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

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

СЛУЖБОВА ЗАПИСКА

місто Київ «24» червня 2026 року

Конкретна назва предмета закупівлі – **Програмна продукція для центральної підсистеми моніторингу стану кіберзахищеності об'єктів кіберзахисту (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 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 центральної підсистеми моніторингу стану кіберзахищеності об'єктів кіберзахисту (далі - ПП).

Обґрунтування необхідності посилання на конкретні марку та виробника:

Посилання на конкретне найменування ПП обумовлено її поточним використанням для моніторингу стану кіберзахищеності об'єктів кіберзахисту (далі - ОК) Центром моніторингу та кібербезпеки міських сервісів та Наказом спеціалізованого комунального підприємства "Київтелесервіс" від 29.08.2023 № 76 "Про введення у виробничу експлуатацію підсистем моніторингу та кібербезпеки".

Обґрунтування обсягів закупівлі:

Об'єм ліцензії обумовлено поточною кількістю подій в інформаційно-комунікаційній системі моніторингу та кібербезпеки (далі - ІКС), які потребують аналізу на предмет ідентифікації кіберзагроз та кіберінцидентів.

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 № 66 від 07.07.2026 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 14 982 185,60 (чотирнадцять мільйонів дев'ятсот вісімдесят дві тисячі сто вісімдесят п'ять гривень шістдесят 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 комплект, 1 супутня послуга.

Строк поставки – до 27.10.2026.

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. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 10 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Протокол № 66 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 2 арк.
4. Додаток 4. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 4 арк.

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

«ПОГОДЖЕНО»:

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**

Заступник начальника відділу з організаційних питань _____ Л.М. Задорожна

Додаток 1

ТЕХНІЧНІ ВИМОГИ

Програмна продукція для центральної підсистеми моніторингу стану кіберзахищеності об'єктів кіберзахисту (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 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 центральної підсистеми моніторингу стану кіберзахищеності об'єктів кіберзахисту (далі – ПП) у складі інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС).

1.3. Мета придбання засобу інформатизації

Продовження строку дії ПП для забезпечення безперервного функціонування ІКС та здійснення цілодобового моніторингу, аналізу, реагування і передачі інформації про кіберінциденти та кібератаки щодо об'єктів кіберзахисту (далі – ОК), 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. 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 цілодобового моніторингу, виявлення та реагування на кіберінциденти і кібератаки щодо ОК, 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:

- збір, обробку та зберігання подій;
- цілодобовий моніторинг стану кіберзахищеності шляхом збору та кореляції подій кібербезпеки;

- ідентифікацію зловмисної активності в ІКС;
- модульну архітектуру з можливістю підключення модулів (SIEM, машинне навчання, моніторинг ІТ-інфраструктури);
- управління інцидентами з єдиного порталу;
- автоматизацію заходів реагування.

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 кореляцій 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 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 з обсягом оброблюваних даних 250 ГБ/день. Це забезпечить функціонування ІКС без перерв у захисті ОК, збереження усіх поточних налаштувань, сценаріїв та панелей моніторингу, а також отримання всіх актуальних оновлень програмної продукції та технічної підтримки від виробника або авторизованого партнера протягом ліцензійного періоду.

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 SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year) – 1 комплект** (*склад комплекту наведено у Таблиці 1*);
- **Послуга, пов'язана з постачанням ПП (встановлення та налаштування).**

Таблиця 1. Склад комплекту

№ з/п	Найменування*	Обсяг оброблюваних даних	Строк дії (міс.)
1	Програмна продукція SPLUNK Enterprise (1 Year)	250 ГБ/день	12
2	Програмна продукція SPLUNK Enterprise Security (1 Year)	250 ГБ/день	12

Активація програмної продукції здійснюється 28.10.2026.

Загальні вимоги до побудови:

- ПП повинна функціонувати в існуючому середовищі ІКС без зміни архітектури;
- ПП повинна мати модульну архітектуру;
- ПП повинна встановлюватись та функціонувати на обчислювальних потужностях наземної інфраструктури Замовника;
- ПП повинна зберігати та підтримувати всі поточні конфігурації, сценарії (Use Cases) та інформаційні панелі (Dashboards), що розроблені в рамках попереднього ліцензійного договору.

