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

Начальника центру моніторингу та кібербезпеки міських сервісів Цвєткова Василя Костянтиновича

СЛУЖБОВА ЗАПИСКА

місто Київ «24» вересня 2026 року

Конкретна назва предмета закупівлі – **Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки (72220000-3 Консультаційні послуги з питань систем та з технічних питань (72222300-0 Послуги у сфері інформаційних технологій)).**

Обґрунтування доцільності закупівлі:

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

З метою забезпечення готовності визначених інформаційно-комунікаційних систем спеціалізованого комунального підприємства «Київтелесервіс» (далі - СКП «Київтелесервіс») до первинної авторизації з безпеки.

Обґрунтування обсягів закупівлі:

Обсяг послуг обумовлено кількістю інформаційно-комунікаційних систем, що підлягають первинній авторизації з безпеки, а також обов'язковістю проходження такої авторизації відповідно до статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах», процедурний механізм реалізації якої визначено Порядком авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженим постановою Кабінету Міністрів України від 18.06.2025 № 712.

Обґрунтування якісних характеристик закупівлі:

Технічні вимоги до предмета закупівлі розроблені з урахуванням необхідності проходження авторизації, про що зазначено вище, на виконання заходу 6.5 переліку завдань та заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки з урахуванням фактичних характеристик та складу інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки, та рекомендовані до використання протоколом № 87 від 04.09.2026 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 СКП «Київтелесервіс», розробленого на основі Примірної методики визначення очікуваної вартості предмета закупівлі (наказ Мінекономіки від 18.02.2020 № 275) та затвердженого наказом СКП «Київтелесервіс» від 21.08.2023 № 68, з використанням методу порівняння ринкових цін у спосіб, що передбачає направлення не менше 3-х письмових запитів цінових пропозицій (електронною поштою) виробникам, офіційним представникам та дилерам, постачальникам конкретного товару, надавачам послуг.

СКП «Київтелесервіс» було направлено 10 запитів цінових пропозицій підприємствам-учасникам ринку, що надають схожі послуги, та отримано три відповіді. Комерційні пропозиції надано двома підприємствами. Відповідь від третього підприємства (ДП «ІНФОТЕХ») не містить ціни, оскільки виробничий план підприємства уже затверджений до кінця 2026 року, у зв'язку з чим

підприємство не має можливості сформувати обґрунтовану орієнтовну вартість виконання зазначеного комплексу робіт та фактично їх виконати.

У висновку, згідно проведеного Ініціатором закупівлі моніторингу цін шляхом направлення запитів учасникам ринку, очікувана вартість закупівлі становить 4 992 500,00 грн. (чотири мільйони дев'ятсот дев'яносто дві тисячі п'ятсот гривень нуль копійок) з ПДВ, що є середнім значенням отриманих комерційних пропозицій.

Використання загальнодоступної інформації про ціни на послуги з авторизації з безпеки, що міститься у відкритих джерелах (зокрема на спеціалізованих торговельних майданчиках, в електронних каталогах, рекламних матеріалах, прайс-листах, в електронній системі закупівель «Prozorro»), є неможливим, оскільки предмет закупівлі є індивідуальним для кожної системи: обсяг та вартість робіт з авторизації залежать від складу, архітектури та кількості підсистем конкретної інформаційно-комунікаційної системи, тому наявні у відкритих джерелах цінові показники за подібними закупівлями не є репрезентативними для визначення очікуваної вартості предмета цієї закупівлі.

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 – послуга.

Кількість – 2 послуги.

Строк надання послуг – до 25.12.2026.

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

Зазначення точної адреси місця поставки товару несе загрозу безпеці замовника.

Додатки:

1. Додаток 1. Технічні вимоги на 10 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Протокол № 87 засідання робочої групи на 3 арк.
4. Додаток 4. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 4 арк.

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

«ПОГОДЖЕНО»:

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

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

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

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

Заступник начальника відділу з фінансових питань _____ **Л. М. Задорожна**

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

Додаток 1

ТЕХНІЧНІ ВИМОГИ

Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки (72220000-3 Консультаційні послуги з питань систем та з технічних питань (72222300-0 Послуги у сфері інформаційних технологій))

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ЗМІСТ РОБІТ

1.1 Підстава для розроблення Технічних вимог

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

1.2 Найменування систем, для яких надаються послуги

Послуги з первинної авторизації з безпеки надаються для:
- інформаційно-комунікаційної системи «Міська мережева інфраструктура» (далі – ІКС «ММІ»);
- інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС МК),

далі разом – визначені Системи.

1.3 Загальні вимоги

Первинна авторизація з безпеки визначених систем здійснюється відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (далі – Порядок авторизації), затвердженого постановою Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» (далі – Постанова № 712).

Первинна авторизація з безпеки проводиться для кожної з визначених Систем окремо, з метою прийняття рішення щодо можливості функціонування (експлуатації) відповідної Системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту.

1.4 Мета отримання Послуг

Метою отримання Послуг є забезпечення готовності визначених Систем до первинної авторизації з безпеки – розроблення та впровадження цільового профілю безпеки (далі – ЦПБ) кожної з визначених Систем, підготовка повного комплекту документації, необхідної для оцінювання дотримання вимог цільового профілю безпеки, та супроводження процедури подання матеріалів на авторизацію до Адміністрації Держспецзв'язку відповідно до Порядку авторизації.

