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

Начальника центру моніторингу та кібербезпеки міських сервісів Цвєткова Василя Костянтиновича

СЛУЖБОВА ЗАПИСКА

місто Київ «20» жовтня 2026 року

Конкретна назва предмета закупівлі – **Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки).**

Обґрунтування доцільності закупівлі:

На виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 14.05.2026 № 604/11071).

З метою забезпечення аналітиків Центру моніторингу та кібербезпеки міських сервісів (далі - Центр) сучасними засобами виявлення та аналізу кіберзагроз необхідно придбати програмну продукцію для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру (далі - ПП).

Обґрунтування необхідності посилання на конкретні марку та виробника:

Посилання на конкретне найменування ПП обумовлено її поточним використанням у складі впровадженої інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі - ІКС) Центру та Наказом спеціалізованого комунального підприємства «Київтелесервіс» від 29.08.2023 № 76 «Про введення у виробничу експлуатацію підсистем моніторингу та кібербезпеки».

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 № 101 від 07.10.2026 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 моніторингу цін шляхом направлення запитів учасникам ринку, очікувана вартість становить 10 500 500,00 (десять мільйонів п'ятсот тисяч п'ятсот гривень нуль копійок) з ПДВ, що є середнім значенням отриманих комерційних пропозицій.

Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення. Розмір бюджетного призначення визначено паспортом бюджетної програми на 2026 рік відповідно до заходів Комплексної міської цільової програми «Цифровий Київ» на 2024 – 2027 роки.

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

Вид предмету закупівлі – товар.

Кількість – 1 комплект, 1 супутня послуга.

Строк поставки – до 25.12.2026.

Місце поставки товарів – місто Київ (відповідно до абз.2 п.10 Особливостей, у разі коли ***оприлюднення в електронній системі закупівель інформації про*** місцезнаходження замовника та/або місцезнаходження (для юридичної особи)/місце проживання (для фізичної особи) постачальника (виконавця робіт, надавача послуг), та/або ***місце поставки товарів***, виконання робіт чи надання послуг (оприлюднення якої передбачено Законом та/або цими особливостями) ***несе загрозу безпеці замовника*** та/або постачальника, ***така інформація в договорі про закупівлю, який оприлюднюється в електронній системі закупівель, може зазначатися як назва населеного пункту*** місцезнаходження замовника та/або місцезнаходження (для юридичної особи)/місце проживання (для фізичної особи) постачальника (виконавця робіт, надавача послуг), та/або назва населеного пункту, ***в який здійснюється доставка товару*** (в якому виконуються роботи чи надаються послуги)).

Зазначення точної адреси місця поставки товару несе загрозу безпеці замовника.

Додатки:

1. Додаток 1. Технічні вимоги на 13 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Протокол № 101 засідання робочої групи на 3 арк.
4. Додаток 4. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.

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

«ПОГОДЖЕНО»:

Заступник директора з технічних питань _____ **О.Ф. Поліщук**

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

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

Начальник загально-правового відділу _____ **В.В. Тихонов**

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

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

Додаток 1

ТЕХНІЧНІ ВИМОГИ

Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки)

1. Загальні положення

1.1. Найменування засобу інформатизації

Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру (далі – ПП), яка є складовою інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС).

1.2. Підстава для розроблення технічних вимог

Технічні вимоги (далі – ТВ) розроблені на виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024–2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 14.05.2026 № 604/11071).

Технічні вимоги розроблено відповідно до постанови Кабінету Міністрів України (далі – КМУ) від 21.02.2025 № 205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації» (в редакції постанови КМУ від 06.08.2026 № 1009).

2. Обґрунтування потреби та результати обстеження

2.1. Опис проблеми, що потребує розв'язання

Потреба у продовженні строку дії ПП виникає 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 пошуку і виявлення вразливостей в об'єктах 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.

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

Використання зазначеної ПП дозволяє забезпечувати:

- мінімізацію впливу ризиків кібербезпеки, пов'язаних з несанкціонованими спробами експлуатації вразливостей в ОК;
- зниження часу простою ОК за рахунок запобігання кіберінцидентів;
- покращення сталої та безперервної роботи ОК;
- систематизація, узагальнення інформації та перетворення її у формат, придатний для проведення подальшого аналізу ефективності заходів із реагування на кіберінциденти та кібератаки;
- виконання процесів автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності.

2.2. Опис 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. Результати обстеження поточних 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. Категорія засобу інформатизації

Засіб інформатизації віднесено до ІІ категорії, оскільки порушення його функціонування призводить до суттєвого обмеження виконання важливого бізнес-процесу (виявлення та мінімізації впливу вразливостей на об'єктах кіберзахисту), що може спричинити негативні наслідки для стану кіберзахищеності Замовника, однак не призводить до повного припинення діяльності Замовника чи припинення надання публічних послуг ОК.

2.5. Очікуваний результат

Очікуваним результатом є продовження строку дії ПП на 1 рік, що забезпечить функціонування ІКС без перерв у захисті ОК, а також мінімізацію впливу ризиків кібербезпеки, пов'язаних з несанкціонованими спробами експлуатації вразливостей в ОК.

