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

**Начальника центру моніторингу та кібербезпеки міських сервісів Цвєткова Василя Костянтиновича**

# СЛУЖБОВА ЗАПИСКА

місто Київ «14» вересня 2026 року

Конкретна назва предмета закупівлі – **Програмна продукція для 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, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань та 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 14.05.2026 № 604/11071).

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

*Обґрунтування необхідності посилання на конкретні марку та виробника:*

Посилання на конкретне найменування ПП обумовлено її поточним використанням для поглибленого аналізу підозрілих та шкідливих файлів в ізольованому середовищі Центром моніторингу та кібербезпеки міських сервісів та Наказом спеціалізованого комунального підприємства «Київтелесервіс» від 30.12.2024 № 151 «Про введення в 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 розроблені на виконання заходу 6.5 переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки з урахуванням характеристик програмної продукції, що вже використовується на підприємстві і виконує всі необхідні функції, та рекомендовані до використання протоколом № 74 від 03.08.2026 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.

*Обґрунтування очікуваної вартості предмета закупівлі:*

Очікувана вартість предмета закупівлі сформована Ініціатором закупівлі відповідно до Порядку визначення очікуваної вартості предмета закупівлі в спеціалізованому комунальному підприємстві «Київтелесервіс» (далі - СКП «Київтелесервіс»), розробленого на основі Примірної методики визначення очікуваної вартості предмета закупівлі (наказ Мінекономіки від 18.02.2020

№ 275) та затвердженого наказом СКП «Київтелесервіс» від 21.08.2023 № 68, з використанням методу порівняння ринкових цін у спосіб, що передбачає направлення не менше 3-х письмових запитів цінових пропозицій (електронною поштою) виробникам, офіційним представникам та дилерам, постачальникам конкретного товару, надавачам послуг.

Згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін шляхом направлення запитів учасникам ринку, очікувана вартість становить 5 254 335,00 (п'ять мільйонів двісті п'ятдесят чотири тисячі триста тридцять п'ять 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 2026 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.

Строк поставки – до 16.12.2026.

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.

**Додатки:**

1. Додаток 1. Технічні вимоги на 8 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Протокол № 86 засідання робочої групи на 2 арк.
4. Додаток 4. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 6 арк.
5. Додаток 5. Лист від дистриб'ютора щодо розбіжності в найменуванні ПП на 1 арк.

**Ініціатор закупівлі** _____ **В.К. Цвєтков**

**«ПОГОДЖЕНО»:**

**Начальник відділу кібербезпеки міських сервісів** _____ **Є.В. Буржинський**

**Перший заступник директора** _____ **С.П. Пашков**

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

## 1. Загальні положення

### 1.1. Підстава для розроблення технічних вимог

Технічні вимоги (далі – ТВ) розроблені на виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань та 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 14.05.2026 № 604/11071).

Технічні вимоги розроблено відповідно до постанови Кабінету Міністрів України (далі – КМУ) від 21.02.2025 № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» (в редакції постанови КМУ від 25.03.2026 № 373).

### 1.2. Найменування засобу інформатизації

Програмна продукція для підсистеми кіберзахисту Sandbox (далі – ПП) у складі інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС).

### 1.3. Мета придбання засобу інформатизації

Продовження строку дії ПП для забезпечення поглибленого аналізу підозрілих та шкідливих файлів в ізольованому середовищі, що дозволяє виявляти нові, раніше невідомі кіберзагрози (zero-day), обфусковані зразки шкідливого програмного забезпечення (далі – ПЗ) та складні багаторівневі кібератаки.

## 2. Обґрунтування потреби

### 2.1. Опис потреби Замовника

З метою забезпечення належного виконання покладених завдань на Центр моніторингу та кібербезпеки міських сервісів спеціалізованого комунального підприємства «Київтелесервіс» (далі – Центр) у сфері кіберзахисту, зокрема здійснення поглибленого аналізу підозрілих та шкідливих файлів в ізольованому середовищі, виникає потреба у продовженні строку дії ПП.

Необхідність закупівлі обумовлена закінченням поточного строку дії ПП та потребою у забезпеченні безперервного функціонування ІКС.