1.5 Цілі отримання Послуг

Цілями отримання Послуг є:
- проведення аналізу середовища функціонування визначених Систем та наявної документації;
- проведення аналізу (категоріювання) інформації, яка обробляється у кожній з визначених Систем, та визначення категорії критичності визначених Систем;
- проведення оцінки ризиків інформаційної безпеки визначених Систем;
- розроблення та затвердження цільового профілю безпеки та політики безпеки інформації для кожної з визначених Систем;

– виконання вимог цільового профілю безпеки визначених Систем та впровадження заходів захисту інформації;

– організація оцінювання дотримання вимог цільового профілю безпеки визначених Систем незалежним суб'єктом оцінювання;

– підготовка та супроводження процесу внесення даних щодо авторизації до переліку авторизованих систем з безпеки в Адміністрації Держспецзв'язку.

1.6 Перелік документів, які мають враховуватися під час надання послуг

Надання послуг з авторизації з безпеки ІКС «ММІ» та ІКС МК має відповідати вимогам чинних нормативно-правових актів, стандартів, документів, а саме:

– Закону України «Про інформацію»;

– Закону України «Про доступ до публічної інформації»;

– Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

– Закону України «Про основні засади забезпечення кібербезпеки України»;

– Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»;

– Указу Президента України від 27.09.1999 № 1229/99 «Про Положення про технічний захист інформації в Україні»;

– постанови Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;

– постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем» (у редакції постанови Кабінету Міністрів України від 26.11.2025 № 1531);

– постанови Кабінету Міністрів України від 31.12.2025 № 1799 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури»;

– рішення Київської міської ради від 07.12.2023 № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки» (у редакції рішення Київської міської ради від 14.05.2026 № 604/11071);

– НД ТЗІ 2.3-025-24 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»;

– НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці, затверджено Наказом Адміністрації Держспецзв'язку від 26.04.2021 № 268;

– НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації», затвердженому наказом Адміністрації Держспецзв'язку від 23.03.2021 № 162;

– НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем, затвердженому наказом Адміністрації Держспецзв'язку від 30.04.2024 № 234;

– НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем, затвердженому наказом Адміністрації Держспецзв'язку від 15.02.2021 № 88;

– наказу Адміністрації Держспецзв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація»;

– наказу Адміністрації Держспецзв'язку від 02.07.2025 № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація»;

– наказу Адміністрації Держспецзв'язку від 11.07.2025 № 438 «Про затвердження Вимог до юридичних осіб, фізичних осіб-підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;

– наказу Адміністрації Держспецзв'язку від 08.12.2025 № 810 «Про затвердження рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи»;

– наказу Адміністрації Держспецзв'язку від 08.12.2025 № 811 «Про затвердження рекомендацій з

розроблення цільового профілю безпеки системи»;

– NIST SP 800-30 Rev.1 «Guide for Conducting Risk Assessments» (або еквівалент).

Цей перелік нормативно-правових актів, стандартів, документів не є вичерпним і може бути доповнений та уточнений.

2 ХАРАКТЕРИСТИКА СИСТЕМ

2.1 Характеристика ІКС «ММІ»

2.1.1 Призначення ІКС «ММІ»

ІКС «ММІ» призначена для формування єдиного середовища для безпечного й ефективного обміну інформацією між користувачами ІКС «ММІ», забезпечення та створення належних умов для захисту даних, у тому числі з використанням технологій хмарних обчислень, а також забезпечення інфраструктурних потреб міста Києва в розвитку інформаційного суспільства, формуванні та використанні міських електронних інформаційних ресурсів, упровадженні сучасних інформаційних та інформаційно-комунікаційних технологій, для реалізації повноважень і виконання покладених на органи місцевого самоврядування функцій.

Завданнями та функціями ІКС «ММІ» є забезпечення:

– функціонування єдиної електронної комунікаційної мережі органів місцевого самоврядування міста Києва для реалізації повноважень і виконання покладених на них функцій (далі – електронна комунікаційна мережа);

– безпечного й ефективного обміну інформацією між користувачами ІКС «ММІ», у тому числі з використанням технологій хмарних обчислень;

– створення умов для розвитку, доступності та використання електронних комунікаційних мереж високої і надвисокої пропускної здатності, у тому числі мереж фіксованого, мобільного зв'язку та бездротового доступу, а також електронних комунікаційних послуг, універсальних електронних комунікаційних послуг та усіх видів наявного електрозв'язку;

– автентифікації та контролю доступу до ІКС «ММІ» користувачів ІКС «ММІ»;

– сталості електронної комунікаційної мережі;

– управління та моніторингу якості електронних комунікаційних послуг;

– взаємодії із суб'єктами забезпечення кібербезпеки;

– безпеки електронних комунікаційних мереж і послуг;

– визначення та локалізація несправностей у роботі технічних засобів електронних комунікацій ІКС «ММІ»;

– організації каналів передачі даних і забезпечення ними, зокрема систем відеоспостереження, центру обробки даних (міського дата-центру), інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем користувачів ІКС «ММІ»;

– захисту інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом проведення організаційних заходів, упровадження засобів і методів технічного та криптографічного захисту інформації;

– надання доступу до мережі Інтернет для користувачів ІКС «ММІ» через власний атестований захищений вузол інтернет-доступу.

2.1.2 Опис інформаційного середовища ІКС «ММІ»

В ІКС «ММІ» обробляється та зберігається інформація, вимоги щодо захисту якої встановлені Законом України «Про захист інформації в інформаційно-комунікаційних системах» та Законом України «Про інформацію».

Суб'єктами відносин у ІКС «ММІ» є:

– власник ІКС «ММІ»;

– розпорядник ІКС «ММІ»;

– адміністратор ІКС «ММІ»;

– користувачі ІКС «ММІ».

Власником ІКС «ММІ» є територіальна громада міста Києва в особі Київської міської ради.

Розпорядником ІКС «ММІ» є виконавчий орган Київської міської ради (Київська міська державна адміністрація) в особі Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Адміністратором ІКС «ММІ» є СКП «Київтелесервіс».

