Виконуючому обов'язки директора Спеціалізованого комунального підприємства «Київтелесервіс» Биструшкіну Олександру Олександровичу
Начальника відділу обслуговування програмних та апаратних комплексів Реута Д.Л.

СЛУЖБОВА ЗАПИСКА

місто Київ «31» липня 2024 року

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

Обґрунтування доцільності закупівлі:

На виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки, затвердженої рішенням Київської міської ради від 07.12.2023 р. № 7516/7557 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 необхідності посилання на конкретні марку та виробника: зазначений програмний продукт був обраний на підставі запитів 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 щодо подовження строку дії ліцензії наявної системи антивірусного захисту робочих станцій та серверів.

Обґрунтування обсягів закупівлі:

Кількість та перелік ліцензійного програмного забезпечення сформовано на підставі заявок, отриманих 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, враховуючи рівень наявного використання ліцензій на антивірусне ПЗ згідно інформації, отриманої з центру керування Eset Protect.

Обґрунтування якісних характеристик закупівлі:

Технічні вимоги до предмета закупівлі рекомендовані протоколом №59 від 23.07.2024 р. засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки.

Обґрунтування очікуваної вартості закупівлі:

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 5 501 313,92 грн. (п'ять мільйонів п'ятсот одну тисячу триста тринадцять гривень 92 копійки) з ПДВ, що є середньоарифметичним значенням отриманих комерційних пропозицій.

Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення.

Розмір бюджетного призначення визначено паспортом бюджетної програми на 2024 рік відповідно до заходів Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2025 роки.

Джерело фінансування закупівлі – місцевий бюджет, КЕКВ 2610 (Субсидії та поточні трансферти підприємствам (установам, організаціям).

Вид предмету закупівлі – товар.

Кількість – 13500 шт.

Місце поставки товару – м. Київ, вул. Фролівська, 1/6 літ. А

Строк поставки товарів – до 05.11.2024 р.

Додатки:

1. Додаток №1. Інформація про необхідні технічні, якісні, кількісні та інші характеристики предмета закупівлі (Технічні вимоги) в 1 прим. на 8 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 Знімок екрану центру керування антивірусним програмним забезпеченням Eset Protect.

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

«ПОГОДЖЕНО»:
Заступник директора з технічних питань _____ О. Ф. Поліщук

Начальник фінансово-економічного відділу –
головний бухгалтер _____ Г. А. Букша

Заступник начальника фінансово-економічного
відділу з економічних питань _____ Ю.В. Волочаєва

Начальник загально-правового
відділу _____ В.В. Тихонов

Додаток 1

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

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

На виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557

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». На 1 рік.)*	12940	1 рік
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням». На 1 рік.)*	560	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):

- 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).
- 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: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
• Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп'ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
• Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.
• Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
• Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
• Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
• Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
• Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
• Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
• Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
• Забезпечення антивірусного захисту в режимі реального часу.
• Використання евристичних технологій власної розробки під час сканування.
• Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
• Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.
• Можливість сканування файлів під час запуску ОС.
• Можливість сканування WMI та системного реєстру, усіх розділів та підрозділів, що забезпечує захист від шкідливого програмного коду та зловмисних посилань, які поширюються у вигляді даних.
• Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
• Сканування комп'ютера у неактивному стані.
• Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об'єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.
• Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
• Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.
• Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.

• Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).
• Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
• Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп'ютер від шкідливих програм і небажаної активності.
• Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.
• Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
• Можливість інтеграції захисту робочих станцій та серверів з хмарною пісочницею (при наявності додаткової ліцензії), без необхідності встановлення додаткових програмних продуктів.
• Автоматична антивірусна перевірка змінних носіїв.
• 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 створювати групи дозволених або заборонених зовнішніх пристроїв.
• Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
• Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
• Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
• Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
• Наявність модуля захисту від спаму власної розробки з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
• Можливість використовувати білі та чорні списки спам-адресатів як користувальницькі (гнучка персоналізація інтелектуального спам-модулю), так і глобальні, інформація до яких надходить з серверів оновлення.
• Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».
• Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
• Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
• Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
• Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
• Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
• 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 створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
- Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.
- Наявність у персональному брандмауеру інтерактивного режиму, що надає детальну інформацію про нове невідоме мережеве з'єднання та дає можливість не тільки створювати на ПК нове правило мережевої фільтрації для виявленого з'єднання, а й вказувати детальні налаштування для нього.
- Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.
- Наявність редактора правил, що дає можливість не тільки редагувати створені правила, а й керувати вбудованими правилами, яких достатньо для первинного ретельного захисту від несанкціонованих мережевих з'єднань та локальних мережевих атак.
- Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.
- Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
- Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.
- Наявність додаткового функціоналу персонального брандмауеру, що дозволяє переглядати всю детальну інформацію по всіх наявних мережевих з'єднаннях, а також попереджати користувача про підключення до незахищеної мережі Wi-Fi.
- Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.
- Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
- Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
- Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE
- Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
- Наявність додаткового функціоналу персонального брандмауеру, що дає можливість переглядати на ПК перелік заблокованих IP-адрес, надає інформацію про причини потрапляння до чорного списку, та дозволяє зробити виключення для конкретних безпечних адрес.
- Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.
- Фільтрація інтернет-трафіку.
- Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
- 27 категорій фільтрації інтернет-трафіку, в яких розподілені більш ніж 100 підкатегорій, а також можливість створювати групи з категорій та підкатегорій.
- Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.
- Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.
- Регламентне оновлення вірусних баз не менше 24 разів за добу.
- Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет.

• Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
• Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
• Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника онлайн, у разі перебування поза корпоративною мережею.
• Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
• Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
• Інструменти моніторингу, оцінки стану безпеки та реагування:
• Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
• 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 визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
• Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
• Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
• Локальне зберігання журналів на робочих станціях.
• Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів програми.
• Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
• Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
• Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
• Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
• Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.
• Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
• Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
• Можливість дозволити оновлення компонентів в автоматичному режимі, що дає можливість завантажити та інсталювати компоненти без втручання адміністратора або користувача.
• Можливість оновлення компонентів в ручному режимі, що дає можливість оновлення компонентів на некерованих робочих станціях.
• Можливість оновлення деяких компонентів без необхідності перезавантаження для початку функціонування.
• Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
• Низьке споживання ресурсів ПК актуальними антивірусними продуктами (сукупно усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору.

• 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. Спеціальний 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.

Активація даної ліцензії здійснюється автоматично в момент припинення дії попередньої - 06.11.2024 р.

**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).
2. Наявність експертних висновків.	2.1 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 учасником надається лист від виробника або його ексклюзивного дистриб'ютора щодо наявності в Україні авторизованого центру технічної підтримки.

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.

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

№ 26/1 від 26.07.2024

СКП «Київтелесервіс»

01001, м. Київ, вул. Хрещатик, 10

Щодо надання комерційної пропозиції

Товариство з обмеженою відповідальністю «Спецбайт» дякує за зацікавленість у співпраці і надає на Ваш запит (№ 242-2024 від 26.07.2024) комерційну пропозицію, щодо наведена нижче.

Комерційна пропозиція

№ з/п	Найменування програмного продукту антивірусного захисту або еквівалент	К-сть ліцензій (одиниці)	Термін дії ліцензії	Вартість грн, разом із ПДВ
1	Антивірусне програмне забезпечення (Продовження) «ESET PROTECT Entry з локальним управлінням». На 1 рік.	12940	1 рік	5 256 537,60
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням». На 1 рік.	560	1 рік	244 776,00
Всього:				**5 501 313,60**

Директор ТОВ «СПЕЦБАЙТ» Микола СОСНИЦЬКИЙ

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 273 / 2024
Від 26 07 2024 р.

ТОВ «СПЕЦБАЙТ»
Юридична адреса: 03151, м. Київ,
вул. Святослава Хороброго, 7, офіс 2
Адреса для листування: 03151, м. Київ, пр-т
Повітряних Сил України, 90, офіс 204
Телефон: (044) 337-25-26
Електронна пошта: info@s-byte.com
Веб сайт: www.s-byte.com

Товариство з обмеженою відповідальністю
"ІН-КЛАУД"
04053, Україна, м. Київ, вул. Конисього Олександра, буд. 57, оф. 17, ЄДРПОУ: 42637290

Вих. № 85/07-24
Від 29.07.2024 р.

Спеціалізоване комунальне підприємство «Київтелесервіс»

На Ваш, запит № 240-2024 від 26.07.2024 р., щодо орієнтовної вартості закупівлі ліцензійного антивірусного програмного забезпечення (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів) надаємо комерційну пропозицію:

Найменування програмного продукту антивірусного захисту	**Од. виміру**	**Вартість (з ПДВ, грн.)**
Програмна продукція «ESET PROTECT Entry з локальним управлінням» (К). На 1 рік. Поновлення. Для захисту 12940 об'єктів	шт.	**5 256 537,60**
Програмна продукція «ESET PROTECT Entry з локальним управлінням» (К). На 1 рік. Пільгова. Понад 12940. Для захисту 560 об'єктів	шт.	**244 776,00**
	Загальна вартість без ПДВ:	**4 584 428,00**
	ПДВ:	**916 885,60**
	Загальна вартість з ПДВ:	**5 501 313,60**

Директор ТОВ «ІН-КЛАУД» **Черниш Павло**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 285/2024
від 30 07 2024 р.