Використання зазначеної ПП дозволяє забезпечувати:

- поглиблений аналіз підозрілих та шкідливих файлів в ізольованому середовищі;
- виявлення нових, раніше невідомих кіберзагроз;
- виявлення обфускованих зразків ПЗ;
- виявлення складних багаторівневих кібератак.

### 2.2. Перелік об'єктів інформатизації, яких стосується потреба

Об'єктом інформатизації є ІКС, що розгорнута на обчислювальних потужностях наземної інфраструктури Замовника та забезпечує цілодобовий моніторинг стану кіберзахищеності шляхом збору та кореляції подій кібербезпеки та ідентифікації зловмисної активності в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах секретаріату Київської міської ради, 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 тощо.

### 2.3. Опис обстежених робочих процесів (бізнес-процесів)

У рамках функціонування ІКС здійснюються такі ключові процеси:

- автоматизація та цифровізація безперервних процесів збору і збереження інформації про кіберінциденти та кібератаки, їх категоризацію, пріоритезацію та атрибуцію;
- моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом або кібератакою щодо об'єктів кіберзахисту, 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 тощо (далі – ОК);
- автоматизація заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки, усунення їх наслідків;
- аналіз та моделювання поведінки зловмисника відповідно до відомих сценаріїв кіберінцидентів;
- систематизація та узагальнення інформації, формування статистичних і аналітичних звітів, візуалізація інформаційних панелей (дашбордів);
- пошук та виявлення вразливостей ОК;
- захист кінцевих точок від шкідливого програмного забезпечення;
- забезпечення електронної взаємодії з ОК;
- захист інформації від несанкціонованого доступу та модифікації шляхом здійснення відповідних організаційних і технічних заходів;
- забезпечення кібербезпеки вебпорталів та вебдодатків;
- виконання інших завдань, необхідних для забезпечення виконання Центром покладених функцій у сфері кіберзахисту.

Зазначені процеси функціонують цілодобово (24/7) та потребують безперервної роботи ПП.

### 2.4. Очікуваний результат

Очікуваним результатом є продовження строку дії ПП на 1 рік, що забезпечить підвищення рівня кіберзахисту ОК шляхом виявлення нових кіберзагроз, обфускованих зразків шкідливого ПЗ та складних багаторівневих кібератак.

## 3. Опис інформаційного середовища об'єктів інформатизації

### 3.1. Володільці інформації, розпорядники системи та користувачі

Власник системи – територіальна громада міста Києва в особі Київської міської ради.

Розпорядник системи – Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Адміністратор системи – спеціалізоване комунальне підприємство «Київтелесервіс» (далі – СКП «Київтелесервіс»).

Користувачі:

- співробітники Центру;
- уповноважені особи підключених організацій – в частині інформації щодо власних ОК.

### 3.2. Суб'єкти та об'єкти доступу до інформації

Суб'єктами доступу є:

- адміністратори системи – мають повний доступ до налаштувань та даних системи;
- аналітики безпеки – мають доступ до подій, інцидентів, звітів та панелей моніторингу відповідно до ролі;
- уповноважені особи підключених організацій – мають обмежений доступ лише до даних, що стосуються їх власних ОК.

Об'єктами доступу є: бази даних подій, інформаційні панелі, звіти, записи про інциденти, конфігураційні дані системи.

## 4. Вимоги до предмету закупівлі

### 4.1. Вимоги до загальної побудови та складу предмету закупівлі

Склад закупівлі:

**Програмна продукція для підсистеми кіберзахисту Sandbox (Recorded Future продовження)*** (*опис наведено у Таблиці 1*).

Таблиця 1. Опис ПП

| Найменування* | Опис | Кількість ліцензій | Термін дії |
|---|---|---|---|
| Програмна продукція для підсистеми кіберзахисту Sandbox (Recorded Future продовження) | Доступ до модулю SecOps Intelligence не менше 5 користувачів | 1 | 1 рік |

Активація програмної продукції здійснюється автоматично в момент припинення дії попередньої ліцензії 16.12.2026.

### 4.2. Вимоги до функціональних можливостей предмету закупівлі

ПП повинна забезпечувати виконання таких функцій:

**Загальні вимоги до функціоналу ПП:**

- 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 скорельовані 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 SNORT 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.