4.2. Вимоги до функціональних можливостей предмету закупівлі

ПП повинна забезпечувати виконання таких функцій:

Вимоги до роботи системи:

- ПП повинна мати можливість підключення модуля збору подій щодо інформаційної безпеки.
- ПП повинна мати можливість підключення модуля машинного навчання.
- ПП повинна мати можливість підключення модуля моніторингу IT інфраструктури.
- ПП повинна мати можливість управління ресурсами для моніторингу та аналізу подій і настройками компонентів ПП.
- ПП повинна забезпечувати можливість створення власних додатків для вирішення задач бізнес-аналітики, кібербезпеки, IoT.
- ПП повинна мати аналітичну мову запитів.

Вимоги до збору подій:

- Компонент збору подій може виконувати збір подій віддалено з джерел подій, за допомогою його установки безпосередньо на джерело подій.
- Компонент збору подій, що встановлюється на джерело подій не повинен суттєво впливати на продуктивність роботи системи цього джерела
- Компонент збору подій повинен мати функціональну можливість збору подій з використанням наступних механізмів:
    - збір подій по протоколу Syslog;
    - збір подій з журналів операційної системи (ОС) Microsoft Windows (Security, System, Application, в тому числі журнали інших джерел подій, записуючих власні події в додаткові журнали Microsoft Windows);
    - збір подій з журналів операційної системи (ОС) Linux;
    - збір подій з баз даних з використанням SQL-запитів;
    - збір подій з текстових файлів;
    - збір подій з XML-файлів;
    - збір подій по протоколу NetFlow;
    - збір подій по протоколу jFlow;
    - збір подій по протоколу sFlow;
    - збір подій по протоколу IPFIX
    - збір подій по протоколу XMPP;
    - збір подій мережевого трафіку;
    - можливість локально завантажити файли формату CSV, TXT;
    - збір подій по протоколу http/https;
    - можливість збору подій через REST API;
    - можливість збору по протоколам IoT такими як: MQTT, JMS, KAFKA.
- Можливість централізованого віддаленого виконання скриптів та індексація результатів їх роботи.
- Компонент збору подій повинен мати функціональну можливість збору подій з наступних систем та обладнання:
    - Files and directories;
    - Network events;
    - Windows sources;
    - Linux sources;
    - HTTP Event Collector (HEC);

- Metrics (OT);
- Database (MySQL, Oracle, PostgreSQL);
- Microsoft Active Directory.

- Компонент збору подій повинен виробляти нормалізацію (приведення подій в єдиний формат подання) і агрегування (угруповання подій за одним або кількома критеріями) подій.
- Компонент збору подій повинен виробляти нормалізацію подій з наступних джерел подій з використанням наданих виробником конфігураційних файлів (правил нормалізації подій):
  - можливість збирати дані з пропрієтарних систем, при умові, що системи мають можливість передавати дані за допомогою озвучених вище протоколів;
  - можливість збирати дані з самописних систем, при умові, що системи мають можливість передавати дані за допомогою озвучених вище протоколам.
- Компонент збору подій повинен мати інструмент для нормалізації подій від джерел цих подій, для яких конфігураційні файли не надаються виробником. Цей інструмент повинен мати інтерактивний майстер додавання джерела для можливості використання його користувачами системи та не повинен потребувати залучення фахівців виробника чи програмування.
- Компонент збору подій повинен мати можливість маскування заданих експлуатуючим персоналом полів подій у відображенні даних.
- Компонент збору подій повинен мати можливість збору ненормалізованих подій (запис події у вихідному форматі джерела подій).
- Компонент збору подій повинен виконувати збір подій з використанням мінімальних привілеїв на джерелі подій, якщо компоненту збору подій необхідний доступ до джерела подій.
- Компонент збору подій повинен мати можливість виконувати передачу подій на компонент обробки подій за допомогою захищеного протоколу SSL.
- ПП повинна дозволяти виконувати нормалізацію (екстракцію полів) із зібраних вихідних даних в реальному часі.

