

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

Начальника Центру моніторингу та  
кібербезпеки міських сервісів  
Журбенко Максима  
Анатолійовича

## С Л У Ж Б О В А   З А П И С К А

місто Київ

«15» травня 2024 року

Конкретна назва предмета закупівлі – **Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахищеності міських сервісів (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).**

### 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 і заходів Програми, Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557.

З метою забезпечення ефективного моніторингу стану кіберзахищеності міських сервісів, необхідно придбати комплект ліцензійного програмного забезпечення Splunk (далі-ПЗ) або еквівалент з такими ж показниками.

Обґрунтування необхідності посилання на конкретні марку та виробника: Придбання ПЗ Splunk обумовлено його поточним використанням для моніторингу стану кібербезпеки 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 №31 від 19.04.2024 засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки.

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 11 052 000,00 (одинадцять мільйонів п'ятдесят дві тисячі гривень нуль копійок) з ПДВ, що є мінімальним значенням отриманих комерційних пропозицій. Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення.

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

Вид предмету закупівлі – товар.

Кількість – 1 комплект.

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)).**

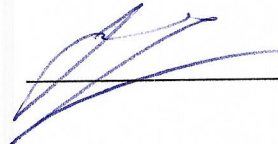
Зазначення точної адреси місця поставки товару несе загрозу безпеці замовника.

Строк поставки товарів – до 30.06.2024.

#### Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 7 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.
4. Додаток 4. Протокол №31 засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки на 5 арк

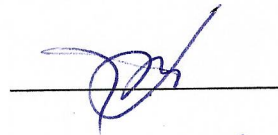
Ініціатор закупівлі



М.А. Журбенко

«ПОГОДЖЕНО»:

Начальник загально-правового відділу



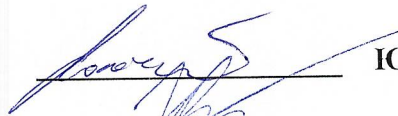
В. В. Тихонов

Начальник відділу - головний бухгалтер



Г. А. Букша

Заступник начальника відділу  
з економічних питань



Ю.В. Волочаєва

Заступник директора з  
питань кібербезпеки



О.О. Волощук



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

**Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).**

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 і заходів Програми, Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557.

З метою забезпечення ефективного моніторингу стану кіберзахисності міських сервісів, необхідно придбати комплект ліцензійного програмного забезпечення Splunk (далі-ПЗ) або еквівалент з такими ж показниками.

Обґрунтування необхідності посилання на конкретні марку та виробника: Придбання ПЗ Splunk обумовлено його поточним використанням для моніторингу стану кібербезпеки 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».

### **Загальні вимоги**

З метою забезпечення функції моніторингу та кібербезпеки міських сервісів Центром моніторингу та кібербезпеки міських сервісів необхідно забезпечити придбання комплекту ліцензійного програмного забезпечення підсистеми моніторингу та контролю кібербезпеки.

**Комплект ліцензійного програмного забезпечення системи моніторингу подій кібербезпеки (ліцензійне програмне забезпечення) - 1 комплект**

Склад комплекту ліцензійного програмного забезпечення:	
Найменування	Об'єм ліцензування
Ліцензійне програмне забезпечення Splunk Enterprise	Term License with Standard Success Plan - 250GB/day строком на 1 рік
Ліцензійне програмне забезпечення Splunk Enterprise Security	Term License with Standard Success Plan - 250GB/day строком на 1 рік

№	Характеристика	Вимога
1.	<b>Вимоги до системи</b>	<i>Загальні вимоги до системи:</i> ✓ Система повина мати модульну архітектуру;

- ✓ Система повинна збирати, обробляти та зберігати події;
- ✓ Система повинна встановлюватись на обчислювальні потужності наземної інфраструктури;

*Вимоги до безпеки системи:*

- ✓ Система повинна мати власний механізм авторизації користувачів
- ✓ Система повинна мати можливість інтеграції зовнішніми системами або хмарними сервісами для забезпечення другого фактора автентифікації (MFA)
- ✓ Система повинна підтримувати інтеграцію з Forti Authenticator за допомогою протоколу SAML
- ✓ Система повинна мати внутрішню ролеву модель розподілу прав доступу та що найменше наступні ролі - *адміністратор безпеки, аналітик безпеки.*
- ✓ Система повинна мати механізм захисту цілостності журналів подій за допомогою XEIP сумм та дозволити здійснювати контрольне порівняння за запитом
- ✓ Система повинна мати діючий експертний висновок Державної служби спеціального зв'язку та захисту інформації України на програмне забезпечення

