Виконуючому обов'язки директора Спеціалізованого комунального підприємства «Київтелесервіс» Волощуку Олександру Олександровичу

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

СЛУЖБОВА ЗАПИСКА

місто Київ «03» вересня 2025 року

Конкретна назва предмета закупівлі – **Програмна продукція підсистеми кіберзахисту Sandbox (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки).**

Обґрунтування доцільності закупівлі:

На виконання пункту 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 та заходів в Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257).

З метою забезпечення аналітиків Центру моніторингу та кібербезпеки міських сервісів сучасними засобами аналізу кіберзагроз необхідно придбати програмну продукцію підсистеми кіберзахисту Sandbox (відокремлене середовище для тестування кіберзагроз) (далі-ПП).

Обґрунтування необхідності посилання на конкретні марку та виробника: Посилання на ПП Recorded Future обумовлено його поточним використанням для аналізу підозрілих та шкідливих файлів в ізольованому середовищі та наказом від 30.12.2024 №151 спеціалізованого комунального підприємства "Київтелесервіс" "Про введення у дослідну експлуатацію системи кібербезпеки".

Обґрунтування обсягів закупівлі:

Обсяг програмної продукції визначається поточною кількістю потенційно небезпечних файлів, що підлягають повному аналізу.

Обґрунтування якісних характеристик закупівлі:

Технічні вимоги до предмета закупівлі рекомендовані протоколом №76 від 16.07.2025 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 2024-2027 роки.

Очікувана вартість та джерела фінансування предмета закупівлі:

Згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, очікувана вартість становить 3 819 400,00 (три мільйони вісімсот дев'ятнадцять тисяч чотириста гривень нуль копійок) з ПДВ, що є середнім значенням отриманих комерційних пропозицій. Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення. Розмір бюджетного призначення визначено паспортом бюджетної програми на 2025 рік відповідно до заходів Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2027 роки.

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

Вид предмету закупівлі – товар.

Кількість – 1 шт.

Місце поставки товарів – місто Київ (відповідно до абз.2 п.10 Особливостей, у разі коли ***оприлюднення в електронній системі закупівель інформації про*** місцезнаходження замовника

та/або місцезнаходження (для юридичної особи)/місце проживання (для фізичної особи) постачальника (виконавця робіт, надавача послуг), та/або ***місце поставки товарів***, виконання робіт чи надання послуг (оприлюднення якої передбачено Законом та/або цими особливостями) ***несе загрозу безпеці замовника*** та/або постачальника, ***така інформація в договорі про закупівлю, який оприлюднюється в електронній системі закупівель, може зазначатися як назва населеного пункту*** місцезнаходження замовника та/або місцезнаходження (для юридичної особи)/місце проживання (для фізичної особи) постачальника (виконавця робіт, надавача послуг), та/або назва населеного пункту, ***в який здійснюється доставка товару*** (в якому виконуються роботи чи надаються послуги)).

Зазначення точної адреси місця поставки товару несе загрозу безпеці замовника.

Строк поставки товарів – до 16.12.2025.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 11 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.
4. Додаток 4. Протокол №76 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 2024-2027 роки на 3 арк

Ініціатор закупівлі _____ **Є.В. Буржинський**

«ПОГОДЖЕНО»:

Заступник директора з юридичних питань _____ **О.Є. Юрко**

Начальник відділу-головний бухгалтер _____ **Г. А. Букша**

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

Додаток 1

ТЕХНІЧНІ ВИМОГИ

Програмна продукція підсистеми кіберзахисту Sandbox (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки)

На виконання пункту 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 та заходів в Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257).

1. Загальні відомості про зміст робіт:

1.1. Повне найменування об'єкта інформатизації

Інформаційно-комунікаційна система моніторингу та кібербезпеки.

1.2. Найменування сторін:

- Замовник – Спеціалізоване комунальне підприємство «Київтелесервіс» (СКП «Київтелесервіс»);
- Виконавець – визначається за результатом проведення закупівлі відповідно до вимог законодавства України у сфері публічних закупівель.

