТ ГРУП»
від 27 травня 2021 року**

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

№	Найменування програмного продукту антивірусного захисту	К-ість	Вартість за одну ліцензію за місяць (грн.)	Загальна вартість за видом ліцензії за 12 місяців (грн.)
1	Антивірусне програмне забезпечення (Продовження дії) 'ESET Endpoint Protection Advanced (EES, EFS)' (K). На 1 рік.)*	12 440	277,00	3 445 880,00
Загальна вартість ліцензій на 12 місяців, грн:			3 445 880,00	

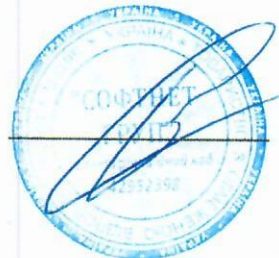
* Податок на додану вартість не нараховується згідно з пунктом 261 підрозділу 2 розділу XX Податкового кодексу України від «02» грудня 2010 року № 2755-VI (зі змінами та доповненнями).

Загальна вартість послуг за цією комерційною пропозицією становить
3 445 880 грн. 00 коп. (три мільйони чотириста сорок п'ять тисяч вісімсот вісімдесят грн)
00 коп. без 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,

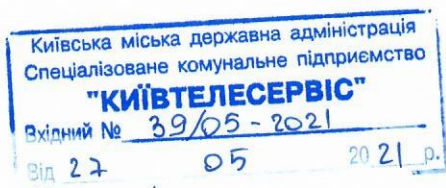
Директор ТОВ «СОФТНЕТ ГРУП»



М. В. Тихонов

ТОВ «СОФТНЕТ ГРУП»
ЄДРПОУ 42952398, ІВАН УА
33305299000026004036703983
у АТ КБ «Приватбанк», МФО 380275

ЮРИДИЧНА АДРЕСА ТА ФАКТИЧНА АДРЕСА:
м. Київ, вул. О. Паргольського, буд. 19 корпус 4.
Тел. +38 044 393 93 23

СПЕЦІАЛІЗОВАНЕ КУМУНАЛЬНЕ
ПІДПРИЄМСТВО «КИЇВТЕЛЕСЕРВІС»

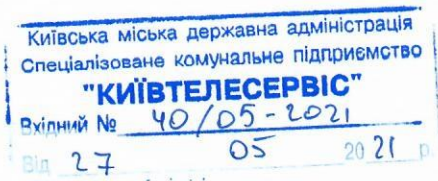
У відповідь на запит щодо вартості ліцензій антивірусного програмного забезпечення ESET Endpoint Protection Advanced (продовження дії ліцензії на 1 рік) повідомляємо про те що для кількості 12 440 одиниць вартість становить **3 457 000,00 грн.** (три мільйони чотириста п'ятдесят сім тисяч грн. 60 коп.) без ПДВ.

№	Найменування товару	Кількість	Вартість, грн. без ПДВ
1	Програмне забезпечення ESET Endpoint Protection Advanced (продовження дії ліцензії на 1 рік)	12440	3 457 000.00
Загальна ціна пропозиції конкурсних торгів, грн. з ПДВ			3 457 000.00

ТОВ «СОФТ ОНЛАЙН»



Матюшко Світлана Михайлівна



ТОВ «Компанія «Аміка»
04128, м. Київ, вул. Стеценка, буд 19/91
Тел/факс: (044) 355-07-70
П/р UA893510050000026002514945700, Банк ПАТ
"УКРСИББАНК"
МФО 351005, ЄДРПОУ 38977500, ІПН 389775026594

**СПЕЦІАЛІЗОВАНЕ КУМУНАЛЬНЕ
ПІДПРИЄМСТВО «КИЇВТЕЛЕСЕРВІС»**

**щодо надання
комерційної пропозиції**

У відповідь на ваш запит ТОВ "КОМПАНІЯ"АМІКА" висловлює Вам свою повагу та звертається з Комерційною пропозицією щодо вартості Антивірусного програмного забезпечення ESET Endpoint Protection Advanced загальна вартість якого, за попередньою оцінкою, складає **3 477 120 грн. 00 коп.** (Три мільйони чотириста сімдесят сім тисяч сто двадцять гривень, 00 копійок) без ПДВ. ПДВ не нараховується згідно з пунктом 261 підрозділу 2 розділу XX Податкового кодексу України від «02» грудня 2010 року № 2755-VI (зі змінами та доповненнями).
Продовження дії ліцензії тривалістю 1 рік.

