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

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

С Л У Ж Б О В А З А П И С К А

місто Київ «6» травня 2026 року

Конкретна назва предмета закупівлі – **Програмна продукція для підсистеми управління привілейованим доступом (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 для підсистеми управління привілейованим доступом (далі - ПП).

Обґрунтування необхідності посилання на конкретні марку та виробника:

Посилання на конкретне найменування ПП обумовлено її поточним використанням для забезпечення централізованого контролю доступу до привілейованих облікових записів об'єктів кіберзахисту (далі - ОК) Центром моніторингу та кібербезпеки міських сервісів та Наказом спеціалізованого комунального підприємства "Київтелесервіс" від 28.06.2024 № 76 "Про введення у дослідну експлуатацію підсистем Центру моніторингу та кібербезпеки міських сервісів".

Обґрунтування обсягів закупівлі:

Об'єм ліцензії обумовлено поточною кількістю привілейованих користувачів на ОК, потребою КП "Інформатика" (вих. № 075/3-945 від 01.04.2026) та КП "Головний інформаційно-обчислювальний центр" (вих. № 075/1-1087 від 27.03.2026).

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 № 36 від 22.04.2026 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», розробленого на основі Примірної методики визначення очікуваної вартості предмета закупівлі (наказ Мінекономіки від 18.02.2020 № 275) та

затвердженого наказом СКП «Київтелесервіс» від 21.08.2023 №68, з використанням методу порівняння ринкових цін у спосіб, що передбачає направлення не менше 3-х письмових запитів цінових пропозицій (електронною поштою) виробникам, офіційним представникам та дилерам, постачальникам конкретного товару, надавачам послуг.

Згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін шляхом направлення запитів учасникам ринку, очікувана вартість становить 10 807 200,00 (десять мільйонів вісімсот сім тисяч двісті 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 – програмна продукція – 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. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 9 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Протокол № 36 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 4 арк.
4. Додаток 4. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.
5. Додаток 5. Листи щодо потреби у ліцензуванні 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 для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки (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 щодо програмної продукції для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки, з послугою зі встановлення та налаштування програмної продукції, що закуповується.

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 в Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257).

1.2. Найменування засобу інформатизації:

Програмна продукція для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки.

1.3. Мета придбання засобу інформатизації

Забезпечення контролю доступу до привілейованих облікових записів, зниження ризиків їх компрометації шляхом автоматизованої ротації облікових даних і приховування паролів, а також підвищення рівня прозорості та безпеки за рахунок аудиту, запису та моніторингу дій користувачів під час роботи з привілейованими сесіями.

1.4. Терміни, скорочення, що використовуються

ПП – програмна продукція для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки.
ОК – об'єкт кіберзахисту, у розумінні визначення у Положенні про забезпечення кібербезпеки в місті Києві, затвердженого рішенням Київської міської ради від 12.12.2024 №477/10285.

2. Призначення засобу інформатизації:

2.1. Основні завдання та функції засобу інформатизації

- Забезпечення централізованого контролю доступу до привілейованих облікових записів ОК, зменшення ризику їх компрометації шляхом автоматизованої ротації облікових даних і приховування паролів.

- Забезпечення прозорості та аудиту дій користувачів через запис і моніторинг привілейованих сесій при роботі з ОК.

2.2. Очікувані результати від впровадження засобу інформатизації

- Підвищення рівня захищеності ОК.
- Покращення реагування на кіберінциденти та підвищення рівня оперативного контролю.
- Мінімізація ризиків, пов'язаних із випадковим чи навмисним порушенням політик безпеки, витоку даних або несанкціонованого використання привілейованих облікових записів ОК.

3. Характеристики об'єкта інформатизації

Підсистема управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки має такі функціональні можливості:

- моніторинг, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом та кібератакою щодо об'єктів кіберзахисту;
- забезпечення електронної взаємодії з об'єктами кіберзахисту;
- захист інформації від несанкціонованого доступу, модифікації (зміни) шляхом здійснення відповідних організаційних і технічних заходів, упровадження засобів та методів захисту інформації.

4. Вимоги до засобу інформатизації:

4.1.Вимоги до структури та функціонування засобу інформатизації

4.1.1. Склад закупівлі

- **Програмна продукція для підсистеми управління привілейованим доступом - 1 комплект.** Склад комплекту (поставки ПП) наведено у таблиці 1.