Вимоги до обробки подій:

- Компонент обробки подій повинен мати можливість відстеження підозрілої активності за тривалі періоди часу на основі подій, що реєструються джерелами подій.
- Компонент обробки подій повинен мати можливість формування статистичних звітів за зібраними подіями та зафіксованими інцидентами в форматах pdf, html, csv.
- Компонент обробки подій повинен забезпечувати можливість автоматичної відправки статистичних звітів на електронну пошту експлуатуючого персоналу за заданим розкладом.
- Компонент обробки подій повинен забезпечувати можливість оповіщення експлуатуючого персоналу за допомогою Microsoft Exchange, Microsoft Teams про особливо критичні події та/або інциденти за заданими шаблонами оповіщення, що включають тільки ті поля подій, які актуальні для даної конкретної події або інциденту.
- Компонент обробки подій повинен автоматично визначати поля в зібраних даних - структурованих і неструктурованих. Також повинна бути можливість визначення та задання структури полів в даних власноруч.

Вимоги до зберігання подій:

- Компонент зберігання подій повинен виконувати зберігання та архівування подій.
- Компонент зберігання повинен мати два періоди зберігання подій:
  - online - період часу, протягом якого події повинні бути доступні для проведення моніторингу, аналізу, розслідування;

- offline - період часу, наступний після закінчення online-періоду, коли події архівуються і перестають бути доступними для проведення моніторингу, аналізу, розслідування.

– ПП повинна дозволяти зберігати вихідні дані в одній базі даних і збагачені дані в додатковій базі даних без збільшення вартості комплекту програмної продукції системи моніторингу подій кібербезпеки.
– Компонент зберігання подій повинен забезпечувати дублювання даних, що зберігаються на декількох серверах і автоматичної синхронізації даних в разі втрати зв'язку між ними.

Вимоги до процесу управління інцидентами:

– Всі інциденти кібербезпеки повинні управлятися з єдиного порталу, який дозволяє команді спеціалістів Центру отримати доступ до оновлень та інформації щодо інцидентів кібербезпеки на основі призначеної ролі користувача;
– Автоматизація повинна надавати змогу команді Центру отримувати дані безпеки та сповіщення з різних джерел даних, автоматично визначати пріоритети подій та керувати стандартизованими діями щодо реагування на інциденти відповідно до стандартного робочого процесу.
– ПП повинна надавати можливість керувати конфіденційними даними відповідно до політики організації завдяки механізму надійного контролю доступу на основі ролей та підтримувати наступні можливості:
  - створення власних ролей та ієрархій команд;
  - можливість визначення дозволу з різними ролями;
  - керувати відображенням даних з кількома рольовими переглядами;
  - налаштовувати власні варіанти відображення даних та макети сторінок за допомогою перетягування або візуального дизайнера;
  - підтримка сценаріїв автоматизації процесу управління інцидентами шляхом автоматичного доповнення інформацією щодо наявного інциденту, присвоєння статусу критичності інциденту, сповіщення спеціаліста про зміни в інциденті, тощо;
  - автоматична та ручна ескалація подій до системи оркестрації, автоматизації та реагування на кіберінциденти.

4.3. Вимоги до режимів функціонування предмету закупівлі

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

4.4. Вимоги до надійності роботи та збереження інформації

– ПП повинна функціонувати у конфігурації відмовостійкого кластера (High-Availability);
– дублювання даних на різних серверах з автоматичною синхронізацією;
– збереження всіх поточних налаштувань, правил кореляції та сценаріїв реагування після активації продовженої ліцензії.

4.5. Вимоги до захисту інформації та кіберзахисту

– відповідність Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
– наявність власного механізму авторизації користувачів;
– можливість інтеграції із зовнішніми системами або хмарними сервісами для забезпечення другого фактору автентифікації (MFA);
– підтримка інтеграції за допомогою протоколу SAML;
– внутрішня рольова модель розподілу прав доступу та щонайменше наступні ролі: адміністратор безпеки та аналітик безпеки;
– механізм захисту цілісності журналів подій за допомогою хеш-сум та можливість здійснювати контрольне порівняння за запитом;

- наявність чинного експертного висновку Державної служби спеціального зв'язку та захисту інформації України на програмне забезпечення.

4.6. Вимоги до продуктивності

- забезпечення можливості обробки даних обсягом не менше 250 ГБ/день без втрати продуктивності;
- при перевищенні обсягу даних ПП повинна продовжувати їх збір без будь-якої втрати;
- ПП повинна підтримувати не менше ніж 11 користувачів одночасно.

4.7. Вимоги до інтерфейсу користувача та зручності використання

- управління списками інцидентів та сповіщеннями щодо безпеки у вигляді сітки з можливістю фільтрації;
- візуальний редактор макетів для формування користувацьких відображень, моделей даних та полів;
- відображення даних у форматі, зручному для проведення розслідувань.

