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

Начальника відділу кібербезпеки міських сервісів Буржинського Євгена Васильовича

СЛУЖБОВА ЗАПИСКА

місто Київ «04» грудня 2025 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 ОК Центром моніторингу та кібербезпеки міських сервісів та Наказом №76 від 28.06.2024 спеціалізованого комунального підприємства "Київтелесервіс" "Про введення у дослідну експлуатацію підсистем Центру моніторингу та кібербезпеки міських сервісів".

Обґрунтування обсягів закупівлі:

Об'єм ліцензії обумовлено поточною кількістю привілейованих користувачів на об'єктах кіберзахисту, потребою КП "Інформатика "(вих. № 075/3-3250 від 25.11.2025) та КП "Головний інформаційно-обчислювальний центр" (вих. № 075/1-4967 від 04.12.2025).

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 №113 від 27.11.2025 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 11 254 235,40 (одинадцять мільйонів двісті п'ятдесят чотири тисячі двісті тридцять п'ять гривень сорок 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 – програмна продукція - 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 8 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.
4. Додаток 4. Протокол №113 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 **Є.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 (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, з послугою, пов'язаною з встановленням та налаштуванням програмної продукції, що закуповуються.

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

1.3. Мета придбання засобу інформатизації.

Забезпечення функціонування підсистеми управління привілейованим доступом 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

- 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:
- 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;
- 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 *	Обсяг ліцензії	Кількість
1	Програмна продукція (ліцензійне програмне забезпечення) *Privileged Standard User with Added Enterprise Advanced - Credential Protection; Session Isolation; Recording; Detection; Remote VPN-less Access; Adaptive MFA and risk-based Authentication; Adaptive Application Access*	70 од. строком дії на 1 рік *(BVA-CKPRIV-STANDARD-USER-SUBS002-AS)*	1
2	Програмна продукція (ліцензійне програмне забезпечення) *Includes external Privileged User, biometric MFA, remote VPN-less access, session isolation and recording through Privileged Session Manager, Backend Vault is the PAM on-premises Vault.*	130 од. строком дії на 1 рік *(BVA-CKEXT-VENDOR-USER-SUBS002-AS)*	1
3	Програмна продукція (ліцензійне програмне забезпечення) *CyberArk Service Units Standard Edition.*	1 од. строком дії на 1 рік *(B2-CA-SRVU)*	1

- **Послуга, пов'язана з програмною продукцією - 1 послуга.**

**Посилання на конкретне найменування програмної продукції обумовлено її поточним використанням для забезпечення централізованого контролю доступу до привілейованих облікових записів ОК Центром моніторингу та кібербезпеки міських сервісів та Наказом №76 від 28.06.2024 спеціалізованого комунального підприємства "Київтелесервіс" "Про введення у дослідну експлуатацію підсистем Центру моніторингу та кібербезпеки міських сервісів".*

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

- 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 з встановлення та налаштування ПП:

Таблиця 2. Склад послуги

№ з/п	Вимоги
1	Проведення аналізу стану ПП CyberArk з урахуванням всіх модулів на предмет конфліктів конфігурацій. Усунення несправностей, оптимізація продуктивності та робочих процесів при використанні ПП. Результати проведеного аналізу мають бути оформлені звітом з наступними розділами: 1. Загальні 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. План тестування програмної продукції з урахуванням можливого оновлення ПП.

2	Налаштування інтеграції з Remote VPN-less Access для автоматичного створення та видалення облікових записів (далі - ОЗ)зовнішніх користувачів на наземних компонентах ПП. 1. Забезпечити налаштування автоматичного створення ОЗ зовнішніх користувачів через CyberArk Remote VPN-less Access; 2. Забезпечити автоматичне видалення або деактивацію ОЗ зовнішніх користувачів після завершення строку доступу; 3. ПП має підтримувати прив'язку ОЗ зовнішнього користувача до відповідних сховищ\рівня привілеїв, згідно з ролями. 4. Забезпечити автоматичну синхронізацію: a. даних профілю зовнішнього користувача (ім'я, компанія, контактні дані); b. прав доступу; c. термінів дії. 5. Передбачити можливість деактивації автоматичного керування ОЗ зовнішнього користувача, адміністратором ПП.
3	Налаштування в ПП процесу ротації паролів та\або ключів привілейованих ОЗ, підготовка відповідної інструкції для адміністраторів, що буде включати не менше 4 типів ОЗ. 1. Забезпечити підтримку ротації паролів для наступних типів ОЗ: a. Windows локальний ОЗ; b. Windows доменний ОЗ; c. UNIX ОЗ з паролем; d. UNIX ОЗ з SSH ключем. 2. Реалізувати політики ротації паролів: a. періодичної (за розкладом згідно політик безпеки); b. ручної (за запитом); 3. Забезпечити автоматичне оновлення паролів у відповідних сховищах. 4. Ротація паролів не повинна порушувати роботу систем, на яких використовуються відповідні ОЗ: a. під час ротації має виконуватись тестування нового пароля; b. у разі помилки має виконуватись повернення попереднього значення.
4.	Побудова інтеграції ПП з AD/LDAP: 1. Вибір оптимального механізму інтеграції, згідно наявності у Виробника інструментів, що дозволяють забезпечити стабільну та безпечну взаємодію без розробки індивідуальних API-інтеграцій. 2. Тестування інтеграційних зв'язків на предмет сталої роботи 3. Налаштування автоматизованого додавання та реєстрації ОЗ з AD шляхом створення не менше 3 правил, в залежності від: a. рівня привілеїв ОЗ; b. ім'я ОЗ; c. адреса/назва сервера; d. тип операційної системи.