**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;
  - Darknet 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 Darknet);
  - CVE (спільні вразливості та експлойти);
  - Продукт і програмне забезпечення.
- Програмна продукція повинна містити у 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.

**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 не менше 5 окремих користувачів без необхідності отримання додаткової ліцензії.

**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 Darknet.
- 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.

**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 (Американський інститут 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 C2-вузол;
  - Активна комунікація з C2-вузол;
  - Активний сервер управління C2;
  - Наявність критичної вразливості;
  - Діяльність ботнету;
  - Діяльність DDoS;
  - Діяльність брутфорсу;
  - Пов'язаність з кібернападом;
  - Пов'язаність з групою APT.

### 4.3. Вимоги до режимів функціонування предмету закупівлі

ПП повинна функціонувати в цілодобовому режимі (24/7).

### 4.4. Вимоги до захисту інформації та кіберзахисту

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

### 4.5. Вимоги до продуктивності

- Кількість користувачів системи – не менше 5.
- Кількість запитів і квот для переданих даних, в тому числі через API-канал, - необмежено.

- Максимальна кількість файлів для аналізу в пісочниці - не менше 1000 на день.
- Система пісочниці повинна підтримувати аналіз файлів максимальним розміром не менше 2 ГБ.

**4.6. Вимоги до сумісності**

Виробник програмної продукції повинен підтримувати інтеграцію з провідними постачальниками рішень у сфері кібербезпеки, принаймні з такими компаніями:

- Palo Alto Networks;
- IBM;
- Fortinet;
- Splunk;
- Microsoft.

**5. Вимоги до гарантійної підтримки**

- Цілодобова (24/7/365) підтримка та надання консультацій за електронною поштою, телефоном та на сайті підтримки виробника щодо питань встановлення, налаштування та експлуатації системи.
- Надання консультацій з питань створення готової розвідки, оновлення та виправлення інформації, її доступності на платформі для аналітиків.
- Постійний (24x7) авторизований доступ до сайту виробника.
- Надання виділеного інженера для налаштування програмної продукції.
- Необмежений доступ до онлайн-матеріалів для навчання на сайті виробника.

**6. Вимоги до приймання предмету закупівлі**

Приймання примірників ПП здійснюється уповноваженими особами Замовника та Постачальника. Перевірці підлягає:

- наявність та дійсність ліцензійних документів з відображенням строку дії та обсягу ліцензування;
- відображення примірників ПП у кабінеті Замовника на порталі виробника;
- активація ліцензій та безперервна робота ПП після поновлення.

Приймання-передача здійснюється на підставі Акту приймання-передачі, підписаного уповноваженими особами Замовника та Постачальника.

---

** У разі використання в цьому 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.*

*Посилання на конкретне найменування програмної продукції в цих технічних вимогах обумовлено її поточним використанням для кіберзахисту Sandbox у складі впровадженої ІКС.*

**Ініціатор закупівлі** **В.К. Цвєтков**

**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.<br>На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії виконаного договору та документів, що підтверджують його виконання.<br>** 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** **В.К. Цвєтков**

**Додаток 3**

Засідання в онлайн режимі
із використанням Microsoft Teams

**ПРОТОКОЛ № 86**
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 «01» вересня 2026 року

**ПРИСУТНІ:**

*Члени робочої групи:*
А. Жежера
Н. Йожиков
М. Клюєва
С. Осіпов
С. Пашков
Т. Самойленко
В. Тихонов

**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 14.05.2026 № 604/11071) (далі – Програма), у 2026 році, а саме:

1.1. проєкт технічних вимог до закупівлі «Засоби зв'язку для забезпечення безпроводових підключень (комплекти обладнання зв'язку)» (пункт 6.2 «Створення, розвиток та модернізація мережевої інфраструктури, сервісної мережевої інфраструктури, платформи Інтернету речей (IoT), мереж доступу, радіомереж, системи отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку» переліку завдань і заходів Програми);

1.2. проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми кіберзахисту Sandbox» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань і заходів Програми).

2. Різне.

*По пункту 1.1 питання 1*

**СЛУХАЛИ:**

В. Тихонова, який поінформував, що з метою створення структурованих кабельних систем з Wi-Fi доступом до мережі Інтернет в закладах загальної середньої освіти міста Києва є необхідність придбання комплектів обладнання зв'язку та представив проєкт технічних вимог до закупівлі «Засоби зв'язку для забезпечення безпроводових підключень (комплекти обладнання зв'язку)» (пункт 6.2 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: А. Жежера, С. Осіпов.