3. Вимоги до предмету закупівлі

3.1. Вимоги до загальної побудови та складу предмету закупівлі

Склад закупівлі:

- **Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру – 1 комплект** (*склад комплекту наведено у Таблиці 1*);
- **Послуга, пов'язана з постачанням ПП (встановлення та налаштування).**

Таблиця 1. Склад комплекту

№ з/п	Найменування*	Назва характеристики	Показник не менше / не гірше	Строк дії (міс.)
1	Програмна продукція Tenable Security Center	IP Bands	2000	12
2	Програмна продукція Tenable Web App Scanning	Web Apps (FQDN)	212	12
3	Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+)	IP Bands	250	12

Активація програмної продукції, що входить до складу комплекту (Таблиця 1), здійснюється датою наступною від закінчення терміну дії попередньої ліцензії, але не пізніше 25 грудня 2026 року.

Загальні вимоги до архітектури та складу:

- якщо запропоноване рішення потребує додаткових пристроїв/систем або ліцензій, то усе це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки;
- всі необхідні ліцензії для забезпечення зазначеного функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення;
- на ПП не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника;
- ліцензія має дозволяти сканувати активи на наявність вразливостей у кількості не менше 2000 IP-адрес;
- ПП повинна поставлятися від одного виробника у вигляді готового рішення, що не потребує окремого придбання та встановлення замовником стороннього системного або прикладного ПЗ (ОС, застосунків, СКБД тощо) для впровадження;
- центральна консоль, активні та пасивні сканери ПП мають встановлюватись локально та функціонувати без обов'язкового підключення до мережі інтернет. Для компонентів, які за архітектурою виробника потребують хмарних сервісів (керування агентами, хмарний сканер веб-додатків, хмарні сканери зовнішнього сканування), підключення до хмарної інфраструктури виробника допускається в обсязі, необхідному для їх функціонування;
- ПП повинна мати центральну консоль для всіх компонентів, що розгортається локально, для збору, управління й аналізу інформації про вразливості без відправлення в хмару;
- ПП повинна дозволяти локально встановлювати активні сканери, агенти на кінцевих точках та пасивні сканери, підключаючи їх до центральної консолі;
- ПП повинна централізувати й повністю автоматизувати щоденне оновлення бази вразливостей від постачальника, з підтримкою автономного оновлення без доступу до інтернету;
- ПП повинна забезпечувати інтегровану модель зберігання даних, незалежну від стороннього продукту БД;

- ПП повинна мати комплексний, відкритий REST API для автоматичного створення сценаріїв сканування й експорту даних без додаткових витрат.

Загальні вимоги до взаємодії компонентів:

- агент повинен збирати та відправляти дані на центральну консоль для зменшення навантаження на мережу та кінцевий пристрій;
- агенти можуть бути підключені та управлятися як через локальну консоль, так і хмарну;
- агент повинен мати можливість встановлюватися у хмарних середовищах, таких як AWS та Microsoft Azure;
- агент повинен надавати можливість регулювати власне навантаження на кінцеву точку, для запобігання порушення робочих процесів;
- агент повинен мати можливість з'єднуватись з консоллю через проксі сервер;
- агент повинен мати можливість встановлюватись через сторонні рішення такі як Active Directory або Microsoft Configuration Manager (SCCM);
- ПП повинна мати можливість створювати групи агентів для автоматизації процесу виявлення вразливостей;
- ПП повинна надавати інформацію відносно статусу агентів;
- агент повинен мати унікальний ідентифікатор для виявлення одного і того пристрою в різних підмережах.

3.2. Вимоги до функцій предмету закупівлі

ПП повинна забезпечувати виконання таких функцій:

Вимоги до виявлення активів:

- ПП повинна підтримувати можливість виявлення активів, що не використовують ліцензію;
- ПП повинна забезпечувати активне сканування і пасивний моніторинг мережі для виявлення активів;
- ПП повинна вміти виявляти мобільні пристрої;
- ПП не повинна покладатися на сторонні сканери для виявлення активів, сканування портів або ідентифікації ОС;
- ПП не повинна покладатися на сторонні сканери для сканування вразливостей;
- ПП повинна забезпечувати виявлення веб-служб і служб баз даних;
- ПП повинна вміти виявляти служби на нестандартних портах та служби без банерів підключення;
- ПП повинна бути здатна тестувати кілька примірників однієї й тієї ж служби на різних портах;
- ПП повинна вміти сканувати «мертві» кінцеві точки (що не відповідають на ICMP);
- ПП повинна підтримувати необов'язкове використання netstat для перерахування відкритих портів при наданні облікових даних;
- ПП повинна підтримувати SMB і WMI для сканування систем Windows, з автоматичним запуском/зупинкою служби віддаленого реєстру;
- ПП повинна підтримувати безпечне з'єднання (SSH) з підвищенням привілеїв для сканування вразливостей і аудиту конфігурації Unix;
- ПП повинна мати можливість збирати/імпортувати й відображати дані про активи IT та OT мереж в єдиній консолі;
- ПП повинна забезпечувати виявлення точок бездротового доступу (WAP) активним і пасивним скануванням;
- ПП повинна виявляти нові пристрої та надсилати попередження email/syslog/консоллю, з можливістю автозапуску сканування нових пристроїв;
- ПП повинна підтримувати використання агента для аудиту SCAP;

- ПП повинна мати можливість виявляти всі активи, не використовуючи ліцензії, а потім мати можливість вибирати, які активи сканувати на вразливості.

