В. о. директора СКП «Київтелесервіс»
Волощуку О.О.
Начальника відділу обслуговування
програмних та апаратних комплексів
Реута Д.Л.

СЛУЖБОВА ЗАПИСКА

м. Київ

«12» червня 2025 року

Назва предмету закупівлі:

Програмна продукція для захисту від вірусів (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)

На виконання заходу 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, яка затверджена рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки» (в редакції рішення Київської міської ради від 12 грудня 2024 року № 449/10257), з метою централізованого придбання антивірусних програмних засобів для забезпечення захисту автоматизованих робочих місць працівників структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва від зловмисного програмного забезпечення, вважаю за доцільне провести закупівлю ліцензій на програмну продукцію згідно переліку:

№ з/п	Найменування	Од. виміру	Кількість ліцензій	Термін дії
1	Програмна продукція ESET PROTECT Entry з локальним управлінням. На 1 рік. Для захисту 13200 об'єктів – 1шт	шт	1	Не менше 12 місяців

Фінансування закупівлі здійснюється за рахунок коштів місцевого бюджету (КЕКВ 2610).

Обґрунтування доцільності закупівлі

На виконання заходу 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, яка затверджена рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки» (в редакції рішення Київської міської ради від 12 грудня 2024 року № 449/10257), з метою організації ефективного захисту від зловмисного програмного забезпечення серверної інфраструктури та автоматизованих робочих місць працівників Київської міської ради, структурних підрозділів

виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва.

Обґрунтування обсягів закупівлі

Кількість та перелік ліцензійного програмного забезпечення сформовано на підставі заявок, отриманих від структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, враховуючи рівень наявного використання ліцензій на антивірусне ПЗ згідно інформації, отриманої з центру керування Eset Protect.

Обґрунтування якісних характеристик закупівлі

Технічні та якісні характеристики предмета закупівлі розроблені з урахуванням потреб структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації) районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва і рекомендовані до використання протоколом № 56 від 28.05.2025 року засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, яка затверджена рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки» (в редакції рішення Київської міської ради від 12 грудня 2024 року № 449/10257).

Придбання даного виду програмної продукції здійснюється по причині найкращого співвідношення сукупності функціональних можливостей, рівня захисту та вартості, для організації максимально ефективного захисту серверів та робочих місць працівників Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації) районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва.

Обґрунтування очікуваної ціни закупівлі

Очікувана вартість закупівлі визначена відповідно до Методики визначення очікуваної вартості закупівлі та згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін шляхом запиту комерційних пропозицій від учасників ринку і складає 5 803 815,33 грн. (п'ять мільйонів вісімсот три тисячі вісімсот п'ятнадцять грн. 33 коп.) з ПДВ, що є середньоарифметичним значенням отриманих комерційних пропозицій.

Фінансування закупівлі здійснюється за рахунок коштів бюджету м. Києва (КЕКВ 2610) згідно заходу 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, яка затверджена рішенням Київської міської ради від 07 грудня 2023 року № 7516/7557 «Про затвердження Комплексної міської цільової програми «Цифровий Київ» на 2024-2025 роки» (в редакції рішення Київської міської ради від 12 грудня 2024 року № 449/10257)

Очікувана вартість предмету закупівлі не перевищує розмір бюджетного призначення.

Розмір бюджетного призначення визначено відповідно до паспорту бюджетної програми.

Процедура закупівлі - Відкриті торги.

Місце поставки товару – 04070, Україна, Київська область, місто Київ, вулиця Фролівська, будинок 1/6, літера А.

Строк поставки товарів – по 04 листопада 2025 року.

Додатки:

Додаток №1. Технічні вимоги в 1 прим. на 7 арк.

Додаток №2. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) в 1 прим. на 3 арк.

Додаток №3. Кваліфікаційна вимога до учасників тендеру - на 2 арк.

Ініціатор закупівлі _____ Д. Л. Реут

«ПОГОДЖЕНО»:

Заступник директора з технічних питань _____ О. Ф. Поліщук

Начальник фінансово-економічного відділу – головний бухгалтер _____ Г. А. Букша

Заступник начальника фінансово-економічного відділу з економічних питань _____ Ю.В. Волочаєва

Заступник директора з юридичних питань _____ О.Є. Юрко

Додаток 1.