1.3. Перелік документів, які мають враховуватись під час розробки.

- Закон України «Про Національну програму інформатизації»;
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;
- Постанова Кабінету Міністрів України від 21.02.2025 №205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»;
- рішення Київської міської ради від 12.12.2024 № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві».

Цей перелік документів не є вичерпним та може бути доповнений та уточнений під час підписання Договору.

2. Призначення та цілі інформатизації:

2.1. Призначення

Придбання програмної продукції підсистеми кіберзахисту Sandbox, забезпечує поглиблений аналіз підозрілих та шкідливих файлів в ізольованому середовищі, що дозволяє виявляти нові, раніше невідомі загрози (zero-day), обфусковані зразки шкідливого ПЗ та складні багаторівневі кібератаки. Також забезпечується функціонування інформаційно-комунікаційної системи моніторингу та кібербезпеки, для здійснення заходів, передбачених законодавством України у сфері кібербезпеки, проведення цілодобового моніторингу, аналізу, реагування та передачі інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту.

2.2. Цілі інформатизації

Організація цілодобового моніторингу стану кіберзахищенності шляхом збору та кореляцій подій кібербезпеки та ідентифікації зловмисної активності в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах 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 та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних послуг, електронної комерції, електронного документообігу.

3. Характеристики об'єкта інформатизації

Інформаційно-комунікаційна система моніторингу та кібербезпеки має такі функціональні можливості:

- автоматизація та цифровізація процесів збору і збереження інформації про кіберінциденти, категоризації кіберінцидентів та кібератак, їх пріоритезації (визначення першочерговості заходів реагування для ефективного розподілу ресурсів, зменшення негативних наслідків кіберінциденту та кібератаки), інформування (звітності) та ідентифікації (атрибуції);
- моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом та кібератакою щодо об'єктів кіберзахисту;
- автоматизація заходів із запобігання, виявлення та реагування на кіберінциденти та кібератаки, усунення їх наслідків;

4. Вимоги до засобу інформатизації:

4.1. Вимоги до структури та функціонування засобу інформатизації

Зазначена у Таблиці 1 програмна продукція надає можливість аналізу шкідливих файлів і програм в ізольованому середовищі, виявлених в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, які використовуються в структурних підрозділах виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністраціях, підприємствах, установах та організаціях, що належать до комунальної власності територіальної громади міста Києва та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних послуг, електронної комерції, електронного документообігу.

Опис програмної продукції наведено у таблиці 1:

Таблиця 1

Найменування*	Опис	Кількість ліцензій	Строк дії
Програмна продукція підсистеми кіберзахисту Sandbox (Recorded Future продовження)	**Доступ до модулю SecOps Intelligence до 10 користувачів**	**1**	**1 рік**

Вимоги до виробника та функціональних можливостей засобу інформатизації:

Таблиця 2

№	Характеристика	Вимога
1	**Загальні вимоги до функціоналу програмної продукції**	– Програмна продукція надає доступ до бази даних Cyber Threat Intelligence від виробника (вендора) – Програмна продукція працює повністю в моделі SaaS – Програмна продукція повинна мати власні механізми аналізу для аналізу шкідливого трафіку (в Інтернет-мережі), аналізу шкідливої інфраструктури (фішингові сайти, C2 вузли) та аналізу шкідливих програм (пісочниця). – Програмна продукція повинна надавати централізований вигляд, що відображає принаймні: • Категорію шкідливого програмного забезпечення (наприклад, програми-вимагачі, програми для викрадення даних, бот) • Правила виявлення для цього шкідливого програмного забезпечення • Матрицю MITRE та TTP (тактики, техніки, процедури), що використовуються цим шкідливим програмним забезпеченням • Нещодавно зкорельовані індикатори компрометації (IOC) (за останні 24 години та останні 7 днів) • Завершену розвідувальну інформацію про це шкідливе програмне забезпечення • Зловмисників, які використовують це шкідливе програмне забезпечення • Жертв цього шкідливого програмного забезпечення – Виробник програмної продукції повинен надавати звіти щонайменше за такими категоріями/темами: • Кіберподія • Профіль зловмисника • Аналіз шкідливого ПЗ • Аналіз кіберзагроз • Валідація кібернападів – Програмна продукція повинна використовувати технологію генеративного штучного інтелекту для автоматичного створення звітів – Автоматизовані звіти повинні генеруватися принаймні англійською та українською мовами.