5.	Розробити не менше 5 нестандартних інтеграцій між ПП CyberArk та зовнішніми системами/сервісами із використанням Web application for PSM, які не вбудовані за замовчуванням у штатний функціонал ПП.
6.	Налаштування моніторингу компонентів, звітності та візуалізації ПП: 1. Забезпечення безперервного контролю доступності та працездатності основних компонентів ПП CyberArk (Vault, PVWA, CPM, PSM, PSM для SSH, PTA, Remote VPN-less Access). 2. Налаштування автоматичного сповіщення (email) у разі зупинки компонентів, деградації їх функцій або відхилень у роботі. 3. Тестування працездатності системи сповіщень після впровадження. 4. Розробка та налаштування не менше 5 типів звітів, що охоплюють такі напрями: a. активність користувачів системи; b. CPM статус для привілейованих ОЗ; c. активні/неактивні сховища; d. наявні привілейовані ОЗ; e. звіт по наявним правам доступу. 5. Підготовка та налаштування не менше 3 інтерактивних дашбордів для відображення ключових показників роботи ПП CyberArk, зокрема: a. стан компонентів ПП, b. статистика ротації паролів, c. статистика активності платформ.

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.
- Постачальник повинен надати інструмент, доступний для вільного користування, що забезпечує функціонал автоматизації процесу створення компонентів підключення для нових / невідомих веб-додатків. Додаток повинен мати можливість записувати процес підключення кінцевого користувача до захищеного додатку, визначати веб-форми / поля, які використовуються для введення облікових даних користувача до програми, та на основі запису автоматично генерувати відповідний сценарій для автоматичного встановлення веб-сеансу.
- 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 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 підписання Сторонами акту передачі-приймання ПП з подальшим її терміном дії протягом 12 місяців;
- 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.*

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 4

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 113

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки

м. Київ «27» листопада 2025 року

ПРИСУТНІ:

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

проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми управління привілейованим доступом» (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 питанню 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що для забезпечення функціонування підсистеми управління привілейованим доступом 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, необхідно придбати відповідну програмну продукцію та представив проєкт технічних вимог до закупівлі «Програмна продукція для підсистеми управління привілейованим доступом» (пункт 6.5 переліку завдань і заходів Програми).

В обговоренні проєкту технічних вимог брали участь: Д. Цвігун.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для підсистеми управління привілейованим доступом» (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

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

Вих№ 120325/4 від 03.12.2025
На № 446-2025 від 28.11.2025

Спеціалізованому комунальному підприємству
«Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Товариство з обмеженою відповідальністю «ОПТІДАТА» надає комерційну пропозицію за Вашим запитом 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 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. Term: 12 months),70 шт.; 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. Term: 12 months), 130 шт.; Програмна продукція CyberArk Service Units Standard Edition	Компл.	1	7 581 935,00	7 581 935,00
2	Послуга, пов'язана з програмною продукцією у складі: Консультаційні послуги з питань інформатизації щодо адміністрування ІТ-рішень CyberArk ; Консультаційні послуги з питань інформатизації щодо керування інтеграціями ІТ-рішень CyberArk; Консультаційні послуги з питань інформатизації щодо моніторингу і звітності ІТ-рішень CyberArk; Консультаційні послуги з питань інформатизації щодо діагностики та усунення несправностей ІТ-рішень CyberArk;	послуга	1	1 559 875,00	1 559 875,00

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

Opti Data
Enforce your security

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області,
АТ «Ощадбанк» ТВБВ 10026/020, МФО:
322669, ЄДРПОУ: 39693067

	Консультаційні послуги з питань інформатизації щодо рекомендацій з експлуатації IT-рішень CyberArk; Консультаційні послуги з питань інформатизації щодо планування та підготовки до інтеграції IT-рішень CyberArk з додатковими системами (до 10 систем.				
				Всього, грн. без ПДВ:	9 141 810,00
				ПДВ, 20%:	1 828 362,00
				Всього, грн. З ПДВ:	**10 970 172,00**

Всього: 10 970 172,00 грн. (десять мільйонів дев'ятсот сімдесят тисяч сто сімдесят дві грн. 00 коп.)