*Вимоги до роботи системи*

- ✓ Система повинна мати можливість підключення модуля збору подій щодо інформаційної безпеки.
- ✓ Система повинна мати можливість підключення модуля машинного навчання.
- ✓ Система повинна мати можливість підключення модуля моніторингу ІТ інфраструктури.
- ✓ Система повинна мати можливість управління ресурсами для моніторингу та аналізу подій і настройками компонентів Системи.
- ✓ Система повинна забезпечувати можливість створення власних додатків для вирішення задач бізнес-аналітики, кібербезпеки, IoT.
- ✓ Система повинна зберігати події (данні з логів) в неструктурованому вигляді без змін, та без використання класичних реляційних баз даних (no sql).
- ✓ Система повинна мати аналітичну мову запитів.
- ✓ Система повинна мати відкритий API для можливості інтеграції з іншими системами як для отримання даних та і для їх експорту.
- ✓ Система повинна надавати доступ до інцидентів засобами API.



- ✓ Система повинна мати інтеграцію з сканером вразливостей Tenable для автоматизації реєстрація вразливостей та автоматичного запуску сценарія 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:
  - ✓ 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 HTTP;
  - ✓ збір подій по протоколу IMAP;
  - ✓ збір подій по протоколу POP3;
  - ✓ 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)
- ✓ Data Base (SQL, MY SQL, Oracle, Prostagress)
- ✓ 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 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:
  - ✓ 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.
- ✓ 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 датацентрах і автоматичного синхронізації даних в разі втрати зв'язку між майданчиками.

#### *Складові сервісної підтримки*

- ✓ Отримання актуальних всіх необхідних оновлень.
- ✓ Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у 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).

		<ul style="list-style-type: none"> <li>✓ Постійний (24x7) авторизований доступ до сайту виробника.</li> </ul> <p><i>Вимоги до ліцензування системи</i></p> <ul style="list-style-type: none"> <li>✓ Має бути забезпечена можливість обробки даних подій об'ємом не менше 250 гігабайт/день без врати продуктивності системи</li> <li>✓ При перевищенні об'єму система повинна продовжувати збір даних без будь-якої їх врати.</li> <li>✓ Не менше 14 користувачів, строк дій комплекту програмної продукції системи моніторингу подій кібербезпеки не менше 1-го року.</li> <li>✓ Постачальник надає ключ активації в електронному вигляді Замовнику не пізніше 5 днів після отримання коштів на рахунок Постачальника</li> </ul>
2.	<p><b>Вимоги по налаштуванню системи</b></p>	<p><b>Вимоги по налаштуванню системи</b></p> <p><i>Загальні вимоги</i></p> <ul style="list-style-type: none"> <li>✓ Платформа повинна забезпечувати такі основні задачі:</li> <li>✓ 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;</li> <li>✓ 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.</li> </ul> <p><i>Вимоги до інтерфейсу</i></p> <ul style="list-style-type: none"> <li>✓ Інтуїтивно зрозумілий інтерфейс.</li> <li>✓ Система повинна мати механізм розслідування інцидентів.</li> <li>✓ Платформа для управління інцидентами повинна надавати декілька варіантів ефективного керування даними:</li> <li>✓ Керування списками інцидентів та сповіщеннями щодо безпеки у вигляді сітки з можливістю фільтрації.</li> <li>✓ Візуальний редактор макетів для формування користувацьких відображень, моделей даних, полів і сіток. Інтуїтивно зрозумілий інтерфейс.</li> <li>✓ Дані повинні відображатися у формі зручній для проведення розслідувань.</li> </ul> <p><i>Вимоги до процесу управління інцидентами</i></p>



		<ul style="list-style-type: none"> <li>✓ Платформа управління інцидентами повинна надавати можливість керувати конфіденційними даними відповідно до політики організації завдяки механізму надійного контролю доступу на основі ролей та підтримувати наступні можливості:</li> <li>✓ Створення власних ролей та ієрархій команд</li> <li>✓ Можливість визначення дозволу з різними ролями</li> <li>✓ Керувати відображенням і шифруванням даних з кількома рольовими переглядами</li> <li>✓ Налаштовувати власні варіанти відображення даних та макети сторінок за допомогою перетягування або візуального дизайнера.</li> <li>✓ Підтримка сценаріїв автоматизації процесу управління інцидентів шляхом автоматичного доповнення інформацією щодо наявного інциденту, присвоєння статусу критичності інциденту, сповіщення спеціаліста про зміни в інциденті, тощо.</li> <li>✓ Автоматична та ручна ескалація подій до системи оркестрації, автоматизації та реагування на кіберінциденти</li> </ul>
--	--	---

#### **Вимоги до учасників:**

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 ліцензійного програмного забезпечення та терміну його дії, що пропонується учасником.