		– Програмна продукція повинна використовувати власну технологію оптичного розпізнавання символів (OCR) для виявлення та інтерпретації змісту графічних зображень. – Програмна продукція повинна підтримувати лише одну централізовану базу даних для кожного користувача платформи. Функціонал, що передбачає створення окремої бази даних для кожного користувача, є недопустимим. – Програмна продукція повинна проводити автоматизовану оцінку ризиків для типів об'єктів IOC (IP-адреси, домени, URL-адреси, хеш-файли). – Програмна продукція повинна мати вбудований у веб-інтерфейс інструмент пошуку, який дозволяє здійснювати пошук інформації розвідки щодо вибраного типу об'єкта IOC (індикатора компрометації). – Програмна продукція не повинна вводити ліцензійних обмежень на кількість виконаних пошукових запитів за об'єктами IOC. – Програмна продукція повинна підтримувати пошук і завантаження правил детекції типів SIGMA, YARA та SNOART безпосередньо через WebUI. – Програмна продукція повинна містити розвідувальну інформацію та каталогізувати щонайменше 3000 сімейств шкідливого програмного забезпечення. – Програмна продукція повинна підтримувати спеціалізований інструмент пошуку, доступний в інтерфейсі WebUI, для пошуку розвідувальної інформації про відповідне шкідливе програмне забезпечення. – Програмна продукція не повинна вводити жодних обмежень на кількість об'єктів шкідливого програмного забезпечення, що підлягають пошуку – Для типів об'єктів IOC програмна продукція повинна відображати наступний контент у централізованому вигляді, окрім оцінки ризику: • Метадані • Фактори ризику • Докази для всіх факторів ризику • Історичну оцінку ризику з часовою шкалою • Інші пов'язані IOC • Посилання на шкідливе ПЗ або зловмисника • Відповідність TTP (включаючи MITRE T-codes) – Кожен звіт повинен мати унікальний заголовок та категорію

		– Виробник програмної продукції повинен підтримувати інтеграцію з провідними постачальниками рішень у сфері кібербезпеки, принаймні з такими компаніями: • Palo Alto Networks • IBM • Fortinet • Splunk • Microsoft
2	**Вимоги до джерел даних**	– Збір даних повинен виконуватись автоматизовано за допомогою мережі спеціально запрограмованих ботів, які постійно обробляють інформацію з джерел постачальника – Програмна продукція повинна збирати дані з наступних джерел: • Telegram • Discord • Twitter (X) • Соціальні мережі (LinkedIn, Meta, VK and similar) • Github • Файлообмінні платформи (Scribd, тощо) • Новинні видання • Кіберфоруми • Dark Web форуми • Darknet магазини та ринки • Блоги угруповувань Ransomware • Сайти для вимагання викупу, пов'язані з програмами-вимагачами – Програмна продукція повинна аналізувати та інтерпретувати неструктурований текст, написаний будь-якою мовою – Обробка мови та переклад повинні виконуватися за допомогою алгоритмів обробки природної мови (NLP), при цьому необхідно зберігати правильний синтаксис та розуміти сленг – Для всіх інших мов переклад має виконуватися за допомогою технології глибокого мовного перекладу (Deep Language Translation). Використання Google Translate не прийнятне. – Програмна продукція повинна підтримувати автоматичне розпізнавання шаблонів та класифікацію об'єктів. • Індикатор компрометації (IOC) (IP-адреса, домен, URL, хеш файлу) • Назва шкідливого програмного забезпечення