Користувачами ІКС «ММІ» є секретаріат Київської міської ради, структурні підрозділи виконавчого органу Київської міської ради (Київської міської державної адміністрації), районні в місті Києві державні адміністрації, підприємства, установи та організації, що належать до комунальної власності територіальної громади міста Києва або координація діяльності яких здійснюється виконавчим органом Київської міської ради (Київської міської державної адміністрації), інші органи державної влади, які розташовані на території міста Києва та отримують доступ (підключення) до ІКС «ММІ».

2.1.3 Характеристика інформації, що оброблюється в ІКС «ММІ»

Інформація, що обробляється та зберігається в ІКС «ММІ», поділяється на два види:

- відкрита інформація;
- інформація з обмеженим доступом.

Інформацією з обмеженим доступом, що обробляється в ІКС «ММІ», є конфіденційна інформація (а саме персональні дані та технологічна інформація).

2.1.4 Суб'єкти та об'єкти доступу до інформації, що обробляється в ІКС «ММІ»

Суб'єктами доступу до інформації, що обробляється в ІКС «ММІ», є:

– адміністратори безпеки – обслуговуючий персонал, який здійснює контроль за станом безпеки в ІКС «ММІ», контролює відповідність налаштувань програмних та технічних засобів прийнятій політиці безпеки;

– системний адміністратор – обслуговуючий персонал, який забезпечує працездатність компонентів ІКС «ММІ» в цілому, проводить налаштування апаратного і програмного забезпечення ІКС «ММІ», проводить технічне обслуговування апаратного і програмного забезпечення ІКС «ММІ», проводить відновлення працездатності ІКС «ММІ», здійснює аналіз журналів реєстрації подій, здійснює моніторинг доступності вузлів, завантаження каналів зв'язку, помилок, які трапляються у каналах зв'язку, аварій на каналах зв'язку і обладнанні ІКС «ММІ».

Об'єктами доступу є:

- журнали реєстрації подій;
- засоби функціонування ІКС «ММІ»;
- засоби інтеграції із зовнішніми інформаційними системами.

2.1.5 Об'єкти захисту в ІКС «ММІ»

Об'єктами захисту в ІКС «ММІ» є:

– інформація, що обробляється в ІКС «ММІ»;

– програмне забезпечення – загальне, системне та прикладне програмне забезпечення підсистем ІКС «ММІ»;

– канали інформаційної (електронної) взаємодії з об'єктами кіберзахисту та іншими інформаційними системами;

– апаратні засоби, апаратно-програмні засоби, що забезпечують функціонування ІКС «ММІ», у тому числі, але не виключно: сервери, робочі станції, мережне обладнання, системи зберігання даних.

2.2 Характеристика ІКС МК

2.2.1 Призначення ІКС МК

ІКС МК призначена для забезпечення цілодобового моніторингу, аналізу та реагування на кіберінциденти і кібератаки, що відбуваються або можуть відбутися щодо об'єктів кіберзахисту, якими є інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні, комунікаційні та технологічні системи, електронні комунікаційні мережі, що належать до комунальної власності територіальної громади міста Києва та/або використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних послуг, електронної комерції,

електронного документообігу, а також інші об'єкти кіберзахисту відповідно до актів органів місцевого самоврядування в місті Києві (далі – ОК).

Завданнями та функціями ІКС МК є забезпечення:

– автоматизації та цифровізації безперервних процесів збору і збереження інформації про кіберінциденти та кібератаки, їх категоризацію, пріоритезацію та атрибуцію;

– моніторингу, виявлення та сповіщення про підозрілу поведінку, що може бути пов'язана з кіберінцидентом або кібератакою щодо ОК;

– автоматизації заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки, усунення їх наслідків;

– аналізу та моделювання поведінки зловмисника відповідно до відомих сценаріїв кіберінцидентів;

– систематизації та узагальнення інформації, формування статистичних і аналітичних звітів, візуалізація інформаційних панелей (дашбордів);

– пошуку та виявлення вразливостей ОК;

– захисту кінцевих точок від шкідливого програмного забезпечення;

– електронної взаємодії з ОК;

– кібербезпеки вебпорталів та вебдодатків;

– захисту інформації від несанкціонованого доступу та модифікації шляхом здійснення відповідних організаційних і технічних заходів.

2.2.2 Опис інформаційного середовища ІКС МК

В ІКС МК обробляється та зберігається інформація, вимоги щодо захисту якої встановлені Законом України «Про захист інформації в інформаційно-комунікаційних системах» та Законом України «Про інформацію».

Суб'єктами відносин у ІКС МК є:

– власник ІКС МК;

– розпорядник ІКС МК;

– адміністратор ІКС МК;

– користувачі (внутрішні та зовнішні) ІКС МК.

Власником ІКС МК є територіальна громада міста Києва в особі Київської міської ради.

Розпорядником ІКС МК є виконавчий орган Київської міської ради (Київська міська державна адміністрація) в особі Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації).

Адміністратором ІКС МК є СКП «Київтелесервіс» в особі Центру моніторингу та кібербезпеки міських сервісів.

Внутрішніми користувачами ІКС МК є співробітники Центру моніторингу та кібербезпеки міських сервісів СКП «Київтелесервіс», які в установленому порядку отримали відповідне право доступу до ІКС МК у зв'язку з виконанням службових та посадових обов'язків.

Зовнішніми користувачами ІКС МК можуть бути уповноважені адміністраторами підключених до ІКС МК ОК особи, яким в установленому порядку надається відповідне право доступу до ІКС МК або окремих її компонентів.