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


## Додаток 2

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

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)	<p>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.</p> <p>На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії: виконаного договору, видаткової (видаткових) накладної (накладних) або акту (ів), листа-відгука, що підтверджують його виконання.</p> <p><i>* 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.</i></p>
2.	Інформація про технічні, якісні та кількісні характеристики предмета закупівлі	<p>Для підтвердження відповідності тендерної пропозиції технічним, якісним та кількісним характеристикам (вимогам) замовника Учасник у складі тендерної пропозиції повинен надати:</p> <p>Для підтвердження відповідності тендерної пропозиції технічним, якісним та кількісним характеристикам (вимогам) замовника Учасник у складі тендерної пропозиції повинен надати:</p> <p>1) порівняльну таблицю із зазначенням найменування, виробника та технічних характеристик запропонованого учасником товару для підтвердження відповідності вимогам замовника;</p> <p>2) авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника, дистриб'ютора в Україні, який підтверджує наявність у Учасника статусу партнера та права на здійснення продажу запропонованого Учасником товару, виданий на адресу Замовника із посиланням на процедуру закупівлі.</p>

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



М.А. Журбенко



Спеціалізоване комунальне підприємство  
"Київтелесервіс"  
вул. Хрещатик 10, м. Київ, 01001

**КОМЕРЦІЙНА ПРОПОЗИЦІЯ**  
від 25 квітня 2024 року

**ТОВ «САЙБЕРПРО»** добирає та поставляє оптимальні програмні та програмно-апаратні рішення для захисту інформаційних активів.

На Ваш запит №126-2024 від 24.04.2024 надаємо інформацію щодо вартості пакетів програмного забезпечення операційного центру кібербезпеки відповідно до технічних вимог, отриманих разом із запитом.

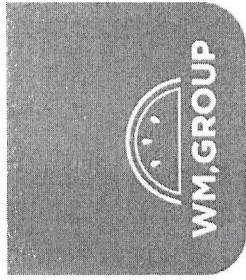
№	Найменування	Кіл-ть	Ціна, грн, з ПДВ	Сума, грн, з ПДВ
1	Комплект ліцензійного програмного забезпечення системи моніторингу подій кібербезпеки (ліцензійне програмне забезпечення) у складі: - Ліцензійне програмне забезпечення Splunk Enterprise Security-Term License with Standard Success Plan - 250GB/day строком на 1 рік – 1 шт. - Ліцензійне програмне забезпечення Splunk Enterprise -Term License with Standard Success Plan - 250GB/day строком на 1 рік – 1 шт.	1 компл	11 064 000,00	11 064 000,00
<b>Разом, грн з ПДВ</b>				<b>11 064 000,00</b>

Строк поставки 7-14 днів.

З повагою

Директор  
ТОВ «САЙБЕРПРО»

Сергій ДІДУР



ТОВ «ВІ ЄМ ДЖІ»

ЄДРПОУ 40844268

+380 96 001 01 61

info@wmggroup.com.ua

wmggroup.com.ua

Вих.№ 45 від 25.04.2024

## Комерційна пропозиція для СКП «КИЇВТЕЛЕСЕРВІС»

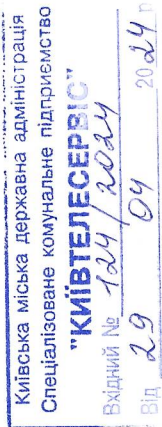
Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).