**УХВАЛИЛИ:**

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Засоби зв'язку для забезпечення безпроводових підключень (комплекти обладнання зв'язку)» (пункт 6.2 переліку завдань і заходів Програми), використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

**ГОЛОСУВАЛИ:** «ЗА» - 7, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

*По пункту 1.2 питання 1*

**СЛУХАЛИ:**

В. Тихонова, який поінформував, що з метою забезпечення належного виконання завдань, покладених на Центр моніторингу та кібербезпеки міських сервісів спеціалізованого комунального підприємства «Київтелесервіс» у сфері кіберзахисту, зокрема щодо здійснення поглибленого аналізу підозрілих та шкідливих файлів в ізольованому середовищі, що дозволяє виявляти нові, раніше невідомі кіберзагрози (zero-day), обфусковані зразки шкідливого програмного забезпечення та складні багаторівневі кібератаки, використовується відповідна програмна продукція, у якої закінчується строк дії ліцензії, та представив проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми кіберзахисту Sandbox» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: А. Жежера, С. Осіпов.

**УХВАЛИЛИ:**

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

**ГОЛОСУВАЛИ:** «ЗА» - 7, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

# Інформація про електронні підписи (ЕП)

**№ документа** 075-2025 **Дата реєстрації** 01.09.2026
**Документ зареєстровано у картотеці:** Вихідна
**Вид документа:** Лист
**Стислий зміст:**
Матеріали засідання робочої групи 01.09.2026 (Протокол № 86 від 01.09.2026)

**Кількість файлів:** 3 **Кількість ЕП:** 21

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
01.09.2026 № 075-2025

**Перелік електронних підписів**

| П.І.Б. | Дати і час нанесення ЕП | Погодження | Час останнього нанесення ЕП |
|---|---|---|---|
| ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 3 | 02.09.2026 09:59:18 ;<br>02.09.2026 09:59:20 ;<br>02.09.2026 09:59:22 ; | 02.09.2026 09:59:22<br>Погодив; | 02.09.2026 09:59:22<br>Погодив |
| Тихонов Володимир Володимирович **Кількість ЕП:** 3 | 01.09.2026 17:34:05 ;<br>01.09.2026 17:34:06 ;<br>01.09.2026 17:34:08 ; | 01.09.2026 17:34:08<br>Погодив; | 01.09.2026 17:34:08<br>Погодив |
| КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 3 | 01.09.2026 15:19:48 ;<br>01.09.2026 15:19:50 ;<br>01.09.2026 15:19:52 ; | 01.09.2026 15:19:52<br>Погодив; | 01.09.2026 15:19:52<br>Погодив |
| Йожиков Нікіта Сергійович **Кількість ЕП:** 3 | 01.09.2026 14:42:52 ;<br>01.09.2026 14:42:53 ;<br>01.09.2026 14:42:54 ; | 01.09.2026 14:42:55<br>Погодив; | 01.09.2026 14:42:54 |
| Пашков Сергій Петрович **Кількість ЕП:** 3 | 01.09.2026 14:14:25 ;<br>01.09.2026 14:14:26 ;<br>01.09.2026 14:14:27 ; | 01.09.2026 14:14:27<br>Погодив; | 01.09.2026 14:14:27<br>Погодив |

| | | | |
|---|---|---|---|
| | | | |
| ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ<br>**Кількість ЕП:** 3 | 01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ; | 01.09.2026 14:12:16<br>Погодив; | 01.09.2026 14:12:16<br>Погодив |
| ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ<br>**Кількість ЕП:** 3 | 01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ; | 01.09.2026 14:12:16<br>Погодив; | 01.09.2026 14:12:16<br>Погодив |
| ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ<br>**Кількість ЕП:** 3 | 01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ;<br>01.09.2026 14:12:16 ; | 01.09.2026 14:12:16<br>Погодив; | 01.09.2026 14:12:16<br>Погодив |
| Самойленко Тамара Анатоліївна<br>**Кількість ЕП:** 3 | 01.09.2026 13:58:41 ;<br>01.09.2026 13:58:42 ;<br>01.09.2026 13:58:43 ; | 01.09.2026 13:58:43<br>Погодив; | 01.09.2026 13:58:43<br>Погодив |

**ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ**
**«СМАРТ СІТІ УКРАЇНА»**

*08131, м. Київ, вул. Німанська,10 А, офіс 3,*
*Код ЄДРПОУ 43236898*
*Тел: +380632540601*
*e_info@smartcityua.com.ua*

*Вих. №0709 від «07» вересня 2026 р.*

**СПЕЦІАЛІЗОВАНЕ КОМУНАЛЬНЕ ПІДПРИЄМСТВО "К И Ї В Т Е Л Е С Е Р В І С" ( С К П « К И Ї В Т Е Л Е С Е Р В І С » )**
вул. Хрещатик, буд. 10, м. Київ, 01001 (юридична адреса),
а/с 38, м. Київ-04071 (для листування), тел.: (044) 366 85 00
*e-mail: KTS@KYIVCITY.GOV.UA, код ЄДРПОУ 31815760*

| № | Найменування | Кі-ть | Вартість шт, грн без ПДВ | Вартість разом, грн без ПДВ |
|---|---|---|---|---|
| 1 | Програмна продукція для забезпечення кіберзахисту Recorded Future CyberOps Solution Package для п'яти користувачів строком на 12 місяців. | 1 | 4 375 250.00 | 4 375 250.00 |
| | | | Загальна вартість, грн. без ПДВ | 4 375 250,00 |
| | | | ПДВ, грн. | 875 050.00 |
| | | | Загальна вартість, грн. з ПДВ | 5 250 300,00 |

**Директор** **Чурсін І.В.**

**ТОВ «СМАРТ СІТІ Україна»**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/784
Від 07.09 2026 р.

**ТОВ «ВІ ЄМ ДЖІ»**

ЄДРПОУ 40844268
+380 96 001 01 61
info@wmgroup.com.ua
wmgroup.com.ua

Вих.№180 від 07.09.2026

**СКП «КИЇВТЕЛЕСЕРВІС»**

## КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 075/2-1492 від 03.09.2026 надаємо вартість Програмної продукції для підсистеми кіберзахисту Sandbox (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки):

| № | Найменування | Кіл-ть | Од. вимір | Ціна, грн без ПДВ | Сума, грн без ПДВ |
|---|---|---|---|---|---|
| 1 | Програмна продукція для забезпечення кіберзахисту Recorded Future CyberOps Solution Package для п'яти користувачів строком на 12 місяців | 1 | шт. | 4 393 700,00 | 4 393 700,00 |
| | | | | **Всього грн, без ПДВ** | **4 393 700,00** |
| | | | | Податок на додану вартість (20%), грн | 878 740,00 |
| | | | | **Загальна сума грн, з ПДВ** | **5 272 440,00** |

Ціну пропозиції вказано на дату надання та може бути змінені при укладанні договору.

Просимо звернути увагу, що комерційна пропозиція підготовлена з урахуванням актуальних пакетних пропозицій виробника, що діють у поточному році.

Комерційний Директор Комар Олександр

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/786
Від 07.09 2026 р.

**ТОВ «САЙБЕРПРО»**
65045 м. Одеса, вул. Велика Арнаутська
буд. 76, офіс 2, email: office@cyber-pro.org

Вих.№ 2026-09-07/1
від 07 вересня 2026 р.

Спеціалізоване комунальне
підприємство «Київтелесервіс»

## КОМЕРЦІЙНА ПРОПОЗИЦІЯ

ТОВ «САЙБЕРПРО» надає послуги в сфері кібербезпеки та добирає кращі рішення для ефективного захисту інформаційних ресурсів клієнтів.

На Ваш запит №075/2-1490 від 03.09.2026 надаємо комерційну пропозицію на постачання програмної продукції

| Найменування | Кількість | Ціна без ПДВ, грн | Вартість без ПДВ, грн |
|---|---|---|---|
| Програмна продукція для забезпечення кіберзахисту Recorded Future CyberOps Solution Package для п'яти користувачів строком на 12 місяців | 1 | 4 405 500,00 | 4 405 500,00 |
| | | **Всього, грн без ПДВ** | 4 405 500,00 |
| | | **ПДВ, грн** | 881 100,00 |
| | | **Разом з ПДВ, грн** | 5 286 600,00 |

**З повагою,**
**Директор ТОВ «САЙБЕРПРО»** /підписано КЕП/ **ДІДУР С.Г.**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/787
Від 07.09 2026 р.