2.2.3 Характеристика інформації, що оброблюється в ІКС МК

Інформація, що обробляється та зберігається в ІКС МК, поділяється на два види:

– відкрита інформація;

– інформація з обмеженим доступом.

Інформацією з обмеженим доступом, що обробляється в ІКС МК, є конфіденційна інформація (а саме персональні дані та технологічна інформація).

2.2.4 Суб'єкти та об'єкти доступу до інформації, що обробляється в ІКС МК

Суб'єктами доступу до інформації, що обробляється в ІКС МК, є:

– адміністратори безпеки – мають повний доступ до налаштувань та даних ІКС МК;

– аналітики безпеки – мають доступ до подій, інцидентів, звітів та панелей моніторингу відповідно до ролі;

– уповноважені особи підключених організацій – мають обмежений доступ лише до даних, що стосуються їх власних ОК.

Об'єктами доступу є:

– бази даних подій;
– інформаційні панелі, звіти;
– записи про інциденти;
– конфігураційні дані ІКС МК.

2.2.5 Об'єкти захисту в ІКС МК

Об'єктами захисту в ІКС МК є:

– інформація, що обробляється в ІКС МК;
– програмне забезпечення – загальне, системне та прикладне програмне забезпечення підсистем ІКС МК;
– канали інформаційної (електронної) взаємодії з об'єктами кіберзахисту та іншими інформаційними системами;
– апаратні засоби, апаратно-програмні засоби, що забезпечують функціонування ІКС МК, у тому числі, але не виключно: сервери, робочі станції, мережне обладнання, системи зберігання даних;
– журнали аудиту та записи дій користувачів.

3 ВИМОГИ ДО ПРЕДМЕТУ ЗАКУПІВЛІ

3.1 Склад предмету закупівлі

Склад закупівлі:

- **Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура»** - 1 послуга *(детальний опис послуги наведено нижче)*;
- **Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи моніторингу та кібербезпеки** - 1 послуга (*детальний опис послуги наведено нижче)*.

Послуга з первинної авторизації з безпеки ІКС «ММІ» та послуга з первинної авторизації з безпеки ІКС МК включає в себе наступні роботи (окремо для кожної з визначених Систем):

1. Проведення обстеження середовищ функціонування визначених Систем та наявної документації;
2. Аналіз (категоріювання) інформації, яка обробляється у визначених Системах;
3. Оцінка ризиків безпеки визначених Систем;
4. Розроблення та затвердження для визначених Систем цільових профілів безпеки та політик безпеки інформації;
5. Виконання вимог цільових профілів безпеки визначених Систем;
6. Залучення та погодження суб'єкта оцінювання, який здійснюватиме оцінювання реалізації ЦПБ визначених Систем;
7. Оцінювання дотримання вимог цільових профілів безпеки визначених Систем;
8. Супроводження процесу внесення даних щодо авторизації до переліку авторизованих систем з безпеки в Адміністрації Держспецзв'язку.

Послуги за цими Технічними вимогами мають бути надані в повному обсязі не пізніше 25 грудня 2026 року.

3.1.1 Вимоги до проведення обстеження середовищ функціонування визначених Систем та наявної документації

Проведення обстеження середовищ функціонування визначених Систем та наявної документації здійснюється з метою визначення особливостей функціонування визначених Систем, повноти та актуальності наявної технічної та експлуатаційної документації, політик та процедур безпеки, їх дотримання та технічної реалізації, а також здійснення опису середовищ функціонування визначених Систем та виявлення в них елементів, які безпосередньо чи опосередковано можуть впливати на безпеку

інформації, виявлення взаємного впливу елементів визначених Систем, документування результатів аналізу для використання на наступних кроках авторизації з безпеки.

Під час аналізу середовищ функціонування визначених Систем мають бути проаналізовані:

- наявні в Замовника організаційно-розпорядчі документи в частині безпеки інформації;
- наявна в Замовника технічна документація визначених Систем, у тому числі в частині безпеки інформації;
- загальна структурна схема і склад визначених Систем (перелік і склад обладнання, технічних і програмних засобів визначених Систем, особливості конфігурації, архітектури тощо);
- компоненти обчислювальної системи, які містять механізми захисту інформації;
- види і характеристики каналів зв'язку;
- склад користувачів визначених Систем, їх функціональні обов'язки у визначених Системах, права різних категорій користувачів у визначених Системах, у тому числі адміністративні повноваження;
- інформація, що обробляється у визначених Системах;
- територіальне розміщення компонентів визначених Систем;
- наявність охорони території та пропускний режим, режим доступу до компонентів фізичного середовища визначених Систем.

Результати аналізу середовищ функціонування визначених Систем мають бути оформлені Виконавцем у вигляді звіту з аналізу середовищ функціонування для кожної з визначених Систем.

3.1.2 Вимоги до аналізу (категоріювання) інформації, яка обробляється у визначених Системах

Аналіз інформації, яка обробляється у визначених Системах, має виконуватися відповідно до вимог НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації», затвердженого наказом Адміністрації Держспецзв'язку від 23.03.2021 № 162.

Під час аналізу інформації потрібно:

- провести аналіз інформації, яка обробляється у визначених Системах, за результатами якого формується перелік категорій інформації, яка обробляється у визначених Системах;
- надати Замовнику пропозиції щодо визначення рівня критичності кожної категорії інформації, що обробляється у визначених Системах;
- надати Замовнику пропозиції щодо визначення категорії критичності визначених Систем.

Результати виконання цього етапу оформлюються Виконавцем у вигляді звіту з визначення категорії критичності для кожної з визначених Систем.

