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

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

С Л У Ж Б О В А З А П И С К А

місто Київ «01» вересня 2025 року

Конкретна назва предмета закупівлі – **Програмна продукція для 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 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 ефективного моніторингу стану кіберзахищеності міських сервісів, необхідно придбати програмну продукцію для моніторингу стану кіберзахищеності об'єктів кіберзахисту Splunk (далі-ПП).

Обґрунтування необхідності посилання на конкретні марку та виробника:

Посилання на ПП Splunk обумовлено його поточним використанням для моніторингу стану кіберзахищеності міських сервісів Центром моніторингу та кібербезпеки міських сервісів та Наказом №76 від 29.08.2023р. Спеціалізованого комунального підприємства "Київтелесервіс" "Про введення у виробничу експлуатацію підсистем моніторингу та кібербезпеки".

Обґрунтування обсягів закупівлі:

Об'єм ліцензії обумовлено поточною кількістю подій ІКС які потребують аналізу на предмет ідентифікації кіберзагроз та кіберінцидентів.

Обґрунтування якісних характеристик закупівлі:

Технічні вимоги до предмета закупівлі рекомендовані протоколом №87 від 27.08.2025 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 15 232 480,00 (п'ятнадцять мільйонів двісті тридцять дві тисячі чотириста вісімдесят 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 комплект, 1 супутня послуга.

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 4 арк.
4. Додаток 4. Протокол №87 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

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 у відпустці _____ **Ю.В. Волочаєва**

Додаток 1

ТЕХНІЧНІ ВИМОГИ
Програмна продукція для моніторингу стану кіберзахищеності об'єктів кіберзахисту (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 (далі – ІКС 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».
- Рішення Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257) Про затвердження Комплексної міської цільової програми "Цифровий Київ" на 2024-2027 роки.

  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 ліцензійного програмного забезпечення, перелік якого наведено у Таблиці 1, його встановлення та налаштування у складі ІКС моніторингу та кібербезпеки, що забезпечить цілодобовий моніторинг стану кіберзахищенності 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.

2.2. Цілі інформатизації

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.

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

4.1.1 Склад закупівлі:

- **Програмна продукція SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year) (Далі – ПП, засіб інформатизації) - 1 комплект** *(склад комплекту наведено у таблиці 1)*

Таблиця 1. Склад комплекту

№ з/п	Найменування	Обсяг оброблюваних. даних, охоплений ліцензією	Кіл.
1	Програмна продукція SPLUNK Enterprise (1 Year)	250GB/day	1
2	Програмна продукція SPLUNK Enterprise Security (1 Year)	250GB/day	1

- **Послуга, пов'язана зі встановленням та налаштуванням програмної продукції**.

4.1.2 Вимоги до функціональних можливостей засобу інформатизації (програмної продукції):

Таблиця 3

№	Характеристика	Вимога
1.	**Загальні вимоги**	*Загальні вимоги до Програмної продукції (далі - ПП):* ✓ ПП повинна мати модульну архітектуру; ✓ ПП повинна збирати, обробляти та зберігати події; ✓ ПП повинна встановлюватись на обчислювальні потужності наземної інфраструктури; *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 зберігати події (данні з логів) в неструктурованому вигляді без змін, та без використання класичних реляційних баз даних (no sql). ✓ ПП повинна мати аналітичну мову запитів. ✓ ПП повинна мати відкритий API для можливості інтеграції з іншими системами як для отримання данних та і для їх експорту. ✓ ПП повинна надавати доступ до інцидентів засобами API. ✓ ПП повинна мати інтеграцію з сканером вразливостей Tenable для автоматизації реєстрація вразливостей та автоматичного запуску сценарію сканування *Вимоги до збору подій* ✓ Компонент збору подій може виконувати збір подій віддалено з джерел подій, за допомогою установки програмного забезпечення (ПЗ) безпосередньо на джерело подій (з джерел, на які можливо встановити необхідне ПЗ). ✓ 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: o збір подій по протоколу Syslog; o 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) o збір подій з журналів операційної системи (ОС) Linux; o збір подій з баз даних з використанням SQL-запитів; o збір подій з текстових файлів; o збір подій з XML-файлів; o збір подій по протоколу NetFlow; o збір подій по протоколу jFlow; o збір подій по протоколу sFlow; o збір подій по протоколу IPFIX o збір подій по протоколу HTTP; o збір подій по протоколу IMAP; o збір подій по протоколу POP3; o збір подій по протоколу XMPP; o збір подій мережевого трафіку; o можливість локально завантажити файли формату CSV, TXT; o збір подій по протоколу http/https; o можливість збору подій через REST API; o можливість збору по протоколам IoT такими як: MQTT, JMS, KAFKA. o Можливість централізованого віддаленого виконання скриптів та індексація результатів їх роботи