Вих. №117/07-29072024
від 29 липня 2024 р.

В.о. Директора
СКП "КИЇВТЕЛЕСЕРВІС"
О. Биструшкіну

Щодо надання цінової пропозиції

Шановний пане Олександре!

ТОВ «СОФТНЕТ ГРУП» висловлює свою повагу і дає відповідь на ваш запит від 26.07.2024 року №241-2024 щодо надання цінової пропозиції орієнтовної вартості закупівлі ліцензійного програмного забезпечення , 4876000-3 «Закупівля антивірусного програмного забезпечення» за ДК 021:2015 Єдиного закупівельного словника на 2024 рік.

У відповідності до наданих Технічних вимог орієнтовна вартість антивірусного програмного забезпечення наведена у Таблиці 1.

Таблиця 1.

№	Найменування програмного продукту антивірусного захисту або еквівалент	К-сть ліцензій (одиниці)	Термін дії ліцензії	Ціна за одиницю, без ПДВ	Загальна вартість, без ПДВ	Загальна вартість, з ПДВ
1	Антивірусне програмне забезпечення (Продовження) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	12 940	1 рік	338,52	4 380 448,80	5 256 538,56
2	Антивірусне програмне забезпечення (Закупівля) «ESET PROTECT Entry з локальним управлінням (EES, EFS)» (К). На 1 рік.)*	560	1 рік	364,25	203 980,00	244 776,00
				Всього без ПДВ, грн:		**4 584 428,80**
				ПДВ, грн:		**916 885,76**
				Всього з ПДВ, грн:		**5 501 314,56**

Орієнтовна вартість антивірусного програмного забезпечення на 2024 рік складає 5 501 314,56 грн (П'ять мільйонів п'ятсот одна тисяча триста чотирнадцять гривень 56 копійок) з ПДВ.