3.1.3 Вимоги до оцінки ризиків безпеки визначених Систем

Оцінка ризиків безпеки здійснюється відповідно до NIST SP 800-30 Rev.1 «Guide for Conducting Risk Assessments» (або еквівалентних міжнародних стандартів з оцінки ризиків), а також відповідно до вимог нормативно-правових актів України у сфері захисту інформації та вимог щодо розробки Цільових профілів безпеки. Її результати повинні бути враховані при розробленні ЦПБ визначених Систем.

Під час оцінки ризиків потрібно:

- розробити та надати Замовнику методику оцінювання ризиків інформаційної безпеки для кожної з визначених Систем;
- надати Замовнику звіт за результатами оцінювання ризиків інформаційної безпеки для кожної з визначених Систем;
- надати Замовнику план оброблення ризиків, який включає визначення рівня ризиків, їх пріоритезацію та рішення щодо їх оброблення (усунення, зменшення, прийняття або передачі) для кожної з визначених Систем.

3.1.4 Вимоги до розроблення та затвердження для визначених Систем цільових профілів безпеки та політик безпеки інформації

Виконавець розробляє цільовий профіль безпеки та політику безпеки інформації для кожної з визначених Систем.

Розроблення та затвердження для визначених Систем цільових профілів безпеки здійснюється відповідно до Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (далі – Порядок розроблення ЦПБ),

затвердженого Постановою № 712 та Рекомендацій з розроблення цільового профілю безпеки системи, затверджених наказом Адміністрації Держспецзв'язку від 08.12.2025 № 811 (далі – Рекомендації з розроблення ЦПБ).

Під час розроблення ЦПБ визначених Систем необхідно враховувати:

– базовий профіль (базові профілі) безпеки, застосовність якого визначається відповідно до видів та категорій інформації, фактично встановлених за результатами виконання п. 3.1.2 цих Технічних вимог. Для інформації, категоріювання якої відповідає сфері застосування Базового профілю безпеки системи (далі – БПБ), де обробляється відкрита або конфіденційна інформація, застосовується БПБ, затверджений наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409. Якщо за результатами обстеження та категоріювання буде встановлено обробку в визначених Системах службової інформації, додатково застосовується Базовий профіль безпеки системи, де обробляється службова інформація, затверджений наказом Адміністрації Держспецзв'язку від 02.07.2025 № 419;

– вимоги законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, зазначених у пункті 1.6;

– політики безпеки визначених Систем, їх структурно-функціональні характеристики та особливості функціонування систем, визначені технороботою та експлуатаційною документацією, звіти з обстеження середовища функціонування визначених Систем, зазначені у пункті 3.1.1;

– результати проведення оцінки (аналізу) ризиків безпеки, зазначеної в пункті 3.1.3.

Політика безпеки інформації повинна забезпечувати визначення вимог щодо впровадження кожного типу заходів захисту інформації, які визначені у переліку заходів захисту НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», затвердженого наказом Адміністрації Держспецзв'язку від 30.04.2024 № 234.

Виконавець має подати Замовнику ЦПБ визначених Систем та політики безпеки інформації на затвердження.

3.1.5 Вимоги до виконання вимог цільових профілів безпеки визначених Систем

Реалізація технічних та організаційних заходів захисту інформації, визначених затвердженим ЦПБ визначених Систем, здійснюється Замовником із залученням та за методичною підтримкою Виконавця відповідно до наступного розподілу обов'язків:

Замовник:

– виконує встановлення та налаштування засобів захисту інформації, а також налаштовує їх взаємодію з системним та/або прикладним програмним забезпеченням.

Виконавець:

– здійснює аналіз фактичного стану реалізації заходів захисту та визначає невідповідності вимогам ЦПБ;

– розробляє рекомендації та технічні вимоги щодо усунення виявлених невідповідностей;

– надає методичну підтримку фахівцям Замовника під час налаштування засобів захисту інформації;

– здійснює перевірку функціонування засобів захисту інформації після реалізації відповідних заходів;

– визначає та описує процедури функціонування комплексу засобів захисту інформації, забезпечує впровадження організаційних процедур функціонування комплексу заходів захисту інформації, які забезпечать виконання вимог цільового профілю безпеки захисту інформації;

– створює документацію функціонування комплексу засобів захисту інформації;

– визначає та описує процедури реагування на інциденти інформаційної безпеки, спрацювання засобів захисту.

Виконавець розроблює комплект документації, визначений ЦПБ визначених Систем й достатній для впровадження заходів захисту визначених ЦПБ та проходження процедури оцінювання дотримання вимог цільового профілю визначених Систем.

Мінімально необхідний комплект політик та процедур наведено в розділі 4 цих Технічних вимог.

3.1.6 Вимоги до залучення та погодження суб'єкта оцінювання, який здійснюватиме оцінювання реалізації ЦПБ визначених Систем

Для оцінювання дотримання вимог ЦПБ визначених Систем Виконавець зобов'язаний залучити за погодженням із Замовником суб'єкта оцінювання, який відповідає вимогам наказу Адміністрації Держспецзв'язку від 11.07.2025 № 438 «Про затвердження Вимог до юридичних осіб, фізичних осіб-підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», зареєстрованого в Мін'юсті України 31 липня 2025 року за № 1125/44531.

3.1.7 Вимоги до оцінювання дотримання вимог цільових профілів безпеки визначених Систем

Оцінювання дотримання вимог ЦПБ визначених Систем повинне здійснюватися відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18.06.2025 № 712, з врахуванням Рекомендацій з оцінювання дотримання вимог цільового профілю безпеки системи, затверджених наказом Адміністрації Держспецзв'язку від 08.12.2025 № 810 та НД ТЗІ 2.3-025-24 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

За результатами оцінювання дотримання вимог ЦПБ складається звіт з оцінювання для кожної з визначених Систем.