		• Ім'я суб'єкта загрози (Threat actor) • Адреса електронної пошти • Назва вектора атаки (MITRE T-codes) • Назва компанії або організації • Ім'я особи • Місцезнаходження (мінімум місто, країна та континент) • Ім'я користувача (у Twitter, на форумах, включно з форумами в даркнеті) • CVE (спільні вразливості та експлойти) • Продукт і програмне забезпечення. – Програмна продукція повинна містити в своїй базі даних щонайменше 5 мільярдів об'єктів, які мають бути категоризовані (відповідно до попередньої вимоги) – Автоматизований збір даних повинен виконуватись у режимі реального часу (із затримкою аналізу в межах декількох хвилин). – Програмна продукція повинна включати алгоритми машинного навчання на етапі аналізу даних, щоб автоматично і миттєво перетворювати неструктурований текст у розвіддані. – Програмна продукція повинна збирати дані за принаймні останні 10 років та мати інформацію за цей період, щоб забезпечити можливість історичного або ретроспективного аналізу.
3	**Вимоги до управління доступом**	– Доступ до платформи надається за допомогою WebUI та API – Мережеві з'єднання з платформою повинні бути криптографічно захищені з використанням протоколу HTTPS, що забезпечує конфіденційність та цілісність даних. Це стосується як WebUI, так і API. – Для автентифікації та авторизації аналітиків програмна продукція повинна підтримувати багатофакторну аутентифікацію (MFA) з використанням щонайменше MFA-токена – Програмна продукція повинна підтримувати функцію SSO, щонайменше для Microsoft Azure AD (Entra ID) – API має підтримувати аутентифікацію запитів через API-токен або Oauth – На API не повинно бути ліцензійних обмежень щодо кількості запитів і квот для переданих даних через API-канал. – Програмна продукція дозволяє створити 10 окремих користувачів без необхідності отримання додаткової ліцензії.

4	**Вимоги до пісочниці**	– Програмна продукція повинна мати власну систему пісочниці, яка дозволяє виконувати перевірку файлів за допомогою методів як WebUI, так і API. Використання сторонніх рішень для пісочниць або OEM є неприйнятним. – Система пісочниці повинна дозволяти запуск та аналіз URL-адрес і веб-сайтів, що мають з'єднання з мережею TOR. Пісочниця повинна підтримувати інтерактивну сесію в реальному часі з віртуальною машиною для запуску, щоб забезпечити безпечне відвідування ресурсів Darkweb – Система пісочниці повинна підтримувати аналіз файлів розміром не менше 2 ГБ. – Система пісочниці повинна підтримувати наступні типи файлів для аналізу: • DLL, EXE, MSI • 7z, bz2, cab, gzip, img, iso, msg, rar, tar, zip • MS Office, html, hta, pdf, swf • bat, ps1, js, vbe, vbs • DMG, ELF, mach-o, PKG – Система пісочниці повинна підтримувати спеціальний API-інтерфейс, що дозволяє завантажувати файли та URL-адреси для аналізу, а також завантажувати звіти про результати аналізу з деталями. – Виробник програмної продукції повинен надати готовий до використання програмний код, що дозволяє взаємодіяти з API пісочниці, написаний щонайменше на Python. – Система пісочниці повинна підтримувати подачу файлів для аналізу за допомогою завантаження локальних файлів через WebUI, отримання з URL та подачі через API. – Система пісочниці повинна підтримувати запобігання технікам шкідливого ПЗ, що використовують методи боротьби з віртуалізацією (Anti-VM). – Система пісочниці повинна бути здатна виявляти віртуалізацію процесора. – Система пісочниці повинна мати власну кастомну структуру для створення образів віртуальних машин, спеціалізовану на аналізі шкідливого ПЗ. – Система пісочниці повинна бути обладнана спеціалізованим агентом ядра, що запобігає методам шкідливого ПЗ проти віртуалізації. – Система пісочниці повинна виконувати як статичний, так і поведінковий аналіз зразка.