Таблиця 1. Склад комплекту

№ з/п	Найменування	Кількість користувачів
1	Програмна продукція (ліцензійне програмне забезпечення) тип 1.	70 од.
2	Програмна продукція (ліцензійне програмне забезпечення) тип 2.	130 од.

- **Послуга зі встановлення та налаштування ПП - 1 послуга.**

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

- **ПП (ліцензійне програмне забезпечення) тип 1** повинна забезпечувати:
  - доступ до ОК із використанням розширеного захисту за допомогою механізмів SSO, ризик орієнтованого способу автентифікації;
  - захищене зберігання облікових даних (секретів, паролів, ключів тощо);
  - адаптивний доступ до додатків;

- ізоляцію та запис сесій користувачів;
- адаптивну багатофакторну автентифікацію;
- виявлення аномалій та підозрілої поведінки;
- використання порталу для доступу до ОК без VPN.

ПП (ліцензійне програмне забезпечення) тип 2 повинна забезпечувати:

- доступ до ОК із використанням базового захисту;
- захищене зберігання облікових даних (секретів, паролів, ключів тощо);
- ізоляцію та запис сесій користувачів;
- виявлення аномалій та підозрілої поведінки;
- біометричну багатофакторну автентифікацію;
- використання порталу для доступу до ОК без VPN.

- Адміністрування комплексу технічних засобів та програмного забезпечення (далі – КТЗ) має забезпечуватися локально та віддалено через вебконсоль або офіційний додаток з безпечного з'єднання між адміністратором та сервером
- ПП повинна мати веб-інтерфейс користувача та адміністратора українською або англійською мовами
- ПП повинна підтримувати можливість входу на вебконсоль через облікові записи Active Directory, локально та через SSO (Single-Sign-On)
- ПП повинна підтримувати гнучку систему надання прав для окремих модулів чи функціоналу
- ПП повинна мати рольове управління з такими можливостями:
  - Розмежування прав доступу для налаштування безпосередньо системи для аудиту дій користувачів;
  - Призначення відповідальних з кіберзахисту на окремі сегменти інфраструктури;
  - Призначення відповідальних з кіберзахисту на аудит певних робочих станцій.
- ПП повинна забезпечувати підтримку (можливість керувати привілейованими обліковими записами, що використовуються в цільовій системі) для додатків поза списком "з коробки" з використанням скриптів або інших механізмів, реалізованих та підтримуваних виробником рішення для зміни та перевірки паролів через: SSH / Telnet , API для зовнішніх програм, моделювання дій користувача в сеансі вебпрограми.
- ПП повинна мати можливість захищати (керувати) та динамічно генерувати нові ключі SSH відповідно до вказаного шаблону.
- ПП повинна перевірити пароль/ключ SSH, що зберігається в запропонованому рішенні, з паролем/ключом SSH, що зберігається в цільовій системі, відповідно до певної політики.
- ПП повинна узгодити пароль/ключ SSH, що зберігається в запропонованому рішенні, з паролем/ключом SSH, що зберігається в цільовій системі, у разі невідповідності
- ПП повинна зберігати необмежену історію паролів та забезпечувати легкий доступ до історії (наприклад, через веб-інтерфейс).
- ПП повинна підтримувати різні середовища LDAP як мінімум: Sun One, MS Active-Directory, IBM Tivoli, Novel eDirectory, Oracle Internet Directory.
- ПП має забезпечувати виявлення пар ключів SSH в інфраструктурі
- ПП повинна забезпечувати керування ключами SSH та безпеку ключів SSH, які використовуються програмами у файлах конфігурації.

4.1.3 Вимоги до послуги зі встановлення та налаштування ПП:

Таблиця 2. Склад послуги

№ з/п	Вимоги
1	Налаштування додаткових компонентів (DV,PSM,RA,PVWA) системи CyberArk. Інсталювати наступні компоненти: 1. Третя нода DR Vault (Digital Vault) - необхідно забезпечити реплікацію та резервування навантаження на дві існуючі ноди. 2. PSM (Privileged Session Manager) - із метою збільшення кількості одночасних сесій для внутрішніх користувачів та оптимізації швидкодії; 3. Remote Access connector - забезпечити збільшення кількості одночасних сесій для зовнішніх користувачів без втрати швидкої роботи існуючих сесій. 4. PVWA (Password Vault Web Access) - для робото здатності системи під час проведення технічних або інших видів робіт.
2	Налаштування двосторонньої інтеграції SIEM Splunk з компонентом Privileged Threat Analytics (PTA) для обміну даними: 1. Налаштувати передачу журналів подій із SIEM Splunk через Syslog для подальшого аналізу на стороні PTA; 2. Налаштувати передачу журналів подій із PTA у SIEM Splunk, для виявлення ознак зловживання або неправильного використання платформи CyberArk привілейованими обліковими записами; 3. Налаштування експорту спрацювань правил безпеки PTA у SIEM Splunk.
3	Під час встановлення компонентів системи CyberArk (серверів, модулів та інших складових системи) забезпечити: 1. Проведення аналізу усіх компонентів системи CyberArk (серверів, модулів та інших складових системи) з метою визначення встановлених версій прикладного програмного забезпечення CyberArk та їх відповідності актуальним версіям, рекомендованих виробником. 2. Оновлення прикладного програмного забезпечення CyberArk на кожному компоненті системи CyberArk PAM до актуальних стабільних версій, що офіційно підтримуються виробником. 3. Оновлення прикладного програмного забезпечення повинно бути виконано з дотриманням вимог та рекомендацій виробника CyberArk, без втрати функціональності системи, налаштувань безпеки та конфігураційних параметрів,а також з забезпеченням безперервної або погодженої працездатності системи.

4.	За результатами встановлення та налаштування розробити та надати документацію згідно наступного переліку: 1. Актуалізувати схему архітектури компонентів CyberArk із відображенням логічної та/або фізичної взаємодії між компонентами системи, враховуючи нові компоненти. 2. Оновлений документ з описом вимог до мережевих підключень між компонентами системи CyberArk PAM, включаючи перелік необхідних мережевих протоколів, портів та напрямків з'єднань, що забезпечують повноцінне функціонування системи. 3. План відновлення системи (Disaster Recovery Plan) - План відновлення системи CyberArk PAM у разі аварійних ситуацій, що містить сценарії відмов, порядок відновлення компонентів, ролі відповідальних осіб.

4.2.Вимоги до безпеки

- ПП повинна мати власний механізм авторизації користувачів
- ПП повинна мати можливість інтеграції із зовнішніми системами або хмарними сервісами для забезпечення другого фактора автентифікації (MFA)
- ПП повинна підтримувати інтеграцію з Forti Authentificator за допомогою протоколу SAML
- ПП повинна мати внутрішню рольову модель розподілу прав доступу та щонайменше наступні ролі - адміністратор безпеки, аналітик безпеки.
- ПП повинна мати діючий експертний висновок про відповідність вимогам технічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

4.3.Вимоги до ергономіки та технічної естетики

- ПП повинна дозволяти керування списками вразливостей та сповіщеннями щодо ідентифікації нових вразливостей з можливістю фільтрації.
- ПП повинна мати візуальний редактор дашбордів аналітичних та статистичних даних.
- ПП повинна відображати дані у формі зручній для проведення аналізу.

4.4.Вимоги до захисту інформації

- ПП має обов'язково забезпечувати можливість створення безпечних (шифрованих) каналів зв'язку на основі сертифікатів SSL між привілейованими користувачами і ПП та між ПП і цільовими системами.
- Відповідність Закону України «Про захист інформації в інформаційно-комунікаційних системах».
- ПП має забезпечувати можливість налаштування таких безпечних (шифрованих) каналів зв'язку по наступним параметрам:
    - на основі само підписних сертифікатів (за допомогою пари «відкритий»-«приватний» ключі)
    - на основі сертифікатів центру сертифікації (CA).

4.5.Вимоги до уніфікації

- ПП має включати всі необхідні компоненти для побудови КТЗ з високою доступністю: забезпечувати функціонування комплексу в цілому при виході з ладу будь-якого компонента, за рахунок механізмів автоматичного балансування навантаження та побудови кластеру(ів) високої доступності;
- ПП має забезпечувати можливість розгортання КТЗ як на базі апаратних серверів так і у віртуальному середовищі VMware або Hyper-V поточних (підтримуваних виробником) версій;
- Під час роботи, рішення повинно бути захищено від впливу інших систем, включаючи зміни та оновлення.
- ПП має забезпечувати вбудоване захищене сховище для збереження записаних сесій привілейованих користувачів, реквізитів доступу (логін, пароль, ключі, доменні імена тощо) до КТЗ і цільових систем, журналів подій.