Вимоги до керування життєвим циклом вразливостей:

- ПП повинна забезпечувати повну автоматизацію сканування, створення звітів і попереджень;
- ПП повинна мати окремі панелі для відображення вразливостей виявлених активно, скануванням на відповідність і в мобільних пристроях;
- ПП повинна об'єднувати результати окремих сканувань вразливостей з можливістю фільтрації, щоб забезпечити можливість деталізації та проведення аналізу;
- ПП повинна мати окремі представлення активних і усунених вразливостей з автоматичним перенесенням вразливостей з активних на усунуті після того, як сканування визначає, що вразливості більше немає;
- ПП повинна мати можливість відзначати вразливість як раніше усунуту, але яка з'явилася знову (це може статися, коли система відновлюється з резервної копії або стара копія віртуальної машини повертається в оперативний режим);
- ПП повинна забезпечувати комплексну фільтрацію виявлених вразливостей з можливістю деталізації по наступним параметрам, але не обмежуватись ними: IP адреса, ідентифікатор агента, актив, аудит файл, ідентифікатор CCE, ідентифікатор CVE, оцінка CVSS v2, оцінка CVSS v3, Ім'я DNS, доступність експлойта, порт, протокол, рівень критичності, дата першого виявлення, дата останнього виявлення, текст вразливості;
- ПП має бути можливість додавати теги до активів, політик, облікових даних або запитів з налаштованим описом для поліпшення фільтрації та управління об'єктами.;
- ПП повинна мати панель для аналітика безпеки, яка автоматично встановлює пріоритети та оптимізує рішення для виправлення вразливостей, а саме надає відсоткове значення зменшення ризиків, при закритті вразливостей на групі пристроїв;
- ПП повинна надавати користувачам можливість запускати сканування на предмет виправлення вразливості, щоб переконатися, що вона усунута без необхідності налаштування параметрів сканування;
- ПП повинна забезпечувати можливість автоматичного групування кінцевих точок, тобто створення динамічних списків активів, що базується на результатах сканування, по наступним критеріям, але не обмежуватись ними: IP адреса, ім'я DNS, тип ОС, рівень критичності вразливості, порт, доступність експлойту, дата першого виявлення, дата останнього виявлення, текст вразливості;
- ПП повинна дозволяти користувачеві приймати ризик (робити виняток) з налаштованими датами закінчення терміну дії виявленої вразливості або змінювати рівень ризику (критичності) до рівня, що відрізняється від того, який постачальник визначив для цієї вразливості;
- ПП повинна забезпечувати функцію створення задач та можливість інтеграції зі сторонніми системами для відслідковування задач;
- ПП повинна підтримувати призначення задач окремим користувачам;
- ПП повинна забезпечувати можливість сповіщення про вразливість і подію;
- ПП повинна підтримувати створення сповіщень на основі результатів сканування вразливостей або аудиту конфігурації. Сповіщення має включати: налаштовуваний електронний лист з декількома змінними контексту, створення задач, запуск сканування, створення події в системному журналі, створення звіту та повідомлення користувачів.

Вимоги до аудиту на відповідність:

- ПП повинна підтримувати аудит на відповідність як з автентифікацією, так і без автентифікації, з або без необхідності встановлення агента на стороні клієнта на кінцевій точці;
- ПП не повинна покладатися на сторонні сканери для аудиту/оцінки конфігурації безпеки;

- ПП повинна надавати єдине представлення про всі результати аудиту вразливостей і відповідності вимогам;
- ПП повинна забезпечувати аудит конфігурацій для відповідності нормативним вимогам та іншим галузевим стандартам і стандартам кращої практики таких постачальників, як Microsoft, Cisco і VMware;
- ПП повинна забезпечувати аудит VMware ESXi і vCenter за допомогою VMware SOAP API;
- ПП повинна забезпечувати аудит операційних систем Microsoft для перевірки параметрів безпеки і конфігурацій;
- ПП повинна забезпечувати аудит всіх основних операційних систем Unix для перевірки параметрів безпеки і конфігурацій;
- ПП повинна забезпечувати аудит баз даних для перевірки параметрів безпеки і конфігурацій, таких як: PostgreSQL, MongoDB, Microsoft SQL Server, IBM Db2, SAP ASE, Oracle Database, MySQL;
- ПП повинна забезпечувати аудит додатків для перевірки параметрів безпеки і конфігурацій, таких як: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office тощо;
- ПП повинна забезпечувати аудит мережевої інфраструктури для перевірки параметрів безпеки і конфігурацій, таких як: Cisco, Arista, HPE, F5 і т.п.;
- ПП повинна забезпечувати аудит певних продуктів безпеки кінцевих точок на предмет статусу установки і оновлення;
- ПП повинна забезпечувати аудит особистої інформації (PII) і іншого конфіденційного контенту;
- ПП повинна дозволяти налаштовувати політики аудиту відповідно до потреб організації;
- ПП повинна надавати можливість проведення аудитів на відповідність стандартам CIS;
- ПП повинна надавати можливість проведення аудитів на відповідність стандартам DISA STIG.