4.8. Вимоги до сумісності та електронної інформаційної взаємодії

- наявність відкритого API для інтеграції з іншими системами (отримання та експорт даних);
- сумісність з операційними системами Microsoft Windows та Linux;
- підтримка протоколів взаємодії: Syslog, NetFlow, IPFIX, REST API, SQL, SAML, SSL/TLS;
- інтеграція зі сканером вразливостей Tenable для автоматизації реєстрації вразливостей та автоматичного запуску сценарію сканування;
- можливість надання доступу до інцидентів засобами API для взаємодії з суміжними системами реагування.

5. Вимоги до супроводу та обслуговування предмету закупівлі

5.1. Вимоги до послуги, пов'язаної з постачанням ПП (встановлення та налаштування)

Таблиця 2. Вимоги до послуги

№ з/п	Вимоги
1	Виправлення невідповідностей платформи Splunk стандартам Common Information Model (CIM). Роботи повинні включати: 1. Проведення комплексного аналізу поточного використання Splunk CIM, включаючи оцінку коректності нормалізації подій, відповідності джерел даних вимогам моделей даних, налаштувань тегів, Event Types та Knowledge Objects; 2. Усунення виявлених невідповідностей за результатами аналізу; 3. Оптимізацію налаштувань Data Model Acceleration для моделей даних, що використовуються в Splunk Enterprise Security; 4. Забезпечення стабільної роботи моделей даних з мінімальним впливом на ресурси платформи.

2	Масштабування архітектури збереження даних платформи Splunk та налаштування відповідних політик. Роботи повинні включати: 1. Проведення аудиту поточної архітектури збереження даних, конфігурації індексів, політик зберігання, використання дискового простору та тенденцій росту обсягів подій; 2. Розробку та впровадження оптимізованої архітектури життєвого циклу даних відповідно до рекомендацій Виробника (Best Practices); 3. Усунення недоліків існуючої конфігурації та оптимізацію параметрів індексації; 4. Реалізацію механізму довготривалого зберігання даних із використанням SmartStore (або аналог) та сервісу AWS S3 як віддаленого сховища; 5. Забезпечення прозорого доступу до історичних даних та їх пошуку через стандартні механізми Splunk без необхідності ручного відновлення архівів; 6. Підготовку опису цільової архітектури, політик зберігання даних та рекомендацій щодо подальшого масштабування платформи.
3	Розробка візуалізацій та дашборду з інтерактивною мапою Києва. Роботи повинні включати: 1. Розробку інтерактивного аналітичного дашборду із використанням Dashboard Studio (або аналогу) для відображення об'єктів моніторингу та стану активів інфраструктури на території міста Києва; 2. Реалізацію географічної візуалізації із відображенням статистичних показників у розрізі адміністративних районів міста та підтримку інтерактивної взаємодії користувачів із даними; 3. Забезпечення підтримки часових та тематичних фільтрів, деталізації інформації шляхом drill-down переходів, відображення агрегованих та деталізованих показників; 4. Інтеграцію всіх елементів візуалізації в поточне середовище Splunk з підтримкою подальшої модифікації силами Замовника.
4	Оптимізація та налаштування моделей даних (Data Models) платформи Splunk. Роботи повинні включати: 1. Проведення аналізу моделей даних та оцінку ефективності їх використання кореляційними правилами, аналітичними дашбордами та пошуковими запитами; 2. Оптимізацію існуючих пошукових механізмів шляхом переходу на використання команд tstats та datamodel-пошуку там, де це технічно доцільно та підтримується архітектурою відповідних моделей даних.
5	Аналіз та оптимізація продуктивності роботи пошукових запитів та навантаження компонентів платформи Splunk. Роботи повинні включати: 1. Проведення комплексного дослідження продуктивності платформи з урахуванням особливостей функціонування Search Head Cluster, Indexer Cluster та інших компонентів;