4.6.Вимоги до надійності засобу інформатизації та збереженості інформації

- ПП повинна мати вбудований механізм захисту від несанкціонованого доступу до інформації що зберігається у КТЗ. Даний захист повинен забезпечувати використання спеціального ключа захисту (пароля або апаратного ключа) під час кожного запуску КТЗ (після вимкнення або перезавантаження).
- ПП має забезпечувати можливість створення відмовостійких конфігурацій КТЗ на базі вбудованих технологій, використання сторонніх (зовнішніх) засобів для побудови таких (відмово стійких) конфігурацій – не допускається.
- ПП має забезпечувати можливість створення резервних копій що мають включати в себе всі параметри та налаштування КТЗ, а також записані сесії привілейованих користувачів. Резервні копії мають створюватися з використанням шифрованих (захищених) протоколів обміну даними (наприклад, на базі пари відкритого та приватного SSH ключа). Створені резервні копії повинні бути захищені від несанкціонованого перегляду даних що в них зберігаються та несанкціонованого відновлення.
- Схема кластеризації повинна надавати можливість взаємодії користувачів та інтеграцію в режимі Active-Active для всіх вузлів кластеру.

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

- ПП має забезпечувати можливість розгортання КТЗ без необхідності інтеграції з корпоративною службою каталогів (AD), тобто забезпечувати функціонування компоненту КТЗ незалежно від функціонування корпоративного каталогу.
- ПП має забезпечувати наявність окремого вебпорталу або додатку для налаштування та адміністрування.
- ПП має обов'язково забезпечувати можливість створення безпечних (шифрованих) каналів зв'язку на основі сертифікатів SSL між привілейованими користувачами і ПП та між ПП і ОК.
- ПП повинна записувати файли, що передаються через SFTP або буфер обміну в RDP підключеннях з можливістю відновлення їх у початковому вигляді.

4.8.Вимоги до режимів функціонування засобу інформатизації

- ПП повинна функціонувати 24/7;

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

- ПП повинна підтримувати ізоляцію та моніторинг сеансу без необхідності розкривати пароль / ключ ssh привілейованого облікового запису для станції користувача. Коли кінцевий користувач надійно автентифікований у модулі запису, ПП має автоматично отримувати привілейовані облікові дані з центрального безпечного репозиторію, запускати програму, вибрану раніше користувачем (додаток встановлений у модулі запису), та автоматично вводити облікові дані до програми (щоб не розповсюджувати їх на робочу станцію користувача). Запис сеансу з індексацією даних має бути доступним як параметр політики.
- ПП має безпечно встановлювати та керувати привілейованими сеансами в наступних системах:
    - Операційні системи: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)
    - Бази даних: Microsoft SQL, Oracle, MySQL, SAP HANA, HeidiSQL, DB2
    - Системи та програми управління інфраструктурою: DELL DRAC, RSA Authentication Manager, HP iLO, SAP GUI, BMC Remedy
    - Мережеві пристрої та пристрої безпеки: Cisco (маршрутизатори, комутатори Nexus, міжмережні екрани), HP, Checkpoint (SmartDashboard, https, ssh), Radware, F5 Networks, FortiGate, Palo Alto Networks
    - Інструменти CI/CD (https, ssh): Chef, Jenkins, Kubernetes, Docker, Jfrog, GitHub
    - Веб-служби: послуги SaaS, веб-інтерфейси, мінімум: Facebook (наприклад, маркетингові облікові записи), веб-служби Amazon (консоль керування, IAM, інтеграція STS), керування Microsoft Azure
    - Середовища віртуалізації: VMWare ESX/ESXi, vCenter (vSphere Client, https, ssh)
- ПП має забезпечувати підтримку (для моніторингу, ізоляції сеансу, функції єдиного входу для привілейованих облікових записів) для інших додатків та систем за допомогою не менш наступних можливостей:
    - Запуск програми із зазначеним набором параметрів, використовуючи описову мову сценаріїв.
    - Вбудований компонент, що забезпечує підтримку керування власними веб-додатками.
- ПП має зберігати записи сеансу в криптографічно захищеному репозиторії, який запобігає їх маніпуляції. Жоден із користувачів, включаючи системного адміністратора, не може вплинути на цілісність збережених записів (включаючи неможливість видалити їх протягом певного періоду зберігання даних).
- ПП має забезпечувати функціональність обмеження доступу до цільових систем та створення списків допустимих та неприпустимих команд, що виконуються через SSH.
- ПП має забезпечувати підзвітність у разі використання спільного облікового запису більше ніж одним користувачем одночасно.
- ПП має використовувати механізми індексації метаданих (у записах сеансів) для забезпечення швидкого пошуку записаних та відстежуваних сеансів з певними ключовими словами та діями (потрібні не менш наступні механізми індексації: натискання клавіш,

відповіді вікна операційної системи, команди SQL). Не можна ідентифікувати метадані за допомогою механізму розпізнавання тексту.