Вимоги до покриття систем та аналітики загроз:

- ПП повинна вміти відслідковувати зміни DHCP, пов'язуючи результати сканування з іменами пристроїв в системі.
- ПП повинна підтримувати можливість збереження результатів сканування неактивних кінцевих станцій протягом налаштованого періоду часу.
- ПП повинна включати детальні дані відносно результатів сканування, включаючи таку інформацію, як знайдені версії DLL.
- ПП повинна повідомляти про відомі недоліки в заданій цілі, виявленої консультативними організаціями з безпеки (наприклад, за базою даних Common Vulnerabilities and Exposures (CVE) та Національною базою даних вразливостей (NVD)).
- ПП повинна підтримувати сканування вразливостей на відповідність PCI. Система повинна включати попередньо визначені профілі сканування PCI, які відповідають поточним критеріям PCI DSS для сканування мережі. Повинна існувати функція для фільтрації всіх інших вразливостей, що не відносяться до PCI.
- ПП повинна забезпечувати аудит виправлень для операційних систем і додатків Microsoft, таких як Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange і інші.
- ПП повинна забезпечувати аудит виправлень для всіх основних операційних систем Unix, включаючи macOS, Linux, Solaris, IBM AIX, HP-UX та інші.
- ПП повинна забезпечувати аудит виправлень для мережевої інфраструктури, включаючи Cisco, Juniper і інші.
- ПП повинна підтримувати сканування SCADA пристроїв.

- ПП повинна вміти збирати/імпортувати і відображати дані про вразливості IT і OT мереж для єдиної візуалізації вразливостей в об'єднаних мережах IT/OT.
- ПП повинна забезпечувати сканування сторонніх додатків, таких як Java і Adobe.
- ПП повинна забезпечувати можливості аудиту пристроїв і мереж SCADA.
- ПП повинна надавати звіти про репутацію загроз, виявлених шкідливих програм і бот-мереж.
- ПП повинна забезпечувати пріоритизацію вразливостей з використанням аналітики загроз в реальному часі і алгоритмів машинного навчання для оцінки вразливостей і прогнозування того, які з них з найбільшою ймовірністю будуть використані в найближчому майбутньому.
- ПП повинна забезпечувати пріоритизацію вразливостей, яка допомагає користувачам зрозуміти ключові фактори, що впливають на кожну оцінку вразливості (наприклад, новизну загрози, зрілість коду використання, категорії джерел Threat Intelligence).
- ПП повинна включати оцінку вразливості відповідно до загальної системи оцінки вразливостей (CVSS).
- ПП повинна забезпечувати налаштовуваний механізм оцінки вразливостей, що базується на прийнятих в галузі стандартах, таких як CVSS.
- ПП повинна надавати інформацію про використання вразливостей з Core Impact, Metasploit і Immunity CANVAS.
- ПП повинна надавати інформацію про використання шкідливих програм на кінцевому пристрої.
- ПП повинна дозволяти вибирати тести на основі інформації, отриманої при первинному скануванні, щоб проводити подальше тестування на основі отриманої інформації про даний пристрій або кінцеву точку.
- ПП повинна відслідковувати життєвий цикл вразливостей стосовно окремих кінцевих пристроїв, а також середовищ, включаючи дату першого виявлення, останнього спостереження і усунення вразливості.
- ПП повинна підтримувати сканування серверів VMware на вразливості і відповідність вимогам за допомогою власного API VMware.
- ПП повинна дозволяти сканувати пристрої за розкладом.
- ПП повинна дозволяти включати або відключати перевірки на певні вразливості під час сканування.
- у ПП має бути передбачена можливість відключення потенційно шкідливих перевірок.
- ПП повинна автоматично запускати і зупиняти сканування за розкладом без втручання користувача.
- ПП повинна дозволяти припиняти і відновлювати сканування вручну.
- ПП повинна дозволяти запускати сканування, незавершене у встановлений термін, або переносити на наступний запланований період.
- ПП повинна мати можливість приймати цілі сканування в різних форматах, включаючи імена DNS, діапазони IP-адрес і класи IP, а також попередньо визначені списки активів. Наприклад, 10.0.1.1 - 10.0.1.100. Також повинен підтримуватися імпорт списку IP-адрес, що містяться в файлі.
- ПП повинна підтримувати сканування IPv6 з пасивним виявленням активів IPv6.
- ПП повинна забезпечувати можливість відключення сканування периферійних пристроїв, наприклад принтерів.

Вимоги до пасивного сканування:

- ПП повинна забезпечувати можливість пасивного сканування.
- пасивний сканер повинен включати можливість виявлення нових активів шляхом моніторингу мережевого трафіку без активного сканування.
- пасивний сканер повинен відображати виявлені в трафіку активи в реальному часі.
- пасивний сканер повинен надавати інформацію про окрему мережу, мережі в цілому або будь-якої конкретної групи хостів.
- пасивний сканер повинен мати можливість відправляти події, пов'язані з трафіком, через системний журнал в системи кореляції подій.

- пасивний сканер повинен поставлятися тим же виробником, що і основна система.