		– Результати кожного аналізу повинні бути представлені у вигляді числового значення на основі внутрішнього рішення. – Звіт з системи пісочниці повинен позначати виявлені MITRE TTPs та візуалізувати їх на матриці MITRE. – Звіт також повинен позначати шкідливі дії та виявлену родину шкідливого ПЗ (якщо це можливо в конфігураційному файлі). – Системи пісочниці повинні підтримувати завантаження повних даних з forensic-аналізу, включаючи: захоплення пакетів, дампи пам'яті та запис екрана віртуальної машини в реальному часі.
5	**Вимоги до оцінки ризиків**	– Ризиковий бал повинен бути представлений у вигляді числового значення – Ризиковий бал повинен обчислюватися на основі валідаційних факторів з прозорим представленням доказів. Фактори повинні бути унікальними для кожного типу IOC. – Описові фактори ризику повинні бути пов'язані з часом, щоб мінімізувати ймовірність неправильної оцінки ризиків і знизити кількість хибнопозитивних результатів. – Для оцінки ризику файлів (хешів) програмна продукція повинна враховувати такі фактори: • Позитивний вердикт про наявність шкідливого ПЗ • Виявлення в сканерах No-Distribute • Пов'язаність із кібератакою • Пов'язаність із APT-групою • Повідомлення від DHS AIS (Міністерства внутрішньої безпеки США). – Для оцінки ризику URL-адрес програмна продукція повинна включати наступні фактори: • Активне розповсюдження шкідливого ПЗ • Фішинг • Наявність у звітах DHS AIS (Американським інститутом безпеки) • Виявлений шахрайський контент • Проксі URL • Наявність у глобальних чорних списках – Для оцінки ризику доменів програмна продукція повинна включати наступні фактори: • Домен C2 • Фішинговий домен • Виявлені шахрайські операції • Джерело спаму

		• Швидка зміна IP (fast flux) • Зв'язок з кібернападом – Для оцінки ризику IP-адрес програмна продукція повинна включати наступні фактори: • Активний С2-узел • Активна комунікація з С2-узел • Активний сервер управління С2 • Наявність критичної вразливості • Діяльність ботнету • Діяльність DDoS • Діяльність брутфорсу • Пов'язаність з кібернападом • Пов'язаність з групою APT
14	**Вимоги до ліцензування**	– Максимальна кількість користувачів системи - до 10 – Кількість запитів і квот для переданих даних в тому числі через API-канал необмежено – Максимальна кількість файлів для аналізу в пісочниці, щодня не менше 1000 – Система пісочниці повинна підтримувати аналіз файлів максимальним розміром не менше 2 ГБ – Строк дії ліцензії 1 рік
15	**Вимоги до підтримки**	– Підтримка 24/7/365 за електронною поштою і телефоном. – Надання виділеного інженера для налаштування програмної продукції – Необмежений доступ до онлайн-матеріалів для навчання на сайті виробника. – Надання консультацій з питань створення готової розвідки, оновлення та виправлення інформації, її доступності на платформі для аналітиків.

Активація програмної продукції здійснюється автоматично в момент припинення дії попередньої ліцензії 16.12.2025.

4.2. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

- Не застосовуються.

4.3. Вимоги до безпеки

- Мережеві з'єднання з програмною продукцією повинні бути криптографічно захищені з використанням протоколу HTTPS, що забезпечує конфіденційність та цілісність даних.

- Для автентифікації та авторизації аналітиків програмна продукція повинна підтримувати багатофакторну аутентифікацію (MFA) з використанням щонайменше MFA-токена
- Програмна продукція повинна підтримувати функцію SSO, щонайменше для Microsoft Azure AD (Entra ID)

4.4. Вимоги до ергономіки та технічної естетики;

- Не застосовуються.