- Проксі-модуль ПП, має підтримувати функцію Microsoft Remote App для публікації програм. Скрипти посилення повинні бути доставлені постачальником PAM та виконані під час інсталяції продукту.
- ПП повинна класифікувати записані сеанси користувачів із заздалегідь визначеними рівнями ризику. Ризик слід визначати на основі набору політик, функцій/команд, виявлених під час сеансу, та ваги, призначеної їм. Ризик повинен автоматично аналізуватися під час поточних сесій. Інформація про рівень ризику, призначеного сеансу, має відображатися як на консолі моніторингу сеансу, так і в інтерфейсі панелі керування інцидентами безпеки. Адміністратор ПП повинен мати можливість вказати, які дії, що виконуються користувачем, повинні бути автоматично припинені або припинені
- ПП повинна збирати та аналізувати дані про активність користувачів із зовнішніх SIEM-систем, а також підтримуватися як мінімум такі рішення: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee та операційні системи: rsyslog (з систем Unix/Linux), Windows Event Forwarder (з систем Windows), AWS CloudTrail, додаток Azure Function
- ПП повинна виявляти інциденти, коли привілейовані облікові дані використовуються для безпосереднього з'єднання з цільовою системою (без отримання пароля з безпечного сховища), а також подію, коли в системі створюється новий привілейований обліковий запис. Для подій безпеки, описаних у цьому пункті, ПП повинно надавати автоматичні процедури виправлення не менше, ніж: скидання пароля для привілейованого облікового запису при виникненні інциденту безпеки, автоматична (некерована) реєстрація облікового запису та автоматичні таємні переговори.

4.10.Вимоги до гарантійної підтримки

- Надання консультацій по телефону, електронній пошті та на сайті підтримки Виробника щодо питань встановлення, налаштування та експлуатації системи з понеділка по неділю (включно) з 00.00 до 24.00 годин (цілодобово).
- Постійний (24x7) 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 (24x7) авторизований доступ до сайту Виробника.
- Можливість реєстрації сервісних випадків в режимі 24x7 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 припинення дії попередньої ліцензії 25.12.2026;
- паперовий примірник Звіту щодо результатів аналізу 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.

Посилання на конкретне найменування програмної продукції в цих технічних вимогах обумовлено її поточним використанням в процесі дослідної експлуатації підсистем Центру моніторингу та кібербезпеки міських сервісів.

Ініціатор закупівлі  **Є.В. Буржинський**

Додаток 2

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

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії виконаного договору та документів, що підтверджують його виконання. ** Під аналогічним договором розуміється договір подібний за предметом закупівлі за період з 2014 року по теперішній час. Якщо в довідці учасник вказує декілька аналогічних договорів, то всі документи щодо підтвердження виконання таких договорів надаються щодо кожного із вказаних в довідці договорів.*

Для належного захисту інтересів Замовника щодо авторизованого джерела постачання за даними торгами Учасник повинен надати Авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника, дистриб'ютора в Україні, який підтверджує наявність у Учасника права на здійснення продажу запропонованого Учасником ліцензійного програмного забезпечення.

Учасник у технічній частині своєї пропозиції повинен надати інформаційний лист або довідку в довільній формі про можливість поставки товару відповідно до технічної специфікації із зазначенням конкретної назви програмної продукції, що пропонується учасником, та терміну її дії.

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **Є.В. Буржинський**

Додаток 3

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 36
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 «22» квітня 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 12.12.2024 № 449/10257) (далі – Програма), у 2026 році, а саме:

1.1.проєкт технічних вимог до закупівлі «Модернізація інформаційно-комунікаційної системи «Платформа цифрових мобільних сервісів «Київ цифровий» № 2-2026» (пункт 6.1 «Створення, розвиток, впровадження та модернізація цифрових сервісів, систем та реєстрів даних» переліку завдань і заходів Програми);

1.2. доопрацьований проєкт технічних вимог до закупівлі «Ліцензія на право використання інформаційно-аналітичної системи пошуку і обробки інформації у сфері господарської та інших видів діяльності CLARITY PROJECT» (пункт 6.3 «Створення, розвиток, модернізація, функціональне розширення та забезпечення безперервності функціонування міської інфраструктури обробки даних, оренда дата-центрів, придбання комп'ютерного обладнання, оргтехніки, програмного забезпечення та ліцензій на відповідні програмні продукти» переліку завдань і заходів Програми) у частині уточнення технічних вимог та назви закупівлі;