Вимоги до сканування веб-додатків:

- ПП повинна мати можливість сканувати не менше 212 веб-додатків з можливістю придбання додаткових ліцензій сканування веб-додатків.
- ПП повинна мати можливість сканувати як внутрішні, так і зовнішні веб-додатки.
- ПП повинна вміти визначати частини критично важливих веб-додатків, які безпечно сканувати, та визначати інші частини, які ніколи не слід сканувати, щоб запобігти затримці роботи або порушенням.
- ПП повинна мати можливість сканувати веб-застосунки, що використовують HTML5 та динамічне завантаження контенту за технологією AJAX.
- ПП повинна мати можливість звітувати про всі вразливості в веб-додатках - як внутрішніх, так і зовнішніх - в одній єдиній інформаційній панелі.
- ПП повинна мати можливість сканувати веб-програми за допомогою: облікових даних для автентифікації на основі сервера HTTP, автентифікації за допомогою форми входу, автентифікації за допомогою файлів cookie, автентифікації за допомогою Selenium.
- ПП повинна мати можливість регулювати навантаження для сканування.
- ПП повинна мати можливість обирати тести, які будуть використовуватися для сканування.
- ПП має ідентифікувати та класифікувати проблеми, ризики та вразливості. Він також повинен надавати детальну інформацію про ризики, вразливості та рекомендації щодо їх мінімізації.
- ПП повинна відстежувати дату виявлення вразливості.
- ПП повинна мати можливість розгортання локального сканера веб-додатків для виявлення вразливостей у веб-програмах, недоступних з мережі Інтернет.
- ПП повинна забезпечувати можливість розгортання локального сканера веб-додатків без додаткових витрат.
- Сканер веб-додатків повинен надавати той самий виробник ПП.
- ПП повинна мати власний сканер у хмарі для виявлення вразливостей у веб-додатках, до яких можна отримати доступ через мережу інтернет.
- ПП повинна мати можливість імпортувати сценарій Selenium, який містить один або кілька сценаріїв для відтворення дій сканера на певних сторінках для оцінки.
- ПП має оцінювати веб-програми і специфічні компоненти в веб-додатках та класифікувати вразливості по OWASP Top 10.
- ПП повинна бути простим у використанні та масштабуватися, щоб включати всі веб-додатки організації.
- ПП повинна сканувати та виявляти вразливості в API.
- ПП повинна перевіряти реалізацію SSL / TLS в веб-додатках.
- ПП повинна мати вбудований інструмент аналітики вразливостей, який консолідує інформацію з таких джерел, як внутрішня експертиза, рекомендації постачальників, GitHub Advisory Database і Національна база даних вразливостей (NVD).
- ПП повинна відображати профіль вразливості, що детально описує окрему вразливість, включаючи графічну хронологію подій, уражені активи, джерела, а також метрики, такі як профіль ризику та ступінь серйозності.
- ПП повинна надавати можливість переглядати вразливості, що належать до критичних категорій, таких як нещодавно активно експлуатовані, нові загрози, використані у програмах-вимагачах, та порівняти з даними про вразливості в середовищі організації.

3.3. Вимоги до режимів функціонування

- ПП повинна функціонувати 24/7.
- ПП повинна включати в себе інтегровану можливість активного та пасивного сканування для повної видимості вразливостей і відповідності стандартам.
- ПП повинна забезпечувати сканування без агентів і на основі агентів.

- додатковий віртуальний образ модулів сканування і консолі повинен бути доступний без додаткових витрат.
- ПП повинна підтримувати кілька географічно або логічно розподілених механізмів сканування, керованих центральною консоллю.
- ПП повинна підтримувати балансування навантаження і перемикання між декількома сканерами шляхом динамічного розподілу навантаження сканування між сканерами в залежності від доступності сканера протягом всього завдання сканування.
- ПП повинна надавати клієнтам можливість розгортати додаткові сканера в своєму середовищі без додаткових витрат.
- ПП повинна надавати клієнтам можливість розгортати додаткові агенти в своєму середовищі без додаткових витрат.
- ПП повинна надавати клієнтам можливість розгортати додаткові пасивні сканери в своєму середовищі без додаткових витрат.
- загальна кількість повнофункціональних сканерів, повнофункціональних агентів і пасивних сканерів для виявлення активів має бути необмежена.
- ПП повинна забезпечувати можливість підключення хмарних сканерів і запуску сканування зовнішньої мережі, що охоплює не менше 250 IP адрес організації з використанням єдиного системного інтерфейсу, розташованого локально.
- ПП повинна забезпечувати можливість налаштування портів, протоколів і служб для підключень до сканерів, розгорнутим по всій мережі.
- ПП повинна налаштовуватись, щоб регулювати сканування, для запобігання генерації трафіку, достатнього для порушення нормальної роботи мережевої інфраструктури.
- ПП повинна забезпечувати можливість підтримки автономного сканування і імпорту результатів на сервер.
- ПП повинна підтримувати сканування з аутентифікацією і без аутентифікації для локального і віддаленого виявлення вразливостей без необхідності установки агента на стороні клієнта на цільовому пристрої.
- ПП повинна забезпечувати сканування цільових систем як з аутентифікацією, так і без аутентифікації.