		✓ Компонент збору подій повинен мати функціональну можливість збору подій з наступних систем та обладнання: o Files and directories o Network events o Windows sources o Linux sources o HTTP Event Collector (HEC) o Metrics (OT) o Data Base (SQL, MY SQL, Oracle, Prostgress) o 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): o можливість збирати дані з пропрієтарних систем, при умові, що системи мають можливість передавати дані за допомогою озвучених вище протоколів; o 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 в 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. ✓ Система 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: o online - період часу, протягом якого події повинні бути доступні для проведення моніторингу, аналізу, розслідування; o offline - період часу, наступний після закінчення online-періоду, коли події архівуються і перестають бути доступними для проведення моніторингу, аналізу, розслідування. ✓ Система 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 в кількох дата-центрах і автоматичного синхронізації даних в разі втрати зв'язку між майданчиками. *Вимоги до ліцензування системи* ✓ Має бути забезпечена можливість обробки даних подій об'ємом не менше 250 гігабайт/день без втрати продуктивності системи ✓ При перевищенні об'єму система повинна продовжувати збір даних без будь-якої їх втрати. ✓ Не менше 14 користувачів, строк дій комплекту програмної продукції системи моніторингу подій кібербезпеки не менше 1-го року. ✓ Постачальник надає ключ активації та ліцензію в електронному вигляді Замовнику не пізніше 5 днів після укладення договору відповідне оформлення ліцензійності, яке повинно однозначно ідентифікувати визначене програмне забезпечення.
2.	**Вимоги функціональних можливостей**	✓ ПП повинна забезпечувати такі основні задачі: o управління інцидентами - всі інциденти кібербезпеки повинні управлятися з єдиного порталу, який дозволяє команді спеціалістів Центру моніторингу та кібербезпеки міських сервісів отримати доступ до оновлень та інформації щодо інцидентів кібербезпеки на основі назначеної ролі користувача; o автоматизація управлінням безпеки - автоматизація повинна надавати змогу команді Центру моніторингу та кібербезпеки міських сервісів 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. *Вимоги до процесу управління інцидентами* ✓ ПП управління інцидентами повинна надавати можливість керувати конфіденційними даними відповідно до політики організації завдяки механізму надійного контролю доступу на основі ролей та підтримувати наступні можливості: o Створення власних ролей та ієрархій команд o Можливість визначення дозволу з різними ролями o Керувати відображенням і шифруванням даних з кількома рольовими переглядами o Налаштовувати власні варіанти відображення даних та макети сторінок за допомогою перетягування або візуального дизайнера. o Підтримка сценаріїв автоматизації процесу управління інцидентів шляхом автоматичного доповнення інформацією щодо наявного інциденту, присвоєння статусу критичності інциденту, сповіщення спеціаліста про зміни в інциденті, тощо. o Автоматична та ручна ескалація подій до системи оркестрації, автоматизації та реагування на кіберінциденти

Активація Програмної продукції - автоматично в день підписання Сторонами акту передачі-приймання Програмної продукції та подальшим її терміном дії протягом 12 місяців.

Встановлення (інсталяція) програмної продукції здійснюється Постачальником

4.1.3 Вимоги до послуги **з-встановлення та налаштування ПП**

№ з/п	Вимоги
1	Проведення аудиту поточного стану ПП Splunk Enterprise & Splunk Enterprise Security з урахуванням всіх модулів та їх конфігурацій на предмет конфліктуючих та не ефективних правил, політик, конфігурацій. Результати проведеного аудиту мають бути оформлені звітом з наступними розділами : 1. Загальний відомості ПП; 2. Технічні характеристики та мережеві налаштування ПП; 3. Результати аналізу (недоліки, помилки, перенавантаження складових ПП, застарілі версії компонентів ПП та інш); 4. Рекомендації щодо покращення функціонування ПП.
2	Розробка та впровадження сценаріїв (Use Cases) для покращення рівня реагування на інциденти. Не менше ніж 15 сценаріїв. Кожен сценарій повинен: 1. Ідентифікувати нові кіберзагрози (по відношенню до існуючих Use Cases); 2. Описувати повний сценарій дій аналітика з етапу ідентифікації кіберзагрози до етапу локалізації; 3. Дозволяти симулювати коректність ідентифікації кібезагроз в існуючий інфраструктурі Замовника;
3	Розробка та впровадження інформаційних панелей (Dashboards). Не менше ніж 5 панелей. Кожна панель має