1.3. проєкт технічних вимог до закупівлі «Супровід та підтримка електронної комунікаційної системи «Мережа транкінгового радіозв'язку за технологією «TETRA» (пункт 6.4 «Супровід, проведення ремонтів, обслуговування та технічна підтримка мережевої інфраструктури, сервісної мережевої інфраструктури, інфраструктури обробки даних, платформи Інтернету речей (IoT), мереж доступу, радіомереж, систем отримання та передачі інформації на базі LPWAN та інших сучасних технологій зв'язку, системи відеоконференцзв'язку, комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, систем моніторингу та кібербезпеки міських сервісів, інформаційно-комунікаційних, інформаційних (автоматизованих), електронних комунікаційних систем, платформ, вебпорталів та сервісів, обладнання, технічних засобів, модулів, програмно-апаратних комплексів, програмного забезпечення, ліцензій» переліку завдань і заходів Програми);

1.4. доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми) у частині уточнення технічних вимог.

2. Різне.

По пункту 1.1 питання 1

СЛУХАЛИ:

Н. Йожикова, який поінформував про необхідність модернізації інформаційно-комунікаційної системи «Платформа цифрових мобільних сервісів «Київ цифровий» (далі – ІКС ПЦМС «Київ цифровий»), складовими частинами якої є мобільний додаток «Київ цифровий» та мобільний додаток «АРМ інспектора з паркування», для удосконалення мобільного додатка «Київ цифровий» шляхом розширення функціональних можливостей адміністративної панелі ІКС ПЦМС «Київ цифровий» для покращення зручності його використання користувачами, зокрема модернізація сервісу «ОСББ»; створення сервісу «Читацький квиток»; розширення функціональних можливостей мобільного додатка «АРМ інспектора з паркування»; розширення функціональних можливостей ІКС ПЦМС «Київ цифровий» для оптимізації діяльності інспекції з паркування; відображення інформації про чинний поліс страхування транспортного засобу; підключення чат-бота в мобільному додатку «Київ цифровий» шляхом налаштування електронної інформаційної взаємодії з інформаційно-комунікаційною системою «Інформаційний бот»; оптимізація мобільного додатка «Київ цифровий» для можливості роботи через супутниковий зв'язок direct to cell тощо та представив проєкт технічних вимог до закупівлі «Модернізація інформаційно-комунікаційної системи «Платформа

цифрових мобільних сервісів «Київ цифровий» № 2-2026» (пункт 6.1 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: А. Жежера.

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Головний інформаційно-обчислювальний центр» під час процедури закупівлі «Модернізація інформаційно-комунікаційної системи «Платформа цифрових мобільних сервісів «Київ цифровий» № 2-2026» (пункт 6.1 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:

В. Тихонова, який поінформував, що у працівників Департаменту економіки та інвестицій виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час виконання покладених на них завдань виникає потреба у використанні інформаційно-аналітичної системи пошуку і обробки інформації у сфері господарської та інших видів діяльності CLARITY PROJECT. Ураховуючи відповідний запит щодо придбання ліцензій необхідного програмного забезпечення, представив доопрацьований проєкт технічних вимог до закупівлі «Ліцензія на право використання інформаційно-аналітичної системи пошуку і обробки інформації у сфері господарської та інших видів діяльності CLARITY PROJECT» (пункт 6.3 переліку завдань і заходів Програми) у частині уточнення технічних вимог та назви закупівлі.

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

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Ліцензія на право використання інформаційно-аналітичної системи пошуку і обробки інформації у сфері господарської та інших видів діяльності CLARITY PROJECT» (пункт 6.3 переліку завдань і заходів Програми) використовувати доопрацьований проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.3 питання 1

СЛУХАЛИ:

В. Тихонова, який поінформував про необхідність забезпечення супроводу та підтримки електронної комунікаційної системи «Мережа транкінгового радіозв'язку за технологією «TETRA» для забезпечення її надійної та безперебійної

роботи, своєчасного виявлення і усунення несправностей та представив проєкт технічних вимог до закупівлі «Супровід та підтримка електронної комунікаційної системи «Мережа транкінгового радіозв'язку за технологією «TETRA» (пункт 6.4 переліку завдань і заходів Програми).