Opti Data

Enforce your security

# Комерційна пропозиція

## СКП «Київтелесервіс»

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/783
Від 07.09 2026 р.

Opti Data
Enforce your security

## Про компанію

Шановні панове!

**OptiData** – українська IT-компанія, яка покликана надати інструменти для підвищення ефективності Вашого бізнесу з забезпеченням належного рівня безпеки.

**Стратегія OptiData**

Ми пропонуємо насамперед випробувані рішення, які дозволять раціонально використовувати наявні ресурси та вивільнити їх для подальшого розвитку. При цьому сучасні реалії IT-ринку потребують забезпечення належного рівня безпеки.

Наші пропозиції базуються на рішеннях лідерів ринку згідно досліджень Гартнера, що дозволяє забезпечити капіталовкладення та захист інвестицій бізнесу.

## Серед наших партнерів:

CROWDSTRIKE
MICRO FOCUS
LogRhythm
paloalto NETWORKS
Trellix
LABYRINTH
SOCRadar®
Skyhigh Security
tenable
FUDO SECURITY
Recorded Future
RAPID7
Hewlett Packard Enterprise
PICUS
TREND MICRO™
aruba a Hewlett Packard Enterprise company
SOTI MOBICONTROL
acer
DELL

Opti Data
Enforce your security

Згідно Вашого запиту просимо розглянути комерційну пропозицію від ТОВ «ОПТІДАТА»:

| № | Найменування | Кількість | Вартість за одиницю, грн без ПДВ | Вартість, грн без ПДВ |
|---|---|---|---|---|
| 1 | Програмна продукція для забезпечення кіберзахисту Recorded Future CyberOps Solution Package для п'яти користувачів строком на 12 місяців. | 1 | 4 340 000,00 | 4 340 000,00 |
| | | | Загальна вартість, грн. без ПДВ | 4 340 000,00 |
| | | | ПДВ, грн. | 868 000,00 |
| | | | Загальна вартість, грн. з ПДВ | 5 208 000,00 |

З повагою,

Комерційний директор ТОВ «ОПТІДАТА» К.С. Атаманенко

Дата: 07.09.2026

**ТОВ «Кліко Україна»**
04080, Україна, м. Київ, вулиця Вікентія Хвойки, будинок 18/14

ЄДРПОУ: 45201359
ІПН: 452013526549
IBAN UA493209840000026000210448784
в АТ «Прокредит Банк», м. Київ, Україна
МФО: 320984

Телефон: +38 (098) 242-93-53
Email: info@clico.ua

Вих. № 2609/11-01 від «11» вересня 2026 року

СКП «КИЇВТЕЛЕСЕРВІС»
kts@kyivcity.gov.ua

**Щодо найменування та функціональних можливостей програмної продукції Recorded Future**

Шановний Олександре Олександровичу!

ТОВ «КЛІКО УКРАЇНА», розглянувши Ваш лист № 075/2-1543 від 09.09.2026 року щодо розбіжності в найменуванні програмної продукції Recorded Future, повідомляє таке.

1. Щодо співвідношення «CyberOps Solution Package» та «SecOps Intelligence».

Використання в комерційній пропозиції найменування «CyberOps Solution Package» обумовлене актуальною моделлю ліцензування та найменуванням пакета виробника Recorded Future і не призводить до зменшення функціональних можливостей, передбачених технічними вимогами.

2. Щодо відповідності функціональним вимогам.

Підтверджуємо, що запропонований CyberOps Solution Package не звужує функціональні можливості програмної продукції, визначені технічними вимогами.

Відповідно до актуальної моделі ліцензування виробника Recorded Future, CyberOps Solution Package є мінімальним доступним пакетом, до складу якого входить SecOps Intelligence і який забезпечує функціональні можливості, передбачені технічними вимогами Замовника.

Просимо врахувати зазначену інформацію під час аналізу отриманої комерційної пропозиції.

Директор Олександр КРАМАРЕНКО

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/806
Від 14.09 2026 р.