4.5. Вимоги до захисту інформації

- Відповідність Закону України «Про захист інформації в інформаційно-комунікаційних системах».

4.6. Вимоги до стандартизації та уніфікації

- Не застосовуються.

4.7. Вимоги до надійності засобу інформатизації та збереженості інформації

- Не застосовуються.

4.8. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи

- Виробник програмної продукції повинен підтримувати інтеграцію з провідними постачальниками рішень у сфері кібербезпеки, принаймні з такими компаніями:
    - Palo Alto Networks
    - IBM
    - Fortinet
    - Splunk
    - Microsoft

4.9. Вимоги до режимів функціонування засобу інформатизації

- 24/7.

4.10. Вимоги до функцій (завдань), що виконуються засобом інформатизації

- Не застосовуються.

5. Вимоги до розробки та передачі послуг

5.1. Вимоги до розробки

- Відсутні

5.2. Вимоги до передачі

- Забезпечення відображення примірників ПП у кабінеті Замовника на порталі Виробника програмної продукції.

5.3. Вимоги до гарантійної підтримки

- Надання консультацій по телефону, електронній пошті та на сайті підтримки виробника щодо питань встановлення, налаштування та експлуатації системи з понеділка по неділю з 00.00 до 24.00 годин (цілодобово).
- Постійний (24x7) авторизований доступ до сайту виробника.

6. Висновки.

- Призначення та цілі інформатизації відповідно до цих Технічних вимог забезпечують якісну реалізацію визначених планових потреб Замовника та забезпечення функціонування об'єкту інформатизації і гарантує відповідність набору критеріїв, які описують засіб інформатизації.

7. Додатки.

- Відсутні.

8. Заявка на модернізацію (модифікацію, розвиток).

- Не передбачена.

**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.*

Учасник має право запропонувати еквівалент конкретної торговельної марки чи фірми, патенту, конструкції або типу предмета закупівлі, джерела його походження або виробника, які вживаються в цих вимогах, за умови, що такий еквівалент буде з такими ж показниками та відповідатиме вимогам, встановленим у цій технічній специфікації.

Додаток 2

Кваліфікаційні критерії процедури закупівлі та перелік документів, що підтверджують інформацію учасників про відповідність їх таким критеріям

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії виконаного договору та документів, що підтверджують його виконання. ** Під аналогічним договором розуміється договір подібний за предметом закупівлі за період з 2014 року по теперішній час. Якщо в довідці учасник вказує декілька аналогічних договорів, то всі документи щодо підтвердження виконання таких договорів надаються щодо кожного із вказаних в довідці договорів.*

Для належного захисту інтересів Замовника щодо авторизованого джерела постачання за даними торгами Учасник повинен надати Авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника, дистриб'ютора в Україні, який підтверджує наявність у Учасника права на здійснення продажу запропонованого Учасником ліцензійного програмного забезпечення.

Учасник у технічній частині своєї пропозиції повинен надати інформаційний лист або довідку в довільній формі про можливість поставки товару відповідно до технічної специфікації із зазначенням конкретної назви програмної продукції, що пропонується учасником, та терміну її дії.

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **Є. В. Буржинський**

Додаток 4
Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 76
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 2024-2027 роки

м. Київ «16» липня 2025 року

ПРИСУТНІ:

Члени робочої групи:
В. Жучков
А. Жежера
С. Осіпов
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 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257) (далі – Програма), у 2025 році, а саме:

1.1. проєкт технічних вимог до закупівлі «Обладнання для керування зовнішнім освітленням» (пункт 5.1 «Створення, розвиток та супровід програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення міста Києва» переліку завдань і заходів Програми);

1.2. проєкт технічних вимог до закупівлі «Програмна продукція для моніторингу стану кіберзахищеності об'єктів кіберзахисту» (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);

