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

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

СЛУЖБОВА ЗАПИСКА

місто Київ «15» жовтня 2025 року

Конкретна назва предмета закупівлі – **Програмна продукція 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, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257).

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

Обґрунтування необхідності посилання на конкретні марку та виробника: Посилання на ПП Tenable обумовлено його поточним використанням для пошуку та мінімізації впливу вразливостей в міських сервісах 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 інформаційно-комунікаційних систем які підлягають скануванню на наявність вразливостей.

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 №85 від 25.08.2025 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.

Обґрунтування очікуваної вартості предмета закупівлі:

Очікувану вартість предмета закупівлі визначено методом порівняння ринкових цін у спосіб, що передбачає направлення не менше 3-х письмових запитів цінових пропозицій (електронною поштою) виробникам, офіційним представникам та дилерам, постачальникам конкретного товару, надавачам послуг.

Згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін шляхом направлення запитів учасникам ринку, очікувана вартість становить 10 384

253,87 (десять мільйонів триста вісімдесят чотири тисячі двісті п'ятдесят три гривні вісімдесят сім 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.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 5 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 №85 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»:

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

Заступник директора з юридичних питань _____ **О.Є. Юрко**

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

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

Додаток 1

ТЕХНІЧНІ ВИМОГИ

Програмна продукція 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:

Цей документ визначає технічні та функціональні вимоги до закупівлі програмної продукції керування процесом пошуку та мінімізації впливу вразливостей на міську ІТ інфраструктуру з послугами, пов'язаними з її постачанням.

1.1 Підстава для розроблення технічних вимог

На виконання пункту 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257), а також рішення Київської міської ради від 12.12.2024 № 477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві».

1.2 Найменування засобу інформатизації

Програмна продукція керування процесом пошуку та мінімізації впливу вразливостей на ІТ інфраструктуру

1.3 Мета придбання засобу 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.

1.4 Терміни, скорочення, що використовуються

ПП – програмна продукція

ОК – об'єкт кіберзахисту, у розумінні визначення у Положенні про забезпечення кібербезпеки в місті Києві, затверджене рішенням Київської міської ради від 12.12.2024 №477/10285 «Про деякі питання забезпечення кібербезпеки в місті Києві».

2. Призначення засобу інформатизації:

2.1. Основні завдання та функції засобу інформатизації

- пошук та виявлення вразливостей в ОК;
- систематизація, узагальнення інформації та перетворення її у формат, придатний для проведення подальшого аналізу ефективності заходів із реагування на кіберінциденти та кібератаки, а також виконання процесів автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності.

2.2. Очікувані результати від впровадження засобу інформатизації

- мінімізація впливу ризиків кібербезпеки пов'язаних з несанкціонованими спробами експлуатації вразливостей в ОК;
- зниження часту простою ОК за рахунок упередження кіберінцидентів;
- покращення сталої та безперервної роботи ОК.

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 Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на ІТ інфраструктуру - 1 комплект. Склад комплекту (поставки ПП) наведено у таблиці 1.

Склад комплекту

Таблиця 1.

№ з/п	Найменування програмного забезпечення*	Обсяг ліцензії	Кількість
1	Програмна продукція Tenable Security Center	8000 тис. IP Subscription (TSC) строком на 1 рік	1
2	Програмна продукція Tenable Web Application Scanning	Web Application Scanning (TIO-WAS) (не менше 50 FQDN) строком на 1 рік	1
3	Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+)	IP Bands: не менше 250	1

- Якщо запропоноване рішення для реалізація цих технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки;

- всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення;

- на обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника

- запропоноване рішення має містити ліцензію, що дає змогу сканувати активи на наявність вразливостей у кількості не менше 8000 IP адрес

- ПП повинна поставлятися від одного виробника у вигляді віртуального пристрою та повинно бути виконаним у вигляді єдиної платформи, що не потребує використання будь-якого стороннього системного або прикладного програмного забезпечення (операційних систем, програмних додатків, систем керування базами даних тощо) для його впровадження;

- всі компоненти ПП мають встановлювались локально та не потребувати підключення до мережі інтернет.

- ПП повинна мати центральну консоль для всіх своїх компонентів, яка розгортається локально, щоб збирати, управляти і аналізувати інформацію про вразливості, не відправляючи їх в хмару.

- ПП повинна мати можливість локально встановлювати активні сканера в мережі та підключати їх до центральної консолі

- ПП повинна мати можливість локально встановлювати агенти на кінцеві точки та підключати їх до центральної консолі

- ПП повинна мати можливість локально встановлювати пасивні сканера та підключати їх до центральної консолі.