	2. Аналіз параметрів Search Scheduler, Search Concurrency, Skipped Searches, Delayed Searches, тривалості виконання запитів та впливу навантаження на ресурси платформи; 3. Виявлення вузьких місць архітектури та пошукових запитів, що створюють надмірне навантаження; 4. Виконання оптимізації виявлених проблем; 5. Підготовку технічного звіту із описом виявлених проблем, виконаних оптимізацій та очікуваного ефекту.
6	Розробка єдиного дашборду з відображенням стану продуктивності платформи Splunk. Роботи повинні включати: 1. Розробку централізованого дашборду моніторингу технічного стану платформи із консолідованим відображенням показників роботи Search Head Cluster, Indexer Cluster, Cluster Manager, License Manager, Deployment Server та інших компонентів; 2. Реалізацію відображення швидкості індексації подій, кількості активних запитів, використання обчислювальних ресурсів, завантаження системних черг, стану Search Scheduler та інших ключових показників продуктивності; 3. Забезпечення централізованого контролю помилок індексації, реплікації, роботи KV Store, сервісів прискорення моделей даних та інших критичних компонентів; 4. Забезпечення оперативного виявлення відхилень у роботі системи, спрощення аналізу причин виникнення проблем та надання аналітикам і адміністраторам єдину точку контролю за станом усієї платформи; 5. Інтеграцію всіх елементів в поточне середовище Splunk з підтримкою подальшої модифікації силами Замовника.

5.2. Вимоги до гарантійної підтримки

- Отримання всіх необхідних актуальних оновлень ПП (основних та проміжних релізів) через сайт виробника;
- Підтримка програмних кодів в актуальному стані відповідно до рекомендацій виробника;
- Цілодобовий (24/7) авторизований доступ Замовника до сайту підтримки виробника;
- Надання консультацій щодо встановлення, налаштування та експлуатації системи по телефону, електронній пошті та через сайт підтримки виробника з понеділка по неділю з 00:00 до 24:00 (цілодобово).

6. Вимоги до приймання предмету закупівлі

Приймання примірників ПП та послуги, пов'язаної з постачанням (встановлення та налаштування 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;
- 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 моніторингу стану кіберзахищеності об'єктів кіберзахисту у складі впровадженої ІКС моніторингу та кібербезпеки.

Ініціатор закупівлі **Є.В. Буржинський**

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 3

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 66
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 «07» липня 2026 року

ПРИСУТНІ:

Члени робочої групи:
А. Бухта
А. Жежера
Н. Йожиков
С. Осіпов
С. Пашков
Т. Самойленко

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:

проєкт технічних вимог до закупівлі «Програмна продукція для центральної підсистеми 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, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань і заходів Програми).

2. Різне.

По питанню 1

СЛУХАЛИ:

С. Пашкова, який поінформував про необхідність продовження строку дії програмної продукції для забезпечення безперервного функціонування інформаційно-комунікаційної системи моніторингу та кібербезпеки, здійснення цілодобового моніторингу, аналізу, реагування і передачі інформації про

кіберінциденти та кібератаки 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, та представив проєкт технічних вимог до закупівлі «Програмна продукція для центральної підсистеми моніторингу стану кіберзахищеності об'єктів кіберзахисту» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: А. Жежера, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для центральної підсистеми 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» - 6, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1573 **Дата реєстрації** 07.07.2026
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 07.07.2026 (Протокол № 66 від 07.07.2026)

Кількість файлів: 2 **Кількість ЕП:** 12

ДОКУМЕНТ СЕД АСКОД ІТС СПК

Департамент інформаційно-комунікаційних технологій
07.07.2026 № 075-1573

Перелік електронних підписів

П.І.Б.	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 2	07.07.2026 21:26:48 ; 07.07.2026 21:26:49 ;	07.07.2026 21:26:49 Погодив;	07.07.2026 21:26:49 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 2	07.07.2026 18:39:57 ; 07.07.2026 18:39:59 ;	07.07.2026 18:40:22 Погодив;	07.07.2026 18:39:59
Бухта Андрій Миколайович **Кількість ЕП:** 2	07.07.2026 16:47:42 ; 07.07.2026 16:47:43 ;	07.07.2026 16:47:43 Погодив;	07.07.2026 16:47:43 Погодив
Йожиков Нікіта Сергійович **Кількість ЕП:** 2	07.07.2026 16:07:50 ; 07.07.2026 16:07:52 ;	07.07.2026 16:07:52 Погодив;	07.07.2026 16:07:52 Погодив
Пашков Сергій Петрович **Кількість ЕП:** 2	07.07.2026 15:58:58 ; 07.07.2026 15:58:59 ;	07.07.2026 15:59:00 Погодив;	07.07.2026 15:58:59

Самойленко Тамара Анатоліївна **Кількість ЕН:** 2	07.07.2026 15:55:28 ; 07.07.2026 15:55:29 ;	07.07.2026 15:55:29 Погодив;	07.07.2026 15:55:29 Погодив

CYBERPRO
AUDIT AND PROTECTION

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

Вих.№ 2026-07-16/1
від 16 липня 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.