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

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

ТОВ «ВІ ЄМ ДЖІ»

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

Вих.№256 від 03.12.2025

СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на ваш запит № 448-2025 від 28.11.2025 надаємо вартість на Програмна продукція 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. Term: 12 months)-70 шт. 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. Term: 12 months)- 130 шт. Програмна продукція CyberArk Service Units Standard Edition	1	комплект	7 812 150,00	7 812 150,00
2	Послуга, пов'язана з програмною продукцією у складі: Консультаційні послуги з питань інформатизації щодо адміністрування IT-рішень CyberArk 1 послуга; Консультаційні послуги з питань інформатизації щодо керування інтеграціями IT-рішень CyberArk 1 послуга; Консультаційні послуги з питань інформатизації щодо моніторингу і звітності IT-рішень CyberArk 1 послуга; Консультаційні послуги з питань інформатизації щодо діагностики та усунення несправностей IT-рішень CyberArk 1 послуга; Консультаційні послуги з питань інформатизації щодо рекомендацій з експлуатації IT-рішень CyberArk 1 послуга; Консультаційні послуги з питань інформатизації щодо планування та підготовки до інтеграції IT-рішень CyberArk з додатковими системами (до 10 систем) 1 послуга.	1	послуга	1 604 500,00	1 604 500,00
				Всього грн, без ПДВ	9 416 650,00
				Податок на додану вартість (20%), грн	1 883 330,00
				Загальна сума грн, з ПДВ	11 299 980,00

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 № 3337/2025
Від 03.12 2025 р.

CYBERPRO
AUDIT AND PROTECTION

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

Вих.№2025-12-03/3
від 3 грудня 2025 року

СКП «КИЇВТЕЛЕСЕРВІС»

ЦІНОВА ПРОПОЗИЦІЯ
Програмна продукція для підсистеми управління привілейованим доступом

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

За Вашим запитом №447-2025 від 28.11.2025 року надаємо цінову пропозицію

Найменування товару/послуги	Кіль-кість	Одиниці виміру	Ціна без ПДВ, грн	Вартість без ПДВ, грн
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. Term: 12 months) (70 шт.), 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. Term: 12 months) - (130 шт.), Програмна продукція CyberArk Service Units – (1 шт.)	1	комплект	7 942 975,00	7 942 975,00
Послуга, пов'язана з програмною продукцією у складі: - Консультаційні послуги з питань інформатизації щодо адміністрування IT-рішень CyberArk 1 послуга; - Консультаційні послуги з питань інформатизації щодо керування інтеграціями IT-рішень CyberArk 1 послуга; - Консультаційні послуги з питань інформатизації щодо моніторингу і звітності IT-рішень CyberArk 1 послуга; - Консультаційні послуги з питань інформатизації щодо діагностики та усунення несправностей IT-рішень CyberArk 1 послуга; - Консультаційні послуги з питань інформатизації щодо рекомендацій з експлуатації IT-рішень CyberArk 1 послуга; - Консультаційні послуги з питань інформатизації щодо планування та підготовки до інтеграції IT-рішень CyberArk з додатковими системами (до 10 систем) 1 послуга	1	послуга	1 634 153,50	1 634 153,50

Загальна вартість: 11 492 554,20 грн (одинадцять мільйонів чотириста дев'яносто дві тисячі п'ятсот п'ятдесят чотири гривні 20 копійок, у т.ч. ПДВ (20%) 1 915 425.70 грн. (один мільйон дев'ятсот п'ятнадцять тисяч чотириста двадцять п'ять гривень 70 копійок).

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 3351/2025
Від 03.12 2025 р.

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

Інформація про електронні підписи (ЕП)

№ документа 075-2630 **Дата реєстрації** 27.11.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 27.11.2025 (Протокол № 113 від 27.11.2025)

Кількість файлів: 2 **Кількість ЕП:** 14

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
27.11.2025 № 075-2630

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Жучков Василь Анатолійович **Кількість ЕП:** 2	27.11.2025 13:34:14 ; 27.11.2025 13:34:17 ;	27.11.2025 13:34:17 Погодив;	27.11.2025 13:34:17 Погодив
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 2	27.11.2025 10:29:41 ; 27.11.2025 10:29:43 ;	27.11.2025 10:29:43 Погодив;	27.11.2025 10:29:43 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 2	27.11.2025 09:57:34 ; 27.11.2025 09:57:35 ;	27.11.2025 09:57:36 Погодив;	27.11.2025 09:57:35
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 2	27.11.2025 09:52:43 ; 27.11.2025 09:52:45 ;	27.11.2025 09:52:45 Погодив;	27.11.2025 09:52:45 Погодив
Поліщук Олег Федорович **Кількість ЕП:** 2	27.11.2025 09:32:15 ; 27.11.2025 09:32:16 ;	27.11.2025 09:32:16 Погодив;	27.11.2025 09:32:16 Погодив

ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 2	27.11.2025 08:54:49 ; 27.11.2025 08:54:49 ;	27.11.2025 08:54:49 Погодив;	27.11.2025 08:54:49 Погодив
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 2	27.11.2025 08:54:49 ; 27.11.2025 08:54:49 ;	27.11.2025 08:54:49 Погодив;	27.11.2025 08:54:49 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 2	27.11.2025 08:53:22 ; 27.11.2025 08:53:22 ;	27.11.2025 08:53:22 Погодив;	27.11.2025 08:53:22 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 2	27.11.2025 08:53:22 ; 27.11.2025 08:53:22 ;	27.11.2025 08:53:22 Погодив;	27.11.2025 08:53:22 Погодив