3.4. Вимоги до інтерфейсу користувача та зручності використання

- ПП повинна включати налаштовуванні графічні панелі і створені шаблони панелей для відображення вразливостей і стану безпеки.
- ПП повинна забезпечувати налаштовуваний тренд результатів сканування на інформаційних панелях з використанням відфільтрованих результатів для визначення декількох ліній тренда на одному графіку.
- ПП повинна дозволяти кожному користувачеві створювати кілька користувальницьких інформаційних панелей.
- елементи інформаційної панелі повинні легко змінюватись шляхом фільтрації, для відображення даних на основі списку активів, перевірок вразливостей або відповідностей, часу, пошуку за ключовими словами, IP-адреси і т.п.
- частота оновлення інформаційних панелей повинна налаштовуватись, для оновлення за розкладом.
- ПП повинна забезпечувати можливість імпорту / експорту шаблонів інформаційних панелей.
- ПП повинна надавати можливість додавати різні персоналізовані візуальні елементи для налаштування інформаційних панелей, включаючи кругові діаграми, гістограми, матриці і тенденції.
- ПП повинна надавати користувачам можливість спільно використовувати інформаційні панелі.
- ПП повинна підтримувати налаштування параметрів шаблону і форматування інформаційних панелей.

- ПП повинна підтримувати створення звітів, що налаштовуються з використанням шаблонів, наданих постачальником, або без шаблонів.
- ПП повинна забезпечувати можливість фільтрації результатів в звітах по різним критеріям, включаючи, але не обмежуючись списками активів, репозиторіями, адресами, типами вразливостей, необробленим текстом і полями дат.
- ПП повинна надавати вбудовані звіти про сканування та журнали системи.
- ПП повинна забезпечувати можливість повної автоматизації звітів, включаючи виконання і відправлення за розкладом, а також відправлення звітів після сканування.
- ПП повинна забезпечувати можливість перегляду результатів в консолі, незалежно від процесу створення звітів.
- ПП повинна підтримувати можливість створення звітів в наступних форматах: PDF, CSV, CyberScope, DISA ASR або DISA ARF.
- ПП повинна забезпечувати можливість налаштовувати та відображати тенденції результатів сканування в звітах на одному графіку.
- ПП повинна надавати матричні таблиці, підсумовуючи числа по різним фільтрованим наборам результатів.
- ПП повинна забезпечувати автоматичне відправлення звітів для аналітика безпеки на відповідність стандартам.
- ПП повинна надавати звіти про відповідність нормативним вимогам без додаткових витрат.
- звіти повинні мати можливість включати імена пристроїв (NetBIOS, DNS) разом з IP-адресами.
- ПП повинна забезпечувати можливість шифрування і захисту звітів паролем.
- ПП повинна забезпечувати можливість автоматичної відправки звітів по електронній пошті.
- ПП повинна забезпечувати можливість відправки звітів за допомогою служб веб-публікації.
- ПП повинна дозволяти завантажувати та додавати зображення для створення звіту.
- ПП повинна надавати звіти високого рівня щодо показників безпеки і відповідностей стандартам.

3.5. Вимоги до сумісності та електронної інформаційної взаємодії

- ПП повинна підтримувати різні платформи для розміщення сканера, включаючи Windows, Linux, macOS, а також віртуальні і апаратні пристрої.
- ПП повинна підтримувати різні платформи для розміщення агента, включаючи Windows, Linux, macOS.
- ПП повинна забезпечувати інтеграцію з системами управління виправленнями для аудиту виправлень і створення звітів про зміни результатів сканування, таких як Microsoft Configuration Manager (SCCM) / WSUS, Red Hat Satellite, HCL BigFix, Broadcom Symantec IT Management Suite (ITMS).
- ПП повинна забезпечувати інтеграцію з менеджерами мобільних пристроїв (MDM) для виявлення та аудиту мобільних пристроїв.
- ПП повинна інтегруватися з рішеннями управління привілейованим доступом, такими як CyberArk, BeyondTrust та Delinea (раніше Thycotic), для управління обліковими даними.

3.6. Вимоги до захисту інформації та кіберзахисту

- відповідність Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- ПП повинна забезпечувати управління доступом на основі ролей з метою контролю доступу користувачів до певних наборів даних і функцій, доступним цим користувачам.

- ПП повинна дозволяти адміністраторам визначати ролі в залежності від посадових обов'язків і відповідних рівнів доступу до відповідних функцій.
- ПП повинна мати можливість інтеграції з LDAP для аутентифікації користувача.
- ПП повинна підтримувати кілька серверів LDAP для аутентифікації.
- ПП повинна підтримувати Security Assertion Markup Language (SAML) для забезпечення кілька варіантів єдиного входу / аутентифікації, таких як Okta, OneLogin, Microsoft AD FS або Shibboleth 2.0.
- ПП повинна мати докладний звіт щодо активності користувачів.
- ПП повинна дозволяти адміністраторам обмежувати доступ для окремих користувачів або груп до певних списків активів, політикам сканування і репозиторіїв вразливостей.
- ПП повинна дозволяти адміністраторам призначати ресурси для кожного користувача або групи, наприклад політики сканування, списки активів, запити та облікові дані.
- ПП повинна дозволяти адміністраторам обмежувати дозвіл на проведення: повного сканування, сканування з використанням певних політик.
- у ПП має бути передбачена можливість планування часу, щоб запобігти сканування в заборонені години.
- ПП повинна підтримувати створення організацій з повним поділом даних між цими організаціями в межах однієї консолі.
- ПП повинна надавати можливість визначати обмеження для діапазону IP-адрес для кожної організації.
- ПП повинна забезпечувати можливість прийняття та зміни ризику вразливостей.
- ПП повинна дозволяти введення і безпечне зберігання облікових даних користувачів, включаючи локальні і доменні облікові записи Windows, а також su і sudo для Unix систем з доступом по SSH.
- ПП повинна забезпечувати можливість підвищення привілеїв для цілей зі звичайних користувачів до адміністратора.
- ПП повинна підтримувати необмежену кількість облікових даних «SSH».