	1. Бути побудовані за допомогою функціональних можливостей ПП без використання іншого програмного забезпечення; 2. Оновлюватись в режимі реального часу з можливостю корегування часу оновлення; 3. Мати графічні елементи візуалізації та стислі описи основних показників; 4. Відображати джерела подій для візуалізації; 5. Мати фільтри для управління періодом, джерелом, ідентифікатором подій 6. Контролювати безперевність надходження подій для візуалізації.
4	Побудова відмовостійкого кластеру для сталої та безперебійної роботи ПП (High-Availability cluster)повинна забезпечити: 1. Розгортання повністю ідентичної версії всіх складових поточного ПП; 2. Налаштування окремих віртуальніх машин кластеру ПП; 3. Налаштування мережевих зв'язків між вузлами кластеру ПП; 4. Налаштування режиму функціонування вузлів кластеру ПП Active-Passive: 5. Тестування відмостійкості кластеру ПП з симуляцією відключення одного з вузлів.

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

- Не застосовуються

4.3. Вимоги до безпеки

- ПП повинна мати власний механізм авторизації користувачів
- ПП повинна мати можливість інтеграції із зовнішніми системами або хмарними сервісами для забезпечення другого фактора автентифікації (MFA)
- ПП повинна підтримувати інтеграцію з Forti Authentificator за допомогою протоколу SAML
- ПП повинна мати внутрішню ролеву модель розподілу прав доступу та щонайменше наступні ролі - адміністратор безпеки, аналітик безпеки.
- ПП повинна мати механізм захисту цілісності журналів подій за допомогою ХЕШ сум та дозволяти здійснювати контрольне порівняння за запитом.
- ПП повинна мати діючий експертний висновок Державної служби спеціального зв'язку та захисту інформації України на програмне забезпечення

4.4. Вимоги до ергономіки та технічної естетики

ПП для управління інцидентами повинна надавати декілька варіантів ефективного керування даними:

- керування списками інцидентів та сповіщеннями щодо безпеки у вигляді сітки з можливістю фільтрації.
- візуальний редактор макетів для формування користувацьких відображень, моделей даних, полів і сіток.
- дані повинні відображатися у формі зручній для проведення розслідувань.

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

- Не застосовуються

4.9. Вимоги до режимів функціонування засобу інформатизації

- 24/7

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

- Визначено у таблиці 2.

5. Вимоги до розробки та передачі послуг

5.1. Вимоги до розробки ПП

- Відсутні

5.2. Вимоги до передачі

- Приймання примірників ПП, послуг зі встановлення та налаштування ПП здійснюється уповноваженими особами Виконавця та Замовника на підставі Акту приймання-передачі.
- Виконавець забезпечує відображення примірників ПП у кабінеті Замовника на порталі виробника.

5.3. Вимоги до гарантійної підтримки

- Отримання всіх необхідних актуальних оновлень.
- Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів в актуальному стані відповідно до рекомендацій Виробника.
- 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 (24х7) 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.*

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 № 87

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 «27» серпня 2025 року

ПРИСУТНІ:

Члени робочої групи:
А. Жежера
М. Клюєва
С. Осіпов
О. Поліщук
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:

доопрацьований 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) у частині уточнень у пункті 4.1.3 документа.

2. Різне.

По питанню 1

СЛУХАЛИ:

О. Поліщука, який поінформував про необхідність закупівлі програмної продукції для моніторингу стану кіберзахищеності об'єктів кіберзахисту SPLUNK Enterprise та SPLUNK Enterprise Security з послугою, пов'язаною із встановленням та налаштуванням програмної продукції, та представив доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для моніторингу стану кіберзахищеності

об'єктів кіберзахисту» (пункт 6.5 переліку завдань і заходів Програми) у частині уточнень у пункті 4.1.3 документа.

В обговоренні проєкту технічних вимог брали участь: Д. Цвігун, М. Клюєва.

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 доопрацьований 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 075-1941
Дата реєстрації 27.08.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 27.08.2025 (Протокол № 87 від 27.05.2025)

Кількість файлів: 2
Кількість ЕП: 12

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
27.08.2025 № 075-1941

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Поліщук Олег Федорович **Кількість ЕП:** 2	27.08.2025 19:31:09 ; 27.08.2025 19:31:10 ;	27.08.2025 19:31:10 Погодив;	27.08.2025 19:31:10 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 2	27.08.2025 17:35:54 ; 27.08.2025 17:35:56 ;	27.08.2025 17:35:56 Погодив;	27.08.2025 17:35:56 Погодив
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 2	27.08.2025 16:39:06 ; 27.08.2025 16:39:07 ;	27.08.2025 16:39:07 Погодив;	27.08.2025 16:39:07 Погодив
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 2	27.08.2025 14:49:58 ; 27.08.2025 14:49:59 ;	27.08.2025 14:50:00 Погодив;	27.08.2025 14:49:59
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 2	27.08.2025 14:45:22 ; 27.08.2025 14:45:23 ;	27.08.2025 14:45:24 Погодив;	27.08.2025 14:45:23