- ПП повинна централізувати і повністю автоматизувати щоденне оновлення бази вразливостей від постачальника.
- ПП повинна підтримувати автономний процес оновлення без доступу в інтернет.
- ПП повинна забезпечувати інтегровану модель зберігання даних, яка не залежить від третього стороннього продукту, який надає базу даних.
- ПП повинна мати комплексний, відкритий REST API для автоматичного створення сценаріїв сканування і експорту даних з безпеки, без додаткових витрат.
- ПП повинна підтримувати можливість виявлення активів, що не використовують ліцензію.
- ПП повинна забезпечувати можливість активного сканування і пасивного моніторингу мережі для виявлення активів.
- ПП повинна вміти виявляти мобільні пристрої.
- ПП повинна покладатися на сторонні сканери для виявлення активів, сканування портів або ідентифікації ОС.
- ПП повинна забезпечувати виявлення веб-служб і служб баз даних.
- ПП повинна вміти виявляти служби, що працюють на нестандартних портах.
- ПП повинна вміти виявляти служби, в яких не відображаються банери підключення.
- ПП повинна бути здатна тестувати кілька примірників однієї й тієї ж служби, що працює на різних портах.
- ПП повинна вміти сканувати «мертві» кінцеві точки (пристрої, що не відповідають на ICMP запити).
- ПП повинна підтримувати необов'язкове використання netstat для швидкого і точного перерахування відкритих портів в системі при наданні облікових даних.
- ПП повинна підтримувати використання SMB і WMI для сканування систем Windows.
- ПП повинна мати можливість автоматично запускати служби віддаленого реєстру в системах Windows при виконанні сканування з обліковими даними, а потім автоматично зупиняти службу після завершення сканування.
- ПП повинна підтримувати безпечне з'єднання(ssh) з можливістю підвищення привілеїв для сканування вразливостей і аудиту конфігурації в системах Unix.
- ПП повинна мати можливість збирати/ імпортувати і відображати дані про активи IT і OT мереж в єдиній консолі.
- ПП повинна забезпечувати можливість налаштування політик сканування для мінімального впливу на мережі і цілі сканування.
- ПП повинна забезпечувати виявлення точок бездротового доступу (WAP) за допомогою активного і пасивного сканування.
- ПП повинна забезпечувати можливість виявлення нових пристроїв і відправки попереджень за допомогою електронної пошти, системного журналу або консольним повідомленнями.
- ПП повинна забезпечувати можливість автоматичного запуску 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.

4.1.2 Послуга, пов'язана з встановленням та налаштуванням програмної продукції - 1 послуга.

Таблиця 2. Склад послуги

№ з/п	Вимоги
1	Проведення аналізу стану ПП Tenable Security Center, Tenable Web Application Scanning, Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) з урахуванням всіх модулів та їх конфігурацій на предмет конфліктуючих та неефективних правил, політик, конфігурацій. Результати проведеного аналізу 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 інше); 4. Рекомендації щодо покращення функціонування ПП: 5. Поетапний план міграції ПП на нові версії компонентів; 6. План тестування програмної продукції з урахуванням модернізації ПП.
2	Розробка та впровадження інформаційних панелей (Dashboards). Не менше ніж 5 панелей. Кожна панель має: 1. Бути побудована за допомогою функціональних можливостей ПП без використання іншого програмного забезпечення; 2. Оновлюватися за розписом або за запитом з можливостю коригування часу оновлення; 3. Мати графічні елементи візуалізації та стислі описи основних показників; 4. Відображати сенсор (майданчик) сканування з урахуванням об'єктів сканування; 5. Мати фільтри віджети/компоненти згідно періодів, ідентифікаторов CVE, рівнем критичності, наявності експлоїту; 6. Контролювати безперервну роботу всіх сенсорів сканування.
3	Формування аналітичних звітів. Не менше ніж 5 звітів. Кожен звіт має: 1. Бути побудованим за допомогою функціональних можливостей ПП без використання іншого програмного забезпечення; 2. Формуватися за розкладом та/або тригерною подією; 3. Відображати вичерпну інформацію для аналізу поточного стану ідентифікованих вразливостей та час з моменту їх ідентифікації; 4. Рекомендації щодо усунення вразливостей та/або пом'якшувальних дій спрямованих на зниження рівня кіберризику.
4.	Побудова інтеграції між ПП та іншими ІКС та програмним забезпеченням (таких як Proxy, LDAP, SMTP, SIEM не менше ніж 5 од) 1. Аналіз ПП та інших ІКС та програмного забезпечення та вибір оптимального механізму інтеграції; згідно наявності у вендорів готових інструментів або конекторів, що дозволяють забезпечити стабільну та безпечну взаємодію без розробки індивідуальних API-інтеграцій 2. Побудова інтеграції між ПП та іншими ІКС та програмним забезпеченням; 3. Тестування інтеграційних зв'язків на предмет сталої роботи

4.2 Вимоги до безпеки

- 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 ADFS 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.