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

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Супровід та підтримка електронної комунікаційної системи «Мережа транкінгового радіозв'язку за технологією «TETRA» (пункт 6.4 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.4 питання 1

СЛУХАЛИ:

В. Тихонова, який поінформував, що для забезпечення контролю доступу до привілейованих облікових записів, зниження ризиків їх компрометації шляхом автоматизованої ротації облікових даних і приховування паролів, а також підвищення рівня прозорості та безпеки за рахунок аудиту, запису та моніторингу дій користувачів під час роботи з привілейованими сесіями необхідно придбати відповідну програмну продукцію для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки (з послугою зі встановлення та налаштування програмної продукції), та представив доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: А. Жежера.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для підсистеми управління привілейованим доступом інформаційно-комунікаційної системи моніторингу та кібербезпеки» (пункт 6.5 переліку завдань і заходів Програми) використовувати доопрацьований проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

Протокол вела Тамара САМОЙЛЕНКО

CYBERPRO
AUDIT AND PROTECTION

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

Вих.№ 2026-04-28/1
від 28 квітня 2026 р.

Спеціалізоване комунальне
підприємство «Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

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

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

№	Найменування	Кіль-кість	Од. виміру	Ціна з ПДВ, грн	Вартість з ПДВ, грн
1	Програмна продукція для підсистеми управління привілейованим доступом у складі: Програмна продукція (ліцензійне програмне забезпечення) Privileged Standard User Subscription (Credential Protection; Session Isolation; Recording; Detection; Remote VPN-less Access; Adaptive MFA and risk-based Authentication; Adaptive Application Access; For IT users. Price per user per month with Extended Premium Support. Term: 12 months.) (70 шт.), Програмна продукція (ліцензійне програмне забезпечення) PAM Remote Vendor User with Advanced Remote Access (Includes external Privileged User, biometric MFA, remote VPN-less access, session isolation and recording through Privileged Session Manager. Price per user per month. Backend Vault is the PAM on-premises Vault with Extended Premium Support. Term: 12 months.) (130 шт.)	1	К-т	9 570 938,88	9 570 938,88
2	Послуга зі встановлення та налаштування Програмної продукції	1	послуга	1 115 061,12	1 115 061,12
				Разом з ПДВ, грн: 10 686 000,00	
				ПДВ, грн: 1 781 000,00	

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

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/291
від 28.04 2026 р.

ТОВ «ВІ ЄМ ДЖІ»

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

Вих.№54 від 28.04.2026

СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 075/2-638 від 24.04.2026 надаємо вартість на Програмну продукцію для підсистеми управління привілейованим доступом (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 управління привілейованим доступом у складі: Програмна продукція Privileged Standard User Subscription (Credential Protection; Session Isolation; Recording; Detection; Remote VPN-less Access; Adaptive MFA and risk-based Authentication; Adaptive Application Access; For IT users. Price per user per month with Extended Premium Support. Term: 12 months.) -70 шт. (PRIV-STANDARD-USER-SUBS-EXT-SUP) Програмна продукція PAM Remote Vendor User with Advanced Remote Access (Includes external Privileged User, biometric MFA, remote VPN-less access, session isolation and recording through Privileged Session Manager. Price per user per month. Backend Vault is the PAM on-premises Vault with Extended Premium Support. Term: 12 months.) - 130 шт. (EXT-VENDOR-USER-SUBS-EXT-SUP)	1	комплект	8 042 795,00	8 042 795,00
2	Послуга зі встановлення та налаштування ПП	1	послуга	944 705,00	944 705,00
				Всього грн, без ПДВ	**8 987 500,00**
				Податок на додану вартість (20%), грн	1 797 500,00
				Загальна сума грн, з ПДВ	**10 785 000,00**

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

Комерційний Директор Комар Олександр

Комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
вхідний № 075/2/1289
28.04 2026

ТОВ «АБКОММУНІКЕЙШЕН»
вул. Сагайдачного Петра, буд.33, Київ, 04070
код ЄДРПОУ 44286426
тел. 044-359-00-98
email: info@abcommunication.com.ua

Київ

Вих.№ 160/26 від 28.04.2026 рік

СКП «КИЇВТЕЛЕСЕРВІС»

Комерційна пропозиція

За Вашим запитом вартості на Програмну продукцію для підсистеми управління привілейованим доступом (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48730000-4 Пакети програмного забезпечення для забезпечення безпеки):