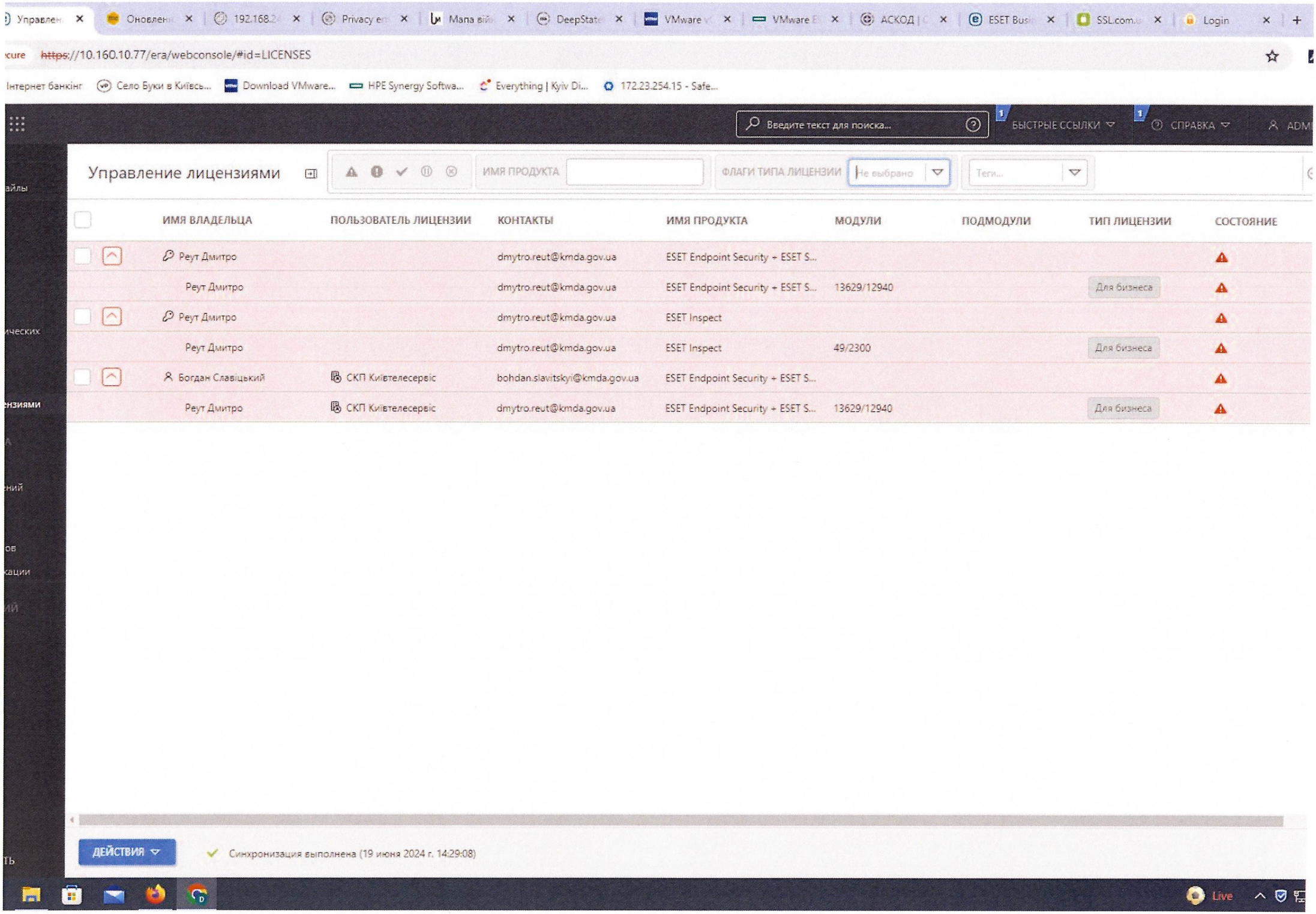
Директор **Тихонов М. В.**

ТОВ "СОФТНЕТ ГРУП"
ЄДРПОУ: 42952398
ІПН: 429523926500

БАНКІВСЬКІ РЕКВІЗИТИ
Р/р: UA333052990000026004036703983
в АТ КБ "ПриватБанк", МФО 380775

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 284/2024
30 07 2024 р.


https://10.160.10.77/era/webconsole/#id=LICENSES
Введите текст для поиска...
БЫСТРЫЕ ССЫЛКИ
СПРАВКА
Управление лицензиями
ИМЯ ПРОДУКТА
ФЛАГИ ТИПА ЛИЦЕНЗИИ
Не выбрано
Теги...
ИМЯ ВЛАДЕЛЬЦА
ПОЛЬЗОВАТЕЛЬ ЛИЦЕНЗИИ
КОНТАКТЫ
ИМЯ ПРОДУКТА
МОДУЛИ
ПОДМОДУЛИ
ТИП ЛИЦЕНЗИИ
СОСТОЯНИЕ
Реут Дмитро
dmytro.reut@kmda.gov.ua
ESET Endpoint Security + ESET S...
Реут Дмитро
dmytro.reut@kmda.gov.ua
ESET Endpoint Security + ESET S...
13629/12940
Для бизнеса
Реут Дмитро
dmytro.reut@kmda.gov.ua
ESET Inspect
Реут Дмитро
dmytro.reut@kmda.gov.ua
ESET Inspect
49/2300
Для бизнеса
Богдан Славіцький
СКП Київтелесервіс
bohdan.slavitskyi@kmda.gov.ua
ESET Endpoint Security + ESET S...
Реут Дмитро
СКП Київтелесервіс
dmytro.reut@kmda.gov.ua
ESET Endpoint Security + ESET S...
13629/12940
Для бизнеса
ДЕЙСТВИЯ
Синхронизация выполнена (19 июня 2024 г. 14:29:08)

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 59
засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки

м. Київ «23» липня 2024 року

ПРИСУТНІ:

Члени робочої групи:
А. Вовнюк
М. Журбенко
М. Клюєва
С. Осіпов
О. Поліщук
П. Сальніков
Т. Самойленко
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (далі – Програма), у 2024 році, а саме:

1.1 доопрацьований проєкт технічних вимог до закупівлі «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» – для систем відеоспостереження у школах Дніпровського району міста Києва (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.2 доопрацьований проєкт технічних вимог до закупівлі «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» – для систем відеоспостереження у школах Дніпровського району міста Києва (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.3 доопрацьований проєкт технічних вимог до закупівлі «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» – для встановлення на в'їздах-виїздах із міста Києва (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.4 проєкт технічних вимог до закупівлі «Антивірусне програмне забезпечення» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми).

2. Різне.

По підпунктах 1.1 – 1.3 питання 1

СЛУХАЛИ:

С. Осіпова, який поінформував, що для забезпечення виконання заходів із запобігання виникненню надзвичайних ситуацій техногенного, природного, соціального характеру та ліквідації їх наслідків є необхідність розвитку комплексної системи відеоспостереження міста Києва шляхом придбання засобів зв'язку та послуг, пов'язаних з їх постачанням, що включають встановлення та налаштування, а також відповідного обладнання та матеріалів, та представив два доопрацьовані проєкти технічних вимог до закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» для встановлення у школах Дніпровського району міста та для встановлення на в'їздах-виїздах із міста Києва, а також доопрацьований проєкт технічних вимог «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (для систем відеоспостереження у школах Дніпровського району міста) (пункт 2.1 переліку завдань і заходів Програми) у частині уточнення технічних та кількісних характеристик обладнання.