У відповідності до запиту від 24.04.2024 № 127-2024 надаємо комерційну пропозицію щодо вартості комплекту пакетів програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів

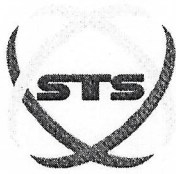
№	Найменування товару	Кіл-ть	Од. вимір	Ціна, грн без ПДВ	Сума, грн без ПДВ
	Комплект ліцензійного програмного забезпечення системи моніторингу подій кібербезпеки (ліцензійне програмне забезпечення) у складі: Ліцензійне програмне забезпечення Splunk Enterprise - Term License with Standard Success Plan - 250GB/day строком на 1 рік - 1 шт.; Ліцензійне програмне забезпечення Splunk Enterprise Security- Term License with Standard Success Plan - 250GB/day строком на 1 рік - 1 шт.	1	комплект	9 210 000,00	9 210 000,00
Всього, без ПДВ					9 210 000,00
Податок на додану вартість (20%)					1 842 000,00
Загальна сума, з ПДВ					11 052 000,00

Комерційний Директор

Комар Олександр







ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "СПЕЦІАЛЬНІ  
ТЕЛЕКОМУНІКАЦІЙНІ РІШЕННЯ"

02140 Київ, вул. Єлизавети Чавдар, буд. 1 оф.9,  
тел.: 0503901809, www.st-solution.com.ua

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Пакети програмного забезпечення операційного центру кібербезпеки

(48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника)

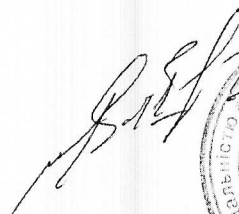

№	Опис ПП	Кількість	Ціна GPL за одиницю, USD (без ПДВ)	Ціна GPL за одиницю, грн. * (без ПДВ)	Ціна, за одиницю, грн. (без ПДВ)	Вартість, грн. (без ПДВ)
1	Комплект ліцензійного програмного забезпечення Splunk Enterprise - Term License with Standard Success Plan - 250GB/day	1	198099	7 940 996,514	7 940 996,514	7 940 996,514
	Комплект ліцензійного програмного забезпечення Splunk Enterprise Security - Term License with Standard Success Plan - 250GB/day	1	52866	2 119 186,476	2 119 186,476	2 119 186,476
Вартість ПП, грн. (без ПДВ)						10 060 182,99
ПДВ						2 012 036,598
Загальна вартість ПП, грн. (з ПДВ)						12 072 219,588

\*для розрахунку ціни взято офіційний курс долара США по відношенню до гривні плюс 2%, встановленого НБУ станом на 06.05.2024 р. Курс 40,086

З повагою,

Директор

Дата: 28.04.2024

С.С. Лівенцев

Київська міська державна адміністрація  
Спеціалізоване комунальне підприємство  
**"КІЇВТЕЛЕСЕРВІС"**  
Вхідний № 167/2024  
Від 06 05 2024 р.

Засідання в онлайн режимі  
із використанням Microsoft Teams

### **ПРОТОКОЛ № 31**

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки

м. Київ

«19» квітня 2024 року

#### **ПРИСУТНІ:**

*Члени робочої групи:*

А. Вовнюк  
М. Журбенко  
В. Жучков  
С. Осіпов  
О. Поліщук  
П. Сальніков  
М. Спичка  
Д. Цвігун

#### **ПОРЯДОК ДЕННИЙ:**

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

1.1 доопрацьований проєкт технічних вимог до закупівлі «Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів» (пункт 6.5. «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми);

1.2 доопрацьований проєкт технічних вимог до закупівлі «Придбання та налаштування програмного продукту для забезпечення розвитку програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення» (пункт 5.1. «Створення, розвиток та супровід програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення міста Києва» переліку завдань і заходів Програми);



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

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

1.5 доопрацьований проєкт технічних вимог «Придбання засобів зв'язку (обладнання, комплектуючі та супутні послуги з побудови опорної безпроводової мережі зв'язку LoRaWAN)» (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);

1.6 доопрацьований проєкт технічних вимог «Модернізація інформаційно-комунікаційної системи «Карта освітніх потреб» (пункт 7.1 «Створення, впровадження, модернізація платформ та систем автоматизації процесів управлінської діяльності (інформаційних систем управління) та великих даних» переліку завдань і заходів Програми).

1. Різне.

По підпункту 1.1 питання 1

#### **СЛУХАЛИ:**

О. Поліщука, який представив доопрацьований проєкт технічних вимог до закупівлі «Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів» (пункт 6.5. переліку завдань і заходів Програми) та доповів, що доопрацювання пов'язано з помилковим зазначенням у відповідному проєкті технічних вимог, який розглянуто на засіданні робочою групою 09.04.2024 (Протокол № 29), назви об'єму ліцензування програмного забезпечення Splunk Enterprise.

В обговоренні брали участь: А. Вовнюк, М. Журбенко.