1.3. проєкт технічних вимог до закупівлі «Програмна продукція підсистеми кіберзахисту Sandbox» (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 пункту 1.1 питання 1

СЛУХАЛИ:

С. Осіпова, який повідомив, що підвищення рівня безпеки на вулицях міста, економії коштів на зовнішньому освітленні планується придбання комплектів демодуляторів для керування LED драйвером, які забезпечують високу економію електроенергії при низьких витратах на установку і обслуговування пристрою, та призначені для управління потужністю освітлювальних приладів через 0-10 В інтерфейс та представив проєкт технічних вимог до закупівлі «Обладнання для керування зовнішнім освітленням» (пункт 5.1 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: Д. Цвігун, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівель «Обладнання для керування зовнішнім освітленням» (пункт 5.1 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 5, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По пункту 1.2 питання 1

СЛУХАЛИ:

В. Жучкова, який поінформував про необхідність забезпечення функціонування інформаційно-комунікаційної системи моніторингу та кібербезпеки, здійснення заходів, передбачених законодавством України у сфері кібербезпеки, проведення цілодобового моніторингу, аналізу, реагування та передачі інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту, що належать до комунальної власності територіальної громади міста Києва, шляхом використання відповідного програмного забезпечення та представив проєкт технічних вимог до закупівлі «Програмна продукція для моніторингу стану кіберзахищеності об'єктів кіберзахисту» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: Д. Цвігун, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для моніторингу стану кіберзахищеності об'єктів кіберзахисту» (пункт 6.5 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 5, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

По пункту 1.3 питання 1

СЛУХАЛИ:

В. Жучкова, який поінформував, що для організації цілодобового моніторингу стану кіберзахищенності шляхом збору та кореляцій подій кібербезпеки та

ідентифікації зловмисної активності в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах 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 придбати відповідне програмне забезпечення та представив проєкт технічних вимог до закупівлі «Програмна продукція підсистеми кіберзахисту Sandbox» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: Д. Цвігун, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція підсистеми кіберзахисту Sandbox» (пункт 6.5 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 5, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1641 **Дата реєстрації** 16.07.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 16.07.2025 (Протокол № 76 від 16.07.2025)

Кількість файлів: 4 **Кількість ЕП:** 20

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
16.07.2025 № 075-1641

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Жучков Василь Анатолійович **Кількість ЕП:** 4	17.07.2025 13:33:11 ; 17.07.2025 13:33:13 ; 17.07.2025 13:33:15 ; 17.07.2025 13:33:18 ;	17.07.2025 13:33:18 Погодив;	17.07.2025 13:33:18 Погодив
Цвігун Дмитро Вікторович **Кількість ЕП:** 4	16.07.2025 21:01:18 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ;	16.07.2025 21:01:19 Погодив;	16.07.2025 21:01:19 Погодив
Цвігун Дмитро Вікторович **Кількість ЕП:** 4	16.07.2025 21:01:18 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ;	16.07.2025 21:01:19 Погодив;	16.07.2025 21:01:19 Погодив
Цвігун Дмитро Вікторович **Кількість ЕП:** 4	16.07.2025 21:01:18 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ; 16.07.2025 21:01:19 ;	16.07.2025 21:01:19 Погодив;	16.07.2025 21:01:19 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 4	16.07.2025 20:23:17 ; 16.07.2025 20:23:18 ; 16.07.2025 20:23:19 ; 16.07.2025 20:23:20 ;	16.07.2025 20:23:20 Погодив;	16.07.2025 20:23:20 Погодив

ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 4	16.07.2025 17:14:34 ; 16.07.2025 17:14:35 ; 16.07.2025 17:14:36 ; 16.07.2025 17:14:38 ;	16.07.2025 17:14:39 Погодив;	16.07.2025 17:14:38
Самойленко Тамара Анатоліївна **Кількість ЕП:** 4	16.07.2025 17:04:46 ; 16.07.2025 17:04:47 ; 16.07.2025 17:04:47 ; 16.07.2025 17:04:48 ;	16.07.2025 17:04:48 Погодив;	16.07.2025 17:04:48 Погодив

Україна, 01133, м. Київ,
вул. Євгена Коновальця, 32-Г,
приміщення 267
Тел./факс +38 044-239-15-33

02.09.2025р.