№ з/п	Найменування	Од. виміру	Кількість	Вартість без ПДВ, грн.	Загальна вартість, грн., без ПДВ
1	Програмна продукція для підсистеми управління привілейованим доступом у складі: Програмна продукція (ліцензійне програмне забезпечення) тип 1- Privileged Standard User Subscription (Credential Protection; Session Isolation; Recording; Detection; Remote VPN-less Access; Adaptive MFA and risk-based Authentication; Adaptive Application Access; For IT users. Price per user per month with Extended Premium Support. Term: 12 months.),70 шт.; Програмна продукція (ліцензійне програмне забезпечення) тип 2 - PAM Remote Vendor User with Advanced Remote Access (Includes external Privileged User, biometric MFA, remote VPN-less access, session isolation and recording through Privileged Session Manager. Price per user per month. Backend Vault is the PAM on-premises Vault with Extended Premium Support. Term: 12 months.), 130 шт.;	Компл.	1	8 157 565,00	8 157 565,00
2	**Послуга зі встановлення та налаштування ПП - 1 послуга**	послуга	1	967 935,00	967 935,00
ВСЬОГО, грн. без ПДВ:					**9 125 500,00**
ПДВ, 20%					**1 825 100,00**
ВСЬОГО, грн. З ПДВ:					**10 950 600,00**

З повагою Директор

ТОВ «АБКОММУНІКЕЙШЕН» **Сергій Католик**

Київська міська державна ...
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/292
Від 28.04 2026

ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ
(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

ДЕПАРТАМЕНТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

**КОМУНАЛЬНЕ ПІДПРИЄМСТВО
«ГОЛОВНИЙ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИЙ ЦЕНТР»
(КП ГІОЦ)**

*вул. Космічна, 12-А, м. Київ, 02192, тел.: (044) 366 81 05, (044) 366 81 55,
e-mail: secretari.gioc@kyivcity.gov.ua, Код ЄДРПОУ 04013755*

Виконувачу обов'язків директора
Спеціалізованого комунальне підприємство
«КИЇВТЕЛЕСЕРВІС»

Щодо потреби у ліцензуванні
підсистеми управління
привілейованим доступом

Шановний Олександре Олександровичу!

Комунальне підприємство «Головний інформаційно-обчислювальний центр» опрацювало Ваш лист від 23.03.2026 № 075/2-446, щодо надання потреби потреби у ліцензуванні підсистеми управління привілейованим доступом «CyberArk»:.

За результатами опрацювання в межах компетенції надаємо розрахунок потреби в обсягах ліцензування підсистеми управління привілейованим доступом «CyberArk»:

Найменування	Кількість
Привілейований користувач Тип 1	33
Привілейований користувач Тип 2	65

Для надання додаткової інформації фахівці Вашого підрозділу можуть звернутися в робочому порядку за консультацією до виконуючого обов'язки начальника Департаменту експлуатації програмно-апаратних комплексів Жежери Артема Сергійовича, тел. 366-81-18, електронна адреса: artem.zhezhera@kyivcity.gov.ua.

З повагою

Виконуючий обов'язки директора Костянтин ВОРОБЙОВ

ДОКУМЕНТ ІКС ЄІПК СЕД АСКОД (**ПІДПИСАНО КВАЛІФІКОВАНИМ ЕЛЕКТРОННИМ ПІДПИСОМ**)

Сертифікат 47E80D080000000000000000000000000000001
Підписувач Воробйов Костянтин Володимирович
Дійсний з 18.12.2024 11:28:47 по 17.12.2026 23:59:59

КП "Головний інформаційно-обчислювальний центр"

075/1-1087 від 27.03.2026

ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ (КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

ДЕПАРТАМЕНТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КОМУНАЛЬНЕ ПІДПРИЄМСТВО «ІНФОРМАТИКА»

(КП «ІНФОРМАТИКА»)

State Enterprise
Informatics

вул. Левка Лукієвича, 3, м. Київ, 03186 тел. (044) 366 86 55 E-mail:informatika@kmda.gov.ua
Код ЄДРПОУ 31024875

01.04.2026 № 075/3-945

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

Комунальне підприємство «Інформатика», за результатом опрацювання листа СКП «КИЇВТЕЛЕСЕРВІС» від 23.03.2026 № 075/2-446 щодо розрахунку потреби в обсягах ліцензування підсистеми управління привілейованим доступом «CyberArk» повідомляє, що станом на сьогодні потреба підприємства у ліцензіях визначена таким чином:

користувачі Типу 1 — 20;

користувачі Типу 2 — 27.

В.о. генерального директора Микола ЖАНДОРОВ

Денис Осокін
0957277302