4. Вимоги до супроводу та обслуговування предмету закупівлі

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

Таблиця 2. Вимоги до послуги

№ з/п	Вимоги
1	Реорганізація структури організацій та сканерів: 1. Міграція в єдину організацію: перенесення політик і звітів, історичних результатів, налаштування ролей і груп доступу, повторне внесення облікових даних. 2. Тестування: перевірка статусу сканерів, контрольні сканування та порівняння результатів до і після міграції.
2	Розробка політик сканування для спеціалізованих типів систем: 1. Відеоспостереження: політика з обмеженим набором портів, низьким навантаженням (обмеження кількості одночасних перевірок) і перевіркою вбудованих облікових даних. 2. Мережеве обладнання (MikroTik, FortiGate): окремі політики з режимами без автентифікації та з автентифікацією (SSH/SNMPv3, обліковий запис з правами

	лише на читання), перевірка версії операційної системи на відомі вразливості (CVE). 3. Тестування: перевірка коректності відпрацювання політик на кількох системах, налаштування тайм-аутів і послідовності виконання.
3	Створення шаблонів універсального звіту за результатами сканування: 1. Три рівні деталізації: a. короткий (зведення за критичністю, топ ризиків); b. середній (розбивка за групами активів, топ вразливих активів); c. детальний (повний перелік по кожному активу). 2. Актуальні вразливості: без врахування виправлених, з групуванням за одним критерієм через Asset Tag. 3. Зміни відносно попереднього сканування: розділи з новими, усуненими та повторно виявленими вразливостями.

4.2. Вимоги до гарантійної підтримки

- Надання консультацій по телефону, електронній пошті та на сайті підтримки виробника щодо питань встановлення, налаштування та експлуатації ПП з понеділка по неділю з 00.00 до 24.00 годин (цілодобово).
- Постійний (24х7) доступ до центру технічної підтримки виробника через сайт або електронною поштою для отримання консультацій;
- Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення;
- Постійний (24х7) авторизований доступ до сайту виробника;
- Можливість реєстрації сервісних випадків в режимі 24х7 в системі підтримки виробника.

5. 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 керування процесом пошуку та мінімізації впливу вразливостей на IT-інфраструктуру у складі впровадженої ІКС.

Ініціатор закупівлі **В.К. Цвєтков**

Додаток 2

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

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. 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 **В.К. Цвєтков**

Додаток 3

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 101

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» жовтня 2026 року

ПРИСУТНІ:

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

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 14.05.2026 № 604/11071) (далі – Програма), у 2026 році, а саме:

1.1. проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру» (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);

1.2. доопрацьований проєкт технічних вимог до закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (пункт 7.1 «Створення, розвиток, впровадження, модернізація платформ та систем автоматизації процесів управлінської діяльності (інформаційних систем управління) та великих даних» переліку завдань і заходів Програми) у частині внесення змін до підпункту 4.4.5 «Вимоги до захисту інформації та кіберзахисту».

2. Різне.

По пункту 1.1 питання 1

СЛУХАЛИ:

В. Тихонова, який поінформував, що у складі інформаційно-комунікаційної системи центру моніторингу та кібербезпеки міських сервісів експлуатується підсистема керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру, яка використовує відповідну програмну продукцію, що забезпечує мінімізацію впливу ризиків кібербезпеки, пов'язаних з несанкціонованими спробами експлуатації вразливостей в об'єктах кіберзахисту (ОК); зниження часу простою ОК за рахунок запобігання кіберінцидентів; покращення сталої та безперервної роботи ОК, з метою продовження строку дії зазначеної програмної продукції необхідно ппровести відповідну закупівлю та представив проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру» (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 підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ-інфраструктуру (пункт 6.5 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.2 питання 1

СЛУХАЛИ:

Н. Йожикова, який поінформував про необхідність модернізації програмного забезпечення інформаційно-комунікаційної системи «Освіта» (ПЗ ІКС «Освіта») щодо управління довідниками та обліковими записами користувачів в адміністративній панелі ПЗ ІКС «Освіта»; ведення інформації про заклади освіти; процесів електронного зарахування; інформаційного профілю дитини; роботи з інформацією про мережу закладів освіти; цифровізації організації процесу харчування здобувачів освіти; електронної інформаційної взаємодії із зовнішніми інформаційними системами та представив доопрацьований проєкт технічних вимог до закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (пункт 7.1 переліку завдань і заходів Програми) у частині внесення змін до підпункту 4.4.5 «Вимоги до захисту інформації та кіберзахисту».