3.1.8 Вимоги до супроводження процесу внесення даних щодо авторизації до переліку авторизованих систем з безпеки в Адміністрації Держспецзв'язку

У разі позитивного результату оцінювання дотримання вимог ЦПБ визначених Систем Виконавцем надаються послуги з супроводження процесу внесення даних щодо авторизації до переліку авторизованих систем, які полягають в консультуванні Замовника щодо складання документів для подачі до Адміністрації Держспецзв'язку щодо авторизації з безпеки визначених Систем.

Якщо за результатами надання послуг визначені Системи не були включені Адміністрацією Держспецзв'язку до переліку авторизованих систем з безпеки з причин, пов'язаних із виконаними Виконавцем роботами та/або підготовленою ним документацією, Виконавець зобов'язаний без додаткової оплати усунути відповідні недоліки та невідповідності у виконаних ним роботах та/або підготовленій ним документації відповідно до рекомендацій, наданих Адміністрацією Держспецзв'язку, та у строк, визначений Адміністрацією Держспецзв'язку (або у інший узгоджений із Замовником строк).

4 ВИМОГИ ДО ДОКУМЕНТУВАННЯ

Виконавець надає Замовнику зведений реєстр документації із зазначенням назви документа, етапу, до якого він належить, версії, дати підготовки та статусу погодження. За результатами надання Послуги Виконавець формує та передає Замовнику по кожній з визначених Систем такі документи:

№	Документ	Відповідний розділ Технічних вимог
1	Звіт з аналізу середовищ функціонування	3.1.1
2	Звіт з визначення категорії критичності	3.1.2
3	Методика оцінювання ризиків інформаційної безпеки	3.1.3
4	Звіт за результатами оцінювання ризиків інформаційної безпеки	3.1.3
5	План обробки ризиків інформаційної безпеки	3.1.3
6	Проєкт цільового профілю безпеки (ЦПБ)	3.1.4
7	Політика безпеки інформації	3.1.4
8	План захисту інформації	3.1.5
9	План забезпечення безперервної роботи та відновлення функціонування системи	3.1.5
10	Політика та процедура контролю доступу	3.1.5
11	Політика та процедура обізнаності та навчання у сфері забезпечення безпеки та приватності	3.1.5
12	Політика та процедура аудиту та підзвітності	3.1.5
13	Політика та процедура оцінювання, авторизації та моніторингу	3.1.5
14	Політика та процедура управління конфігураціями	3.1.5
15	Політика та процедура ідентифікації та автентифікації	3.1.5
16	Політика та процедура реагування на інциденти (План реагування на інциденти безпеки)	3.1.5
17	Політика та процедура технічного обслуговування	3.1.5
18	Політика та процедура захисту носіїв інформації	3.1.5

19	Політика та процедура в галузі фізичного захисту та захисту робочого середовища	3.1.5
20	Політика та процедура планування	3.1.5
21	Політика та процедура кадрової безпеки	3.1.5
22	Політика та процедура оцінки ризиків	3.1.5
23	Політика та процедура придбання систем та послуг	3.1.5
24	Політика та процедура захисту систем і комунікацій	3.1.5
25	Політика та процедура цілісності систем та інформації	3.1.5
26	Політика та процедура управління ризиками ланцюга постачання	3.1.5
27	Політика забезпечення антивірусного захисту	3.1.5
28	Порядок модернізації та оновлення компонентів системи	3.1.5
29	Порядок моніторингу функціонування системи	3.1.5
30	Інструкції адміністраторів та користувачів з безпеки інформації	3.1.5
31	Звіт з оцінювання дотримання вимог цільового профілю безпеки	3.1.7

Виконавець надає документацію в придатній для редагування електронній та паперовій формі.

Документація та результати робіт, передані Виконавцем Замовнику в рамках виконання цих Технічних вимог, можуть використовуватися Замовником без обмеження строку та без порушення прав інтелектуальної власності третіх осіб.

5 ВИМОГИ ДО ПЕРЕДАЧІ ПОСЛУГ

Виконавець починає надання послуг після отримання від Замовника заявки на початок надання Послуг.

Загальний строк надання послуг – не пізніше 25 грудня 2026 року.

Приймання-передача наданих послуг здійснюється після завершення всіх робіт, які входять в послугу (відповідно до пункту 3.1 цих Технічних вимог), та оформлюється Актом приймання-передачі наданих послуг, підписаним уповноваженими особами Замовника та Виконавця, який є підставою для здійснення розрахунків за Договором.

Ініціатор закупівлі **В.К. Цвєтков**

Додаток 2

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

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність працівників відповідної кваліфікації, які мають необхідні знання та досвід**	1.1. Довідка в довільній формі, що підтверджує наявність в учасника спеціалістів відповідної кваліфікації, які мають необхідні знання та досвід і будуть залучені до виконання умов договору про закупівлю (не менше 1 спеціаліста), із зазначенням посади, прізвища, ім'я, по батькові, освіти та загального стажу роботи (років), а також правової підстави використання праці кожного окремого спеціаліста. 1.2. Для підтвердження кваліфікації спеціалістів, яких учасник планує залучати до виконання умов договору про закупівлю відповідно до довідки, в складі тендерної пропозиції надається сертифікат(и) про проходження навчання/підвищення кваліфікації за програмами у сфері захисту інформації та/або кібербезпеки (зокрема ISO/IEC 27001 або NIST Cybersecurity). *Сертифікати, свідоцтва, дипломи чи інші документи, що підтверджують проходження навчання спеціалістів, які видані на іноземній мові, повинні мати переклад тексту документу на українську мову. Вищезазначені документи надаються щодо кожного із спеціалістів, зазначених в довідці.*
2.	**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, а саме: договір на надання послуг з авторизації з безпеки інформаційно-комунікаційних систем, або розроблення цільових профілів безпеки, або створення комплексних систем захисту інформації, за період з 2016 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.*

Ініціатор закупівлі **В.К. Цвєтков**

Додаток 3

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 87
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 «04» вересня 2026 року

ПРИСУТНІ:

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

ПОРЯДОК ДЕННИЙ:

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

1.1. проєкт технічних вимог до закупівлі «Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та 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, проведення заходів щодо авторизації з безпеки міських інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» переліку завдань і заходів Програми);

1.2. проєкт технічних вимог до закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (пункт 7.1 «Створення, розвиток, впровадження, модернізація платформ та систем автоматизації процесів управлінської діяльності (інформаційних систем управління) та великих даних» переліку завдань і заходів Програми).