4.3 Вимоги до ергономіки та технічної естетики

- 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.

4.4 Вимоги до захисту інформації

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

4.5 Вимоги до уніфікації

- 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.

4.6 Вимоги до надійності засобу інформатизації та збереженності інформації

- 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 постачальників;
- ПП повинна забезпечувати аудит конфігурації, що базується на кращих практиках для 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, DB2, Sybase, Oracle, MySQL;
- ПП повинна забезпечувати аудит додатків для перевірки параметрів безпеки і конфігурацій таких як: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office и т.п.;
- ПП повинна забезпечувати аудит мережевої інфраструктури для перевірки параметрів безпеки і конфігурацій таких як: Cisco, Arista, HP, 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;

4.7 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації

- 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 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 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.

4.8 Вимоги до режимів функціонування засобу інформатизації

- ПП повинно 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;
- 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
- 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 охоплюэ 250 IP адрес організації з використанням єдиного системного інтерфейсу, розташованого локально.

- ПП повинна забезпечувати можливість настройки 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 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».

- ПП повинна інтегруватися з рішеннями управління привілейованим доступом, такими як CyberArk, BeyondTrust, Thycotic і Lieberman для управління обліковими даними.

- 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.

- ПП повинна покладатися на сторонні сканери для сканування вразливостей.

- 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, база даних Common Vulnerabilities and Exposures (CVE), База даних вразливостей з відкритим вихідним кодом (OSVDB), SecurityFocus Bugtraq (BID) або будь-яке їх поєднання).

- 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 інтеграцію з системами управління виправленнями для аудиту виправлень і створення звітів про зміни результатів сканування, таких як Microsoft WSUS / SCCM, Red Hat Satellite, IBM BigFix (раніше IBM Tivoli Endpoint Manager), Symantec Altiris, VMWare Go.

- ПП повинна забезпечувати інтеграцію з менеджерами мобільних пристроїв (MDM) для виявлення та аудиту мобільних пристроїв.

- 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 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.

- 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.

4.9 Вимоги до функцій (завдань), що виконуються засобом інформатизації

- ПП повинна мати можливість сканувати не менше 50 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-програми HTML5, AJAX, HTML.

- 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, консультативна база даних GitHub 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.

4.10 Вимоги до супроводу та обслуговування засобу інформатизації

- 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 передачі результатів виконаних робіт та/або наданих послуг

- Забезпечення відображення примірників ПП у кабінеті Замовника на порталі виробника;
- активація ПП автоматично в день підписання Сторонами акту передачі-приймання ПП та подальшим її терміном дії протягом 12 місяців;
- паперовий примірник Звіту щодо результатів аудиту поточного стану ПП.

**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 № 85

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 «25» серпня 2025 року

ПРИСУТНІ:

Члени робочої групи:
В. Жучков
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:

1.1. 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) для встановлення на мостових та підмостових шляхопроводах на території міста Києва;

1.2. 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) для встановлення на мостових та підмостових шляхопроводах на території міста Києва;

1.3. проєкт технічних вимог до закупівлі «Послуга по встановленню засобів, обладнання та матеріалів 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) для встановлення на мостових та підмостових шляхопроводах на території міста Києва;

1.4. доопрацьований проєкт технічних вимог до закупівлі «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи ліцею №19 «Юніті» Подільського району м. Києва по вул. Білицькій, 55 у Подільському районі» (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) у частині уточнення адреси об'єкта;

1.5. доопрацьований проєкт технічних вимог до закупівлі «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи комунального загальноосвітнього навчального закладу І-ІІІ ступенів «Навчально-реабілітаційний центр № 6 м. Києва» по проспекту Свободи 7 у Подільському районі» (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) у частині уточнення адреси об'єкта;

1.6. проєкт технічних вимог до закупівлі «Програмна продукція 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, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми).

2. Різне.