Директор ТОВ "КОМПАНІЯ "АМІКА"



Мудренко Сергій Григорович

АМІКА - правильний ІТ-партнер
Апаратні та програмні рішення для ефективності та безпеки Вашого бізнесу.

www.amica.ua | info@amica.ua

ПРОТОКОЛ № 10

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 - 2022 роки у 2021 – 2022 роках

м. Київ

«13» травня 2021 року

ПРИСУТНІ:

Члени робочої групи:

В. Болгов
В. Жучков
В. Іцкович
Є. Коробенко
І. Лагутіна
О. Поліщук
Д. Рябіченко
Т. Самойленко
О. Сибіркін

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєкту технічних вимог до закупівлі у межах виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019–2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (далі – Програма), у 2021 році, а саме: проєкт технічних вимог до закупівлі «Пакети програмного забезпечення для захисту від вірусів (Закупівля антивірусного програмного забезпечення)» (пункт 16.20 «Закупівля антивірусного програмного забезпечення» напрямів діяльності та заходів Програми).

2. Різне.

По питанню 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що з метою забезпечення захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації) від зловмисного програмного забезпечення необхідно закупити 12 440 ліцензій антивірусного програмного забезпечення (продовження дії на 1 рік) ESET Endpoint Protection Advanced (пункт 16.20 «Закупівля антивірусного програмного забезпечення» напрямів діяльності та заходів Програми).

В обговоренні брали участь: В. Іцкович, О. Сибіркін

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Закупівля антивірусного програмного забезпечення» (пункт 16.20 напрямів діяльності та заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 9, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела

Тамара САМОЙЛЕНКО

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

на виконання пункту 16.20. «Закупівля антивірусного програмного забезпечення» напрямів та заходів Комплексної міської цільової програми «Електронна столиця» на 2019 – 2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512

найменування закупівлі: за код ДК 021:2015 (CPV) «Єдиний закупівельний словник» – 48760000-3 Пакети програмного забезпечення для захисту від вірусів (Закупівля антивірусного програмного забезпечення)

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 дії) 'ESET Endpoint Protection Advanced (EES, EFS)' (К). На 1 рік.)*	12 440	1 рік

1. Рішення для захисту робочих станцій під управління серверних та несерверних ОС – ESET ENDPOINT PROTECTION ADVANCED

Вимоги щодо підтримки програмного забезпечення (далі ПЗ):

- Наявність експертного висновку Державної служби спеціального зв'язку та захисту інформації, що підтверджується наданням у складі тендерної пропозиції копії документу, завіреного відповідним чином.
- Запропоноване ПЗ забезпечується в Україні технічною підтримкою через українську службу технічної підтримки, яка працює в режимі 24x7x365 – 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 усього функціоналу 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 експлоїтів, 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.

- 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 мережі.

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

- Можливість створювати для персонального брандмауера 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.

- Наявність системи виявлення 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

- Наявність інструменту віддаленого управління з можливістю віддаленої інсталяції користувальницького ПЗ.

Наявність журналу аудиту, у якому відстежуються і реєструються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.

- Можливість відслідковувати все встановлене на робочій станції програмне забезпечення, а

також видаляти встановлене програмне забезпечення за вибором, що дозволяє не тільки виявити несанкціоноване встановлене програмне забезпечення та реагувати на подібні інциденти інформаційної безпеки шляхом видалення

- Можливість налаштування автоматичного розподілу клієнтів по групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань для автоматизації більшості процесів, пов'язаних з реагуванням на інциденти інформаційної безпеки.

- Інструмент віддаленого управління повинен мати веб-орієнтований інтерфейс.

- Можливість встановлення сервера адміністрування на ОС Windows та Linux що значно заощадити на ліцензіях для серверів, а також надає більше можливостей під час вибору серверної платформи.

- Двофакторна аутентифікація для захисту облікових записів адміністраторів.

- Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станціях до яких немає фізичного або віддаленого доступу.