Спеціалізоване комунальне підприємство «Київтелесервіс»

Комерційна пропозиція

У відповідь на Ваш запит №321-2025 від 26.08.2025 щодо закупівлі програмної продукції для підсистеми захисту Sandbox, ТОВ «ОЛМАКС СІСТЕМС» направляє комерційну пропозицію:

№	Назва	к-ть	Ціна за од. грн з ПДВ	Сума, грн з ПДВ
1	Програмна продукція підсистеми кіберзахисту Sandbox (Recorded Future продовження) (Доступ до програмного забезпечення Recorded Future терміном на 12 місяців. Модуль Module Access to the SecOps Intelligence Module for up to 10 users.)	1	3 837 600,00	3 837 600,00
Всього грн. без ПДВ				3 198 000,00
ПДВ				639 600,00
Всього грн з ПДВ				3 837 600,00

Термін постачання: 5 робочих днів з дати підписання договору

Умови оплати: 5 календарних днів з дати підписання акту приймання-передачі ПЗ.

Директор **Гончарук О.С.**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 259/2025
Від 02.09. 2025 р.

ТОВ «ВІ ЄМ ДЖІ»
ЄДРПОУ 40844268
+380 96 001 01 61
info@wmgroup.com.ua
wmgroup.com.ua

Комерційна Пропозиція

Компанія "ВІ ЄМ ДЖІ" вдячна Вам за довіру та проявлений інтерес до нашої продукції. Отримавши Ваш запит, ми готові надати Вам повний спектр IT-послуг на самих вигідних для Вас умовах. Нижче пропонуємо Вашій увазі пропозицію згідно Ваших технічних вимог:

№	Назва	к-ть	Ціна за од. грн без ПДВ	Сума, грн без ПДВ
1	Програмна продукція підсистеми кіберзахисту Sandbox (Recorded Future продовження) (Доступ до програмного забезпечення Recorded Future терміном на 12 місяців. Модуль Module Access to the SecOps Intelligence Module for up to 10 users.)	1	3 185 000,00	3 185 000,00
Всього грн. без ПДВ				3 185 000,00
ПДВ				637 000,00
Всього грн з ПДВ				3 822 000,00

З повагою. Комерційний директор ТОВ «ВІ ЄМ ДЖІ» **Комар О.Л**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 258/2025
Від 04.09. 2025 р.

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

Вих№ 090225/4 від 02.09.2025
На № 320-2025 від 26.08.2025

СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію, у відповідь на Ваш запит щодо вартості закупівлі програмної продукції для підсистеми захисту Sandbox.

№	Назва	К-ть	Ціна за од. грн без ПДВ	Сума, грн з ПДВ
1	Програмна продукція підсистеми кіберзахисту Sandbox (Recorded Future продовження) (Доступ до програмного забезпечення Recorded Future терміном на 12 місяців. Модуль Module Access to the SecOps Intelligence Module for up to 10 users.)	1	3 165 500,00	3 798 600,00
			Всього грн. без ПДВ	3 165 500,00
			ПДВ	633 100,00
			Всього грн з ПДВ	**3 798 600,00**

Умови поставки: 7 календарних днів з дати отримання заявки на постачання

З повагою,
Генеральний директор
ТОВ «ОПТІДАТА» Білик М.А.

Україна Київська область Товариство з обмеженою відповідальністю «ОПТІДАТА» 39693067

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 260/2025
Від 02.09 2025 р.

info@optidata.com.ua
www.optidata.com.ua