По пунктах 1.1-1.3 питання 1

СЛУХАЛИ:

С. Осіпова, який повідомив, що для створення безпечного простору в столиці здійснюється розвиток комплексної системи відеоспостереження міста Києва, зокрема шляхом розширення зони контрольованого покриття системами відеоспостереження, а саме: на мостових та підмостових шляхопроводах на території міста Києва, тому є необхідність придбання засобів відеофіксації, обладнання та матеріалів, послуг з їх встановлення та представив проєкти технічних вимог до закупівель «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки», «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуги по встановленню засобів, обладнання та матеріалів для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: Д. Цвігун, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівель «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки», «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуги по встановленню засобів, обладнання та матеріалів для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми) використовувати проєкти технічних вимог, розглянуті на засіданні робочої групи.

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

По пунктах 1.4 – 1.5 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував про необхідність побудови структурованої кабельної системи ліцею № 19 «Юніті» Подільського району міста Києва та комунального загальноосвітнього навчального закладу І-ІІІ ступенів «Навчально-реабілітаційний центр № 6 м. Києва» у межах модернізації електронних комунікаційних мереж закладів загальної освіти міста Києва та представив доопрацьовані проєкти технічних вимог до закупівлі «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи ліцею № 19 «Юніті» Подільського району м. Києва по вул. Білицькій, 55 у Подільському районі» та «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи комунального загальноосвітнього навчального закладу І-ІІІ ступенів «Навчально-реабілітаційний центр № 6 м. Києва» по проспекту Свободи 7 у Подільському районі» у частині уточнення адрес об'єктів (пункт 6.2 переліку завдань і заходів Програми).

В обговоренні проєктів технічних вимог брали участь: С. Осіпов, М. Клюєва.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи ліцею № 19 «Юніті» Подільського району м. Києва по вул. Білицькій, 55 у Подільському районі» та «Роботи з розроблення проєктної документації на об'єкт будівництва «Нове будівництво структурованої кабельної системи комунального загальноосвітнього навчального закладу І-ІІІ ступенів «Навчально-реабілітаційний центр № 6 м. Києва» по проспекту Свободи 7 у Подільському районі» (пункт 6.2 переліку завдань і заходів Програми) використовувати доопрацьовані проєкти технічних вимог, розглянуті на засіданні робочої групи.

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

По пункту 1.6 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував про необхідність закупівлі програмної продукції керування процесом пошуку та мінімізації впливу вразливостей на міську ІТ інфраструктуру з послугами, пов'язаними з її постачанням та представив проєкт технічних вимог до закупівлі «Програмна продукція 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: С. Осіпов, М. Клюєва.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція 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» - 7, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1921
Дата реєстрації 25.08.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 25.08.2025 (Протокол № 85 від 25.05.2025)

Кількість файлів: 7
Кількість ЕП: 49

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
25.08.2025 № 075-1921

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Жучков Василь Анатолійович **Кількість ЕП:** 7	26.08.2025 12:54:31 ; 26.08.2025 12:54:32 ; 26.08.2025 12:54:34 ; 26.08.2025 12:54:36 ; 26.08.2025 12:54:37 ; 26.08.2025 12:54:39 ; 26.08.2025 12:54:40 ;	26.08.2025 12:54:41 Погодив;	26.08.2025 12:54:40
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 7	25.08.2025 16:54:17 ; 25.08.2025 16:54:19 ; 25.08.2025 16:54:20 ; 25.08.2025 16:54:22 ; 25.08.2025 16:54:23 ; 25.08.2025 16:54:25 ; 25.08.2025 16:54:27 ;	25.08.2025 16:54:28 Погодив;	25.08.2025 16:54:27
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 7	25.08.2025 16:21:15 ; 25.08.2025 16:21:15 ; 25.08.2025 16:21:17 ; 25.08.2025 16:21:18 ; 25.08.2025 16:21:19 ; 25.08.2025 16:21:20 ; 25.08.2025 16:21:21 ;	25.08.2025 16:21:22 Погодив;	25.08.2025 16:21:21
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 7	25.08.2025 16:07:31 ; 25.08.2025 16:07:31 ; 25.08.2025 16:07:32 ; 25.08.2025 16:07:33 ; 25.08.2025 16:07:34 ; 25.08.2025 16:07:35 ; 25.08.2025 16:07:36 ;	25.08.2025 16:07:36 Погодив;	25.08.2025 16:07:36 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 7	25.08.2025 16:04:42 ; 25.08.2025 16:04:43 ; 25.08.2025 16:04:43 ; 25.08.2025 16:04:44 ; 25.08.2025 16:04:45 ; 25.08.2025 16:04:47 ;	25.08.2025 16:04:48 Погодив;	25.08.2025 16:04:48 Погодив