2. Різне.

По пункту 1.1 питання 1

СЛУХАЛИ:

В. Тихонова, який поінформував, що на виконання вимог Закону України «Про захист інформації в інформаційно-комунікаційних системах» відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», необхідно провести первинну авторизацію з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки, а для цього треба закупити відповідні послуги, та представив проєкт технічних вимог до закупівлі «Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки» (пункт 6.5 переліку завдань і заходів Програми).

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

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки» (пункт 6.5 переліку завдань і заходів Програми), використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.2 питання 1

СЛУХАЛИ:

Н. Йожикова, який поінформував, що з метою модернізації програмного забезпечення інформаційно-комунікаційної системи «Освіта», зокрема щодо ведення довідників, ролей та облікових записів користувачів за допомогою інструментів «Довідники», «Управління ролями» та «Управління користувачами» в адміністративній панелі; ведення інформації про заклад освіти за допомогою інструментів «Паспорт закладу освіти», «Класи» та її відображення з використанням інструменту «Дашборди»; подання та опрацювання заяв, зарахування, переведення та відрахування учнів за допомогою інструментів «Реєстр заяв», «Картка заяви» та «Стан Е-зарахування»; ведення інформації про дитину за допомогою інструментів «Реєстр дітей» та «Профіль дитини»; роботи з інформацією про мережу закладів освіти за допомогою інструментів «Реєстр закладів освіти» та

«Освітня мережа»; щодо компонентів «Електронний архів», «Харчування»; забезпечення електронної інформаційної взаємодії з ПАК «АІКОМ», ІКС «Портал послуг» та ІКАС «Єдина школа», порталом «Відкриті дані» та ІКС «Інформаційний бот», необхідно закупити відповідні послуги та представив проєкт технічних вимог до закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (пункт 7.1 переліку завдань і заходів Програми).

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

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Головний інформаційно-обчислювальний центр» під час процедури закупівлі «Модернізація програмного забезпечення інформаційно-комунікаційної системи «Освіта» (пункт 7.1 переліку завдань і заходів Програми), використовувати 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 075-2056 **Дата реєстрації** 04.09.2026
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 04.09.2026 (Протокол № 87 від 04.06.2026)

Кількість файлів: 3 **Кількість ЕП:** 21

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
04.09.2026 № 075-2056

Перелік електронних підписів

П.І.Б.	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Тихонов Володимир Володимирович **Кількість ЕП:** 3	07.09.2026 11:49:08 ; 07.09.2026 11:49:10 ; 07.09.2026 11:49:11 ;	07.09.2026 11:49:12 Погодив;	07.09.2026 11:49:11
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 3	07.09.2026 11:46:39 ; 07.09.2026 11:46:40 ; 07.09.2026 11:46:41 ;	07.09.2026 11:46:41 Погодив;	07.09.2026 11:46:41 Погодив
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 3	07.09.2026 11:19:54 ; 07.09.2026 11:19:56 ; 07.09.2026 11:19:58 ;	07.09.2026 11:19:58 Погодив;	07.09.2026 11:19:58 Погодив
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 3	07.09.2026 10:19:53 ; 07.09.2026 10:19:55 ; 07.09.2026 10:19:57 ;	07.09.2026 10:19:57 Погодив;	07.09.2026 10:19:57 Погодив
Пашков Сергій Петрович **Кількість ЕП:** 3	07.09.2026 09:53:51 ; 07.09.2026 09:53:52 ; 07.09.2026 09:53:53 ;	07.09.2026 09:53:53 Погодив;	07.09.2026 09:53:53 Погодив

Йожиков Нікіта Сергійович **Кількість ЕП:** 3	04.09.2026 14:44:11 ; 04.09.2026 14:44:12 ; 04.09.2026 14:44:14 ;	04.09.2026 14:44:14 Погодив;	04.09.2026 14:44:14 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 3	04.09.2026 13:51:23 ; 04.09.2026 13:51:24 ; 04.09.2026 13:51:25 ;	04.09.2026 13:51:25 Погодив;	04.09.2026 13:51:25 Погодив

ESKA your ITeam

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

Вих. № 186
від 16.09.2026

СКП «Київтелесервіс»

вул. Хрещатик, буд. 10, м. Київ, 01001

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

щодо орієнтовної вартості послуг з первинної авторизації з безпеки

Шановні колеги!

У відповідь на Ваш запит цінової пропозиції від 09.09.2026 № 075/2-1536 щодо орієнтовної вартості Послуг з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки, ТОВ «ЕСКА-ГЛОБАЛ» повідомляє наступне.

Орієнтовна вартість кожної з двох Послуг, розрахована відповідно до складу робіт, визначеного пунктом 3.1 Технічних вимог, наведена у Додатку до цього листа.