До вашої уваги надаємо комерційну пропозицію на постачання програмної продукції та послуг.

№ п/п	Найменування	Кіль-кість	Одиниця виміру	Ціна без ПДВ, гривня	Вартість без ПДВ, гривня
1	Програмна продукція SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year)у складі: - Програмна продукція SPLUNK Enterprise 250GB/day (1 Year) - Програмна продукція SPLUNK Enterprise Security 250GB/day (1 Year)	1	комплект	10 268 122,00	10 268 122,00
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування)	1	послуга	2 110 000,00	2 110 000,00
				Всього, грн без ПДВ	12 378 122,00
				ПДВ, грн	2 475 624,40
				Разом з ПДВ, грн	14 853 746,40

З повагою,

Директор ТОВ «САЙБЕРПРО» **ДІДУР С.Г.**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/551
Від 16.07 2026 р.

ТОВ «ВІ ЄМ ДЖІ»

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

Вих.№ 124 від 20.07.2026

СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 075/2-1126 від 09.07.2026 надаємо вартість програмної продукції для моніторингу стану кіберзахищеності об'єктів кіберзахисту (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 SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year) у складі:** - Програмна продукція для забезпечення кібербезпеки Splunk Enterprise – Term License with Standard Success Plan – 250 GB/day строком на 1 рік" - 1 шт; - Програмна продукція для забезпечення кібербезпеки Splunk Enterprise Security – Term License with Standard Success Plan – 250 GB/day строком на 1 рік" - 1 шт.	1	комплект	10 250 000,00	10 250 000,00
2	**Послуга, пов'язана з постачанням ПП (встановлення та налаштування)**	1	послуга	2 083 330,00	2 083 330,00
				Всього грн, без ПДВ	12 333 330,00
				Податок на додану вартість (20%), грн	2 466 666,00
				Загальна сума грн, з ПДВ	14 799 996,00

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

Комерційний Директор Комар Олександр

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/560
Від 20.07 2026 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№ 071626/1 від 16.07.2026
На № 075/2-1127 від 09.07.2026

СКП «Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію, у відповідь на Ваш запит щодо вартості програмної продукції для моніторингу стану кіберзахищеності об'єктів кіберзахисту.

№ з/п	Найменування	Од. виміру	Кількість	Вартість з ПДВ, грн	Загальна вартість, грн., з ПДВ
1	Програмна продукція SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year)	К-т	1	12 492 000,00	12 492 000,00
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування).	Послуга	1	2 808 000,00	2 808 000,00
Разом з ПДВ, грн:		**15 300 000,00**			
ПДВ, грн:		**2 550 000,00**			

Всього: 15 300 000,00 грн. (П'ятнадцять мільйонів триста тисяч грн. 00 коп.)

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/559
Від 20.07 2026 р.

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

ТОВ «СІЕС КОНСАЛТИНГ»
Код ЄДРПОУ 42953721
03067, Україна, м.Київ,
вул. Олекси Тихого, 42А
Тел.: +380 67 448 30 57
info@cs-consulting.com.ua

Вих.№26-0720-01 від 20 липня 2026 року

Спеціалізоване комунальне підприємство «Київтелесервіс»

(СКП «Київтелесервіс»)

Комерційна пропозиція

щодо постачання програмної продукції SPLUNK та послуг встановлення та налаштування

№ п/п	Найменування товару	Кількість	Одиниці виміру	Ціна без ПДВ, гривня	Вартість без ПДВ, гривня
1	Комплект програмної продукції у складі: - Програмна продукція SPLUNK Enterprise 250GB/day (1 Year) - Програмна продукція SPLUNK Enterprise Security 250GB/day (1 Year)	1	комплект	10 339 166,67	10 339 166,67
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування)	1	послуга	2 140 000,00	2 140 000,00
				Всього, грн	12 479 166,67
				ПДВ, грн	2 495 833,33
				Разом з ПДВ, грн	14 975 000,00

Директор

Шулевський Ю. О.

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/564
Від 20.07 2026 р.