	25.08.2025 16:04:48 ;		
Поліщук Олег Федорович **Кількість ЕП:** 7	25.08.2025 16:04:19 ; 25.08.2025 16:04:20 ; 25.08.2025 16:04:21 ; 25.08.2025 16:04:22 ; 25.08.2025 16:04:23 ; 25.08.2025 16:04:24 ; 25.08.2025 16:04:25 ;	25.08.2025 16:04:25 Погодив;	25.08.2025 16:04:25 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 7	25.08.2025 16:00:52 ; 25.08.2025 16:00:52 ; 25.08.2025 16:00:53 ; 25.08.2025 16:00:54 ; 25.08.2025 16:00:54 ; 25.08.2025 16:00:55 ; 25.08.2025 16:00:56 ;	25.08.2025 16:00:56 Погодив;	25.08.2025 16:00:56 Погодив

CYBERPRO
AUDIT AND PROTECTION

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

Вих.№2025-10-3/1
від 3 жовтня 2025 року

СКП «КИЇВТЕЛЕСЕРВІС»

ЦІНОВА ПРОПОЗИЦІЯ

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

За Вашим запитом №356-2025 від 23.09.2025 року надаємо цінову пропозицію:

№ з/п	Найменування товару/послуги	Од. виміру	Кіль-кість	Ціна, грн з ПДВ	Сума, грн з ПДВ
1	Програмна продукція для підсистеми керування процесом пошуку та мінімізації впливу вразливостей на IT інфраструктуру – 1 комплект: програмна продукція Tenable Security Center 1Y; програмна продукція Tenable Web App Scanning (Web Apps: 50) (50FQDN) 1Y; програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) IP Bands: 250 1Y	комплект	1	8 520 000,00	8 520 000,00
2	Послуга, пов'язана з встановленням та налаштуванням програмної продукції – 1 послуга	послуга	1	1 830 000,00	1 830 000,00
				ПДВ, 20%	**1 725 000,00**
				ВСЬОГО, грн з ПДВ:	**10 350 000,00**

З повагою
Директор
ТОВ «САЙБЕРПРО» /підписано КЕП/ **Сергій ДІДУР**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 293/2025
від 13.10.2025р.

ТОВ «ВІ ЄМ ДЖІ»

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

Вих.№191 від 02.10.2025

КП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 358-2025 від 23.09.2025 надаємо вартість на Програмну продукцію 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: 50) (50FQDN) 1Y-1 шт. Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) IP Bands: 250 1Y-1 шт.	1	комплект	6 950 000,00	6 950 000,00
2	Послуга, пов'язана з встановленням та налаштуванням програмної продукції	1	послуга	1 510 000,00	1 510 000,00
				Всього грн, без ПДВ	**8 460 000,00**
				Податок на додану вартість (20%), грн	1 692 000,00
				Загальна сума грн, з ПДВ	**10 152 000,00**

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 № 242/2025
Від 13.10. 2025 р.

ESKA your ITeam

Комерційна пропозиція

СКП «Київтелесервіс»

ТОВ "ЕСКА-СОФТ"
04050, місто Київ, вул.Глибочицька, буд. 17-Б, оф. 402
office@eska.global, eska.global
+38 (067) 372 39 55

ESKA your ITeam

ТОВ "ЕСКА-СОФТ"
04050, місто Київ, вул.Глибочицька, буд. 17-Б, оф. 402
office@eska.global, eska.global, +380673723955

Спеціалізоване комунальне підприємство «Київтелесервіс»
(СКП «Київтелесервіс»)

на запит цінової пропозиції

Комерційна пропозиція

До вашої уваги надаємо комерційну пропозицію 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 IT інфраструктуру у складі: - Програмна продукція Tenable Security Center 1Y - 1 шт. - Програмна продукція Tenable Web App Scanning (Web Apps: 50) (50FQDN) 1Y - 1 шт. - Програмна продукція Tenable Security Center Agents - Cloud Service (For Subscription SC/SC+) IP Bands: 250 1Y - 1 шт.	1	комплект	7 230 000,00	7 230 000,00
2	Послуга, пов'язана з встановленням та налаштуванням програмної продукції.	1	послуга	1 644 678,00	1 644 678,00
Всього, грн					8 875 634,67
ПДВ, грн					1 775 126,93
Разом з ПДВ, грн					10 650 761,60

Директор ТОВ «ЕСКА-СОФТ» *Іван СКРИПКА*