#### **УХВАЛИЛИ:**

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівель «Пакети програмного забезпечення операційного центру кібербезпеки для моніторингу стану кіберзахисності міських сервісів (пункт 6.5 переліку завдань і заходів Програми) використовувати доопрацьований проєкт технічних вимог розглянутий на засіданні робочої групи.

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

По підпункту 1.2 питання 1



**СЛУХАЛИ:**

С. Осіпова, який наголосив про необхідність внесення змін до розглянутого на засіданні робочою групою 03.04.2024 (Протокол № 28) проекту технічних вимог «Програмний продукт для забезпечення розвитку програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення» (пункт 5.1. переліку завдань і заходів Програми) у зв'язку зі зміною предмета закупівлі та представив доопрацьований проект технічних вимог до закупівлі «Придбання та налаштування програмного продукту для забезпечення розвитку програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення» (пункт 5.1. переліку завдань і заходів Програми).

В обговоренні брали участь: А. Вовнюк, В. Жучков.

**УХВАЛИЛИ:**

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівлі «Придбання та налаштування програмного продукту для забезпечення розвитку програмно-апаратного комплексу управління та контролю мереж зовнішнього освітлення» (пункт 5.1 переліку завдань і заходів Програми) використовувати доопрацьований проект технічних вимог, розглянутий на засіданні робочої групи.

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

По підпунктам 1.3 – 1.4 питання 1

С. Осіпова, який повідомив про внесення змін до проектів технічних вимог до закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки », «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки » (пункт 2.1. переліку завдань і заходів Програми) розглянутих на засіданні робочою групою 17.04.2024 (Протокол № 30) у частині переліку обладнання та представив доопрацьовані проекти технічних вимог до закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки », «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки » (пункт 2.1. переліку завдань і заходів Програми).

В обговоренні брали участь: А. Вовнюк, М. Журбенко, В. Жучков.

**УХВАЛИЛИ:**

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедур закупівель «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки », «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки » (пункт 2.1. переліку завдань і



заходів Програми) використовувати доопрацьовані проекти технічних вимог, розглянуті на засіданні робочої групи.

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

По підпункту 1.5 питання 1

В. Жучкова, який поінформував про необхідність доопрацювання проекту технічних вимог до закупівлі «Придбання засобів зв'язку (обладнання, комплектуючі та супутні послуги з побудови опорної безпроводової мережі зв'язку LoRaWAN)», який розглянуто на засіданні робочою групою 27.02.2024 (Протокол № 20), у зв'язку з необхідністю внесення змін щодо кількості локацій надання послуг з 23 на 20, вимог до порядку контролю та приймання предмету закупівлі та представив доопрацьований проект технічних вимог «Придбання засобів зв'язку (обладнання, комплектуючі та супутні послуги з побудови опорної безпроводової мережі зв'язку LoRaWAN)» (пункт 6.2 переліку завдань і заходів Програми).

В обговоренні брали участь: А. Вовнюк, О. Поліщук.

**УХВАЛИЛИ:**

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Придбання засобів зв'язку (обладнання, комплектуючі та супутні послуги з побудови опорної безпроводової мережі зв'язку LoRaWAN)» (пункт 6.2 переліку завдань і заходів Програми) використовувати доопрацьований проект технічних вимог, розглянутий на засіданні робочої групи.

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

По підпункту 1.6 питання 1

**СЛУХАЛИ:**

Д. Цвігуна, який поінформував про необхідність доопрацювання проекту технічних вимог до закупівлі «Модернізація інформаційно-комунікаційної системи «Карта освітніх потреб», який розглянуто на засіданні робочою групою 17.04.2024 (Протокол № 30), у частині внесення змін до модернізації інформаційно-комунікаційної системи «Карта освітніх потреб» (виключення інтеграції з ЄІСУБом, розширення функціональних можливостей для людей, які мають вади зору, розширення наявної функціональності системи у частині авторизації користувачів та надання доступу до інформації про конкретну організацію) та представив доопрацьований проект технічних вимог до закупівлі «Модернізація інформаційно-комунікаційної системи «Карта освітніх потреб».

В обговоренні брали участь: А. Вовнюк, П. Сальніков.

**УХВАЛИЛИ:**

Рекомендувати комунальному підприємству «Головний інформаційно-обчислювальний центр» під час процедури закупівлі «Модернізація інформаційно-комунікаційної системи «Карта освітніх потреб»» (пункт 7.1. переліку завдань і заходів Програми) використовувати доопрацьований проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

Протокол склав

Олег ПОЛІЩУК