- 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 створення 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 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 10, 8.1, 8, 7, Vista;

- Microsoft Windows Server 2019, 2016, 2012, 2008;

- Microsoft Windows Storage Server 2016, 2012, 2008;

- Microsoft Windows MultiPoint Server 2012, 2011, 2010;

- Microsoft Windows Small Business Server 2011, 2008;

- MacOS 10.9 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 64-bit

- CentOS 7 64-bit

- Debian 9 64-bit

- SUSE Linux Enterprise Server (SLES) 12 64-bit, 15 64-bit

- VMware vSphere 6.0, 6.5+, 6.7+ (vCenter Single Sign-On, vSphere Client/Web Client, vCenter

Server, vCenter Inventory Service)

- VMware NSX Manager 6.3+, 6.4.0, 6.4.1, 6.4.2
- VMware Guest Introspection 6.2.4+, 6.3+, 6.4+

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.

**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.*

Інформація про електронні підписи (ЕП)

№ документа 075-861

Дата реєстрації 13.05.2021

Документ зареєстровано у картотеці:

Вихідна

Вид документа:

Лист

Стислий зміст:

Матеріали засідання робочої групи 13.05.2021 (Протокол № 10 від 13.05.2021)

Кількість файлів: 2

Кількість ЕП: 19






ДОКУМЕНТ СЕД АСКОД ІТС ЄПК






Департамент інформаційно-
комунікаційних технологій
13.05.2021 № 075-861




За підписом:

Лисик Ганна Миколаївна (В.О.)

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Іцкович Вікторія Євгенівна Кількість ЕП: 1	14.05.2021 14:33:08 ;	14.05.2021 14:33:08 Погодив;	14.05.2021 14:33:08 Погодив 
СИБІРКІН ОЛЕКСАНДР МИКОЛАЙОВИЧ Кількість ЕП: 2	14.05.2021 12:10:37 ; 14.05.2021 12:10:39 ;	14.05.2021 12:10:39 Погодив;	14.05.2021 12:10:39 Погодив 
ЖУЧКОВ ВАСИЛЬ АНАТОЛІЙОВИЧ Кількість ЕП: 2	14.05.2021 10:53:00 ; 14.05.2021 10:53:01 ;	14.05.2021 10:53:01 Погодив;	14.05.2021 10:53:01 Погодив 
Поліщук Олег Федорович (2684213893) Кількість ЕП: 2	14.05.2021 10:49:20 ; 14.05.2021 10:49:20 ;	14.05.2021 10:49:21 Погодив;	14.05.2021 10:49:20

			
Поліщук Олег Федорович (2684213893) Кількість ЕП: 2	14.05.2021 10:49:20 ; 14.05.2021 10:49:20 ;	14.05.2021 10:49:21 Погодив;	14.05.2021 10:49:20 
Коробенко Євген Вікторович Кількість ЕП: 2	14.05.2021 09:49:42 ; 14.05.2021 09:49:42 ;	14.05.2021 09:49:42 Погодив;	14.05.2021 09:49:42 Погодив 
Коробенко Євген Вікторович Кількість ЕП: 2	14.05.2021 09:49:42 ; 14.05.2021 09:49:42 ;	14.05.2021 09:49:42 Погодив;	14.05.2021 09:49:42 Погодив 
БОЛГОВ ВАЛЕРІЙ СЕРГІЙОВИЧ Кількість ЕП: 3	13.05.2021 18:51:08 ; 14.05.2021 08:31:56 ; 14.05.2021 08:31:56 ;	14.05.2021 08:31:57 Погодив;	14.05.2021 08:31:56 
БОЛГОВ ВАЛЕРІЙ СЕРГІЙОВИЧ Кількість ЕП: 3	13.05.2021 18:51:08 ; 14.05.2021 08:31:56 ; 14.05.2021 08:31:56 ;	14.05.2021 08:31:57 Погодив;	14.05.2021 08:31:56

			
ЛАГУТІНА ІННА ІГОРІВНА Кількість ЕП: 3	13.05.2021 18:49:34 ; 13.05.2021 22:33:29 ; 13.05.2021 22:33:30 ;	13.05.2021 22:33:30 Погодив;	13.05.2021 22:33:30 Погодив 
Рябіченко Дмитро Володимирович Кількість ЕП: 2	13.05.2021 19:59:01 ; 13.05.2021 19:59:48 ;	13.05.2021 19:32:24 Погодив;	13.05.2021 19:59:48 
Самойленко Тамара Анатоліївна Кількість ЕП: 2	13.05.2021 18:04:05 ; 13.05.2021 19:59:13 ;		13.05.2021 19:59:13 