В обговоренні брали участь: Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури двох закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (для систем відеоспостереження у школах Дніпровського району міста та систем відеоспостереження на в'їздах-виїздах із міста Києва) та закупівлі «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (для систем відеоспостереження у школах Дніпровського

району міста) (пункт 2.1 переліку завдань і заходів Програми) використовувати доопрацьовані проєкти технічних вимог, розглянуті на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 8, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По підпункту 1.4 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував про необхідність забезпечення антивірусним захистом обладнання, робочих станцій шляхом подовження терміну використання ліцензійного антивірусного програмного забезпечення та придбання нового виду антивірусного програмного забезпечення та представив проєкт технічних вимог до закупівлі «Антивірусне програмне забезпечення» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні брали участь: Д. Цвігун.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Антивірусне програмне забезпечення» (пункт 6.5 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 8, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1736
Дата реєстрації 23.07.2024
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 23.07.2024 (Протокол № 59 від 23.07.2024)

Кількість файлів: 5
Кількість ЕП: 48

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
23.07.2024 № 075-1736

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Журбенко Максим Анатолійович **Кількість ЕП:** 9	24.07.2024 16:57:03 ; 24.07.2024 16:57:03 ; 24.07.2024 16:57:04 ; 24.07.2024 16:57:05 ; 25.07.2024 15:14:10 ; 25.07.2024 15:14:10 ; 25.07.2024 15:14:11 ; 25.07.2024 15:14:12 ; 25.07.2024 15:14:13 ;	24.07.2024 16:57:05 Погодив; 25.07.2024 15:14:13 Погодив;	25.07.2024 15:14:13 Погодив
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 9	23.07.2024 17:18:15 ; 23.07.2024 17:18:15 ; 23.07.2024 17:18:15 ; 23.07.2024 17:18:15 ; 24.07.2024 19:13:52 ; 24.07.2024 19:13:52 ; 24.07.2024 19:13:52 ; 24.07.2024 19:13:52 ; 25.07.2024 14:19:03 ;	24.07.2024 19:13:52 Погодив; 25.07.2024 14:20:18 Ознайомився;	25.07.2024 14:19:03
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 5	23.07.2024 17:21:20 ; 23.07.2024 17:21:21 ; 23.07.2024 17:21:23 ; 23.07.2024 17:21:24 ; 25.07.2024 13:47:53 ;	25.07.2024 07:42:03 Погодив;	25.07.2024 13:47:53
САЛЬНІКОВ ПЕТРО ЄГОРОВИЧ **Кількість ЕП:** 5	23.07.2024 17:35:28 ; 23.07.2024 17:35:28 ; 23.07.2024 17:35:30 ; 23.07.2024 17:35:31 ; 25.07.2024 13:35:53 ;	23.07.2024 17:35:31 Погодив;	25.07.2024 13:35:53

КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 5	23.07.2024 17:15:44 ; 23.07.2024 17:15:45 ; 23.07.2024 17:15:47 ; 23.07.2024 17:15:49 ; 25.07.2024 13:29:45 ;	23.07.2024 17:15:49 Погодив;	25.07.2024 13:29:45
Поліщук Олег Федорович **Кількість ЕП:** 5	24.07.2024 09:03:22 ; 25.07.2024 08:53:53 ; 25.07.2024 08:53:53 ; 25.07.2024 08:53:54 ; 25.07.2024 13:29:45 ;	25.07.2024 08:53:55 Погодив;	25.07.2024 13:29:45
Вовнюк Анатолій Віталійович **Кількість ЕП:** 5	25.07.2024 13:27:20 ; 25.07.2024 13:27:57 ; 25.07.2024 13:28:02 ; 25.07.2024 13:28:08 ; 25.07.2024 13:28:12 ;	23.07.2024 17:26:02 Погодив; 25.07.2024 13:28:18 Ознайомився;	25.07.2024 13:28:12
Самойленко Тамара Анатоліївна **Кількість ЕП:** 5	24.07.2024 07:12:13 ; 24.07.2024 07:12:13 ; 24.07.2024 07:12:14 ; 24.07.2024 07:12:14 ; 25.07.2024 13:27:50 ;	25.07.2024 13:27:50 Погодив;	25.07.2024 13:27:50 Погодив