Самойленко Тамара Анатоліївна **Кількість ЕП:** 2	27.08.2025 14:19:13 ; 27.08.2025 14:19:14 ;	27.08.2025 14:19:14 Погодив;	27.08.2025 14:19:14 Погодив

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

Вих.№ 157 від 29.08.2025

КП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 325-2025 від 26.08.2025 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	**Комплект програмного забезпечення системи моніторингу подій кібербезпеки 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	9 302 500,00	9 302 500,00
2	**Послуги у сфері інформаційних технологій з монтажу, встановлення, технічного оснащення і налаштування програмної продукції у складі:** - Проведення аудиту поточного стану Системи з урахуванням всіх модулів та їх конфігурацій на предмет конфліктуючих та не ефективних правил, політик, конфігурацій; - Розробка та впровадження сценаріїв (Use Cases) для покращення рівня реагування на інциденти (15 штук) - Розробка та впровадження інформаційних панелей (Dashboards) (5 штук) - Побудова відмовостійкого кластеру	1	послуга	3 110 700,00	3 110 700,00
				Всього грн, без ПДВ	**12 413 200,00**
				Податок на додану вартість (20%), грн	2 482 640,00
				Загальна сума грн, з ПДВ	**14 895 840,00**

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 № 239/2025
Від 29.08 2025 р.

CYBERPRO
AUDIT AND PROTECTION

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

Вих.2025-8-29/1
від 29 серпня 2025 року

СКП «КИЇВТЕЛЕСЕРВІС»

ЦІНОВА ПРОПОЗИЦІЯ

№ з/п	Найменування товару/послуги	Од. виміру	Кіль-кість	Ціна, грн без ПДВ	Сума, грн без ПДВ
1	Програмна продукція SPLUNK Enterprise (1 Year) та SPLUNK Enterprise Security (1 Year)	комплект	1	9 600 000,00	9 600 000,00
2	Послуга з встановлення та налаштування програмної продукції: проведення аудиту поточного стану ПП Splunk Enterprise & Splunk Enterprise Security з урахуванням всіх модулів та їх конфігурацій на предмет конфліктуючих та не ефективних правил, політик, конфігурацій; розробка та впровадження сценаріїв (Use Cases) для покращення рівня реагування на інциденти - 15 сценаріїв; розробка та впровадження інформаційних панелей (Dashboards) - 5 панелей; побудова відмовостійкого кластеру для сталої та безперебійної роботи ПП (High Availability cluster)	послуга	1	3 200 000,00	3 200 000,00
				Разом, грн без ПДВ:	**12 800 000,00**
				ПДВ, 20%	**2 560 000,00**
				ВСЬОГО, грн з ПДВ:	**15 360 000,00**

Загальна сума пропозиції, в грн з урахуванням ПДВ: 15 360 000,00 грн
(п'ятнадцять мільйонів триста шістдесят тисяч грн. 00 коп.)

Директор
ТОВ «САЙБЕРПРО» **Сергій ДІДУР**

«САЙБЕРПРО»

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 241/2025
Від 29.08. 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№ 082925/1 від 29.08.2025
На № 323-2025 від 26.08.2025

Спеціалізованому комунальному підприємству «Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію щодо постачання програмної продукції SPLUNK та послуг встановлення та налаштування.

№	Найменування товару	К-ть	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	9 020 000,00	9 020 000,00
2	Послуги з встановлення та налаштування програмної продукції (ПП) у складі: - Проведення аудиту поточного стану ПП з урахуванням всіх модулів та їх конфігурацій на предмет конфліктуючих та не ефективних правил, політик, конфігурацій - Розробка та впровадження сценаріїв (Use Cases) для покращення рівня реагування на інциденти. - 15 сценаріїв - Розробка та впровадження інформаційних панелей (Dashboards). - 5 панелей	1	послуга	3 848 000,00	3 848 000,00

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 240/3025
Від 29.08 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

	- Побудова відмовостійкого кластеру для сталої та безперебійної роботи ПП				
			Всього, грн	12 868 000,00	
			ПДВ, грн	2 573 600,00	
			Разом з ПДВ, грн	**15 441 600,00**	

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

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