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

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Головний інформаційно-обчислювальний центр» під час процедури закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (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 вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-2362 **Дата реєстрації** 07.10.2026
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 07.10.2026 (Протокол № 101 від 07.10.2026)

Кількість файлів: 3 **Кількість ЕП:** 24

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
07.10.2026 № 075-2362

Перелік електронних підписів

П.І.Б.	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Тихонов Володимир Володимирович **Кількість ЕП:** 3	08.10.2026 15:07:39 ; 08.10.2026 15:07:40 ; 08.10.2026 15:07:41 ;	08.10.2026 15:07:41 Погодив;	08.10.2026 15:07:41 Погодив
Пашков Сергій Петрович **Кількість ЕП:** 3	07.10.2026 16:07:26 ; 07.10.2026 16:07:28 ; 07.10.2026 16:07:29 ;	07.10.2026 16:07:29 Погодив;	07.10.2026 16:07:29 Погодив
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 3	07.10.2026 15:45:41 ; 07.10.2026 15:45:43 ; 07.10.2026 15:45:44 ;	07.10.2026 15:45:44 Погодив;	07.10.2026 15:45:44 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 3	07.10.2026 15:44:41 ; 07.10.2026 15:44:43 ; 07.10.2026 15:44:44 ;	07.10.2026 15:44:45 Погодив;	07.10.2026 15:44:44
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 3	07.10.2026 15:07:47 ; 07.10.2026 15:07:49 ; 07.10.2026 15:07:50 ;	07.10.2026 15:07:50 Погодив;	07.10.2026 15:07:50 Погодив

Йожиков Нікіта Сергійович **Кількість ЕП:** 3	07.10.2026 15:06:54 ; 07.10.2026 15:06:55 ; 07.10.2026 15:06:56 ;	07.10.2026 15:06:57 Погодив;	07.10.2026 15:06:56 Погодив
Бухта Андрій Миколайович **Кількість ЕП:** 3	07.10.2026 15:06:54 ; 07.10.2026 15:06:55 ; 07.10.2026 15:06:56 ;	07.10.2026 15:06:56 Погодив;	07.10.2026 15:06:56 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 3	07.10.2026 15:03:25 ; 07.10.2026 15:03:26 ; 07.10.2026 15:03:27 ;	07.10.2026 15:03:27 Погодив;	07.10.2026 15:03:27 Погодив

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№ 101926/12 від 19.10.2026
На № 075/2-1808 від 09.10.2026

СКП «КИЇВТЕЛЕСЕРВІС»

Щодо запиту цінової пропозиції

Комерційна пропозиція

Товариство з обмеженою відповідальністю «ОПТІДАТА» просить розглянути комерційну пропозицію щодо постачання програмної продукції Tenable та послуг встановлення та налаштування.

№ п/п	Найменування товару	Кількість	Одиниці виміру	Ціна без ПДВ, гривня	Вартість без ПДВ, гривня
1	Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ інфраструктуру у складі: - Програмна продукція Tenable Security Center 1 рік -1 шт. - Програмна продукція Tenable Web App Scanning (Web Apps 212) 1 рік – 1 шт. - Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) (IP Bands: 250) 1 рік-1 шт.	1	комплект	7 037 500,00	7 037 500,00
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування)	1	послуга	1 737 500,00	1 737 500,00
				Всього, грн	**8 775 000,00**
				ПДВ, грн	**1 755 000,00**
				Разом з ПДВ, грн	**10 530 000,00**

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/953
Від 19.10 2026 р

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

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

Вих.№322 від 16.10.2026

СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 075/2-1810 від 09.10.2026 надаємо вартість на Програмну продукцію для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на IT-інфраструктуру (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки).

№	Найменування	Кіл-ть	Од. вимір	Ціна, грн без ПДВ	Сума, грн без ПДВ
1	**Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на IT-інфраструктуру у складі:** Програмна продукція Tenable Security Center 1Y -1 шт. Програмна продукція Tenable Web App scanning (Web apps: 212) 1Y - 1 шт. Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) (IP Bands: 250) 1Y -1 шт.	1	комплект	7 017 500,00	7 017 500,00
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування)	1	послуга	1 712 500,00	1 712 500,00
				Всього грн, без ПДВ	8 730 000,00
				Податок на додану вартість (20%), грн	1 746 000,00
				Загальна сума грн, з ПДВ	10 476 000,00

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 № 075/2/948
Від 16.10 2026 р.

CYBERPRO
AUDIT AND PROTECTION

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

Вих.№ 2026-10-20/1
від 20 жовтня 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.

За Вашим запитом вартості на Програмну продукцію керування процесом пошуку та мінімізації впливу вразливостей на IT інфраструктуру, надаємо пропозицію:

№ з/п	Найменування	Од. виміру	Кількість	Вартість, грн.	
				без ПДВ	з ПДВ
1	Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на IT-інфраструктуру: Програмна продукція Tenable Security Center-1 шт. Програмна продукція Tenable Web App Scanning (Web apps: 212)-1 шт. Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) (IP Bands: 250) -1 шт.	комплект	1	7 021 250,00	8 425 500,00
2	Послуга, пов'язана з постачанням ПП (встановлення та налаштування)	послуга	1	1 725 000,00	2 070 000,00
				ВСЬОГО, грн. без ПДВ:	**8 746 250,00**
				ПДВ, 20%	**1 749 250,00**
				ВСЬОГО, грн. З ПДВ:	**10 495 500,00**

З повагою,

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/956
Від 20.10 2026