№	Найменування послуги	Од. вим.	Ціна за од., грн без ПДВ	Вартість, грн без ПДВ
1	Послуга з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» (ІКС «ММІ»)	послуга	2 625 000,00	2 625 000,00
2	Послуга з первинної авторизації з безпеки інформаційно-комунікаційної системи моніторингу та кібербезпеки (ІКС МК)	послуга	1 750 000,00	1 750 000,00
РАЗОМ за двома послугами, грн без ПДВ:				4 375 000,00
ПДВ (20%), грн:				875 000,00
РАЗОМ до сплати, грн з ПДВ:				5 250 000,00

Директор
ТОВ «ЕСКА-ГЛОБАЛ»
Ясинська Людмила Віталіївна

Всі права захищені. ESKA 2026 ©

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/823
Від 16.09 2026 р.

GIGASAFE

ТОВ «ГІГАСЕЙФ»
01001, місто Київ, вул. Грушевського Михайла, буд. 10
+38 (044) 355-31-55; info@gigasafe.com.ua

№1 від «22» вересня 2026 року

ДЕРЖАВНА УСТАНОВА " СПЕЦІАЛІЗОВАНЕ КОМУНАЛЬНЕ ПІДПРИЄМСТВО "КИЇВТЕЛЕСЕРВІС""
вул. Хрещатик, буд. 10, м. Київ, 01001 (юридична адреса), а/с 38, м. Київ-04071

ПРОПОЗИЦІЯ НА НАДАННЯ КОНСУЛЬТАЦІЙНИХ ПОСЛУГ У СФЕРІ КІБЕРБЕЗПЕКИ

Компанія ТОВ «Гігасейф» дякує за виявлену зацікавленість у співпраці та з задоволенням пропонує Вашій увазі комерційну пропозицію щодо надання послуги «Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки (72220000-3 Консультаційні послуги з питань систем та з технічних питань (72222300-0 Послуги у сфері інформаційних технологій))». Ми маємо багаторічний досвід роботи у цій сфері та гарантуємо високу якість виконання робіт у визначені терміни.

Вартість та терміни надання послуг

Найменування послуги	Послуги з первинної авторизації з безпеки надаються
Опис / обсяг робіт	1.2 Найменування систем, для яких надаються послуги Послуги з первинної авторизації з безпеки надаються для: інформаційно-комунікаційної системи «Міська мережева інфраструктура» (далі – ІКС «ММІ»); інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС МК), далі разом – визначені Системи.
Термін виконання	2,5 місяці

Цінова пропозиція дійсна протягом 20 календарних днів з моменту надання.

№	Етап / Найменування послуг	Тривалість, роб. днів	Вартість, грн. з ПДВ
1	Послуги з первинної авторизації з безпеки надаються для: інформаційно-комунікаційної системи «Міська мережева інфраструктура» (далі – ІКС «ММІ»);	45	2 604 250,00
2	Інформаційно-комунікаційної системи моніторингу та кібербезпеки (далі – ІКС МК), далі разом – визначені Системи.	30	2 130 750,00
	Всього	75	**4 735 000.00**

Загальна вартість Послуг складає 4 735 000.00 грн з ПДВ

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 015/1/855
Від 22.09 2026 р.

ТОВ «ГІГАСЕЙФ»
01001, місто Київ, вул. Грушевського Михайла, буд. 10
+38 (044) 355-31-55; info@gigasafe.com.ua

Умови оплати

- Передоплата у розмірі 100% протягом 5 банківських днів з моменту підписання договору;
- Остаточний розрахунок - протягом 5 днів після підписання акту наданих послуг.

Директор ТОВ «ГІГАСЕЙФ»

М.В. КУРОЧКО

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНЕ ПІДПРИЄМСТВО "ІНФОТЕХ"

вул. Дегтярівська, 15 Б, м. Київ, 04050,
тел.: (044) 363-43-34
e-mail: info@infotech.gov.ua,
www.infotech.gov.ua
Код за ЄДРПОУ 34239034

ІНФОТЕХ
Мобільність Інновації Аналітика

THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
STATE ENTERPRISE "INFOTECH"

Dehtiarivs'ka str., 15 B, Kyiv, 04050,
phone: (044) 363-43-34
e-mail: info@infotech.gov.ua,
www.infotech.gov.ua
EDRPOU 34239034

На № 075/2-1540 від 09.09.2026

Спеціалізоване комунальне підприємство «Київтелесервіс»

KTS@kyivcity.gov.ua

Державне підприємство «ІНФОТЕХ» (далі – Підприємство), у відповідь на лист від 09.09.2026 № 075/2-1540 про надання інформації щодо орієнтовної вартості «Послуги з первинної авторизації з безпеки інформаційно-комунікаційної системи «Міська мережева інфраструктура» та інформаційно-комунікаційної системи моніторингу та кібербезпеки», повідомляє наступне.

Підприємство проаналізувало технічні вимоги до предмету закупівлі, наведені у додатку до зазначеного листа та зазначає, що має необхідний досвід виконання зазначених робіт. Проте, виробничий план уже затверджений до кінця 2026 року, а профільні спеціалісти повністю залучені до виконання поточних договірних зобов'язань та реалізації запланованих проєктів.

У зв'язку з наведеним, Підприємство не має можливості сформувати обґрунтовану орієнтовну вартість виконання зазначеного комплексу робіт та фактично їх виконати.

Заступник директора з розвитку **Олександр ТАРАСОВ**

Вадим Дутчак (050) 564 36 14

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 075/2/814
Від 15.09 2026 р.

ДП ІНФОТЕХ № 6140/02/2026 від 15.09.2026 (57360)
Підписав: Тарасов Олександр Миколайович
Сертифікат: 6C9E48EB050893DA040000000F570200BA500600
Дійсний: з 05.11.2025 07:46:39 по 05.11.2027 07:46:39