ТЕХНІЧНІ ВИМОГИ

Програмна продукція для захисту від вірусів (за кодом ДК 021:2015 (CPV) «Єдиний закупівельний словник» - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)

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. Загальні відомості про зміст робіт:

1.1. Повне найменування об'єкта інформатизації

Сукупність електронних інформаційних ресурсів, серверної інфраструктури та автоматизованих робочих місць працівників Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, які захищаються від зловмисного програмного забезпечення за допомогою засобу інформатизації.

1.2. Найменування сторін:

Замовник – Спеціалізоване комунальне підприємство «Київтелесервіс» (СКП «Київтелесервіс»);

Виконавець – визначається за результатом проведення закупівлі відповідно до вимог законодавства України у сфері публічних закупівель.

1.3. Перелік документів, які мають враховуватись під час розробки.

Закон України «Про Національну програму інформатизації»;

Постанова Кабінету Міністрів України від 21.02.2025 №205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації»;

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

Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».

розпорядженням Київського міського голови від 24.06.2024 № 557 «Про деякі питання антивірусного захисту засобів інформатизації».

Положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва або передані до сфери управління виконавчого органу Київської міської ради (Київської міської державної адміністрації), затвердженого розпорядженням виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 03.07.2018 № 1135.

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 12.12.2024 № 449/10257).

Цей перелік документів не є вичерпним та може бути доповнений та уточнений під час підписання Договору.

2. Призначення та цілі інформатизації:

2.1. Призначення

Забезпечення захисту серверної інфраструктури та автоматизованих робочих місць працівників Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва від зловмисного програмного забезпечення.

2.2. Цілі інформатизації

Організація ефективного захисту від зловмисного програмного забезпечення серверної інфраструктури та автоматизованих робочих місць працівників Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва

3. Характеристики об'єкта інформатизації

3.1. Програмна продукція для захисту від вірусів.

Сукупність електронних інформаційних ресурсів, серверної інфраструктури та автоматизованих робочих місць працівників структурних підрозділів Київської міської ради, виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, які захищаються від зловмисного програмного забезпечення за допомогою засобу інформатизації – програмної продукції для захисту від вірусів.

4. Вимоги до засобу інформатизації:

4.1. Вимоги до структури та функціонування засобу інформатизації

Програмна продукція для захисту від вірусів:

Таблиця 1

№ з/п	Найменування	Од. виміру	Кількість ліцензій	Термін дії
1	Програмна продукція ESET PROTECT Entry з локальним управлінням. На 1 рік. Для захисту 13200 об'єктів – 1шт*	шт	1	Не менше 12 місяців

Технічні вимоги ESET PROTECT Entry

Рішення для захисту робочих станцій під управління серверних та несерверних ОС.

Категорія	Опис вимог
Технічна підтримка	- Наявність української служби технічної підтримки, яка працює 24×7×365. - Зв'язок із технічними спеціалістами по місцевому телефону без використання міжнародного зв'язку. - Можливість отримувати консультації з конфігурації та функціонування ПЗ по телефону та електронній пошті.
Гнучкість ліцензування	- Можливість розподілу захисту між робочими місцями та файловими серверами у будь-якій пропорції в межах кількості ліцензованих об'єктів. - Доступ до всієї функціональності без необхідності

	додаткових придбань.
Інсталяція та локалізація	- Багатомовний інсталятор, що містить українську мову.
Базовий захист	- Захист від вірусів, троянів, рекламного ПЗ, шпигунських програм, фішингу. - Виявлення та блокування руткітів, бекдорів, програм-вимагачів (Ransomware).
Захист від складних загроз	- Використання машинного навчання для глибокого аналізу загроз. - Виявлення потенційно небажаних програм. - Аналіз поведінки програм у реальному часі. - Захист від експлойтів, що використовують уразливості додатків (Java, Flash тощо).
Сканування та виявлення загроз	- Антивірусне сканування за розкладом або на вимогу. - Сканування WMI, системного реєстру та активних процесів. - Сканування файлів під час запуску ОС. - Використання евристичного аналізу та поведінкової аналітики.
Контроль пристроїв та змінних носіїв	- Контроль доступу до змінних носіїв (USB, CD/DVD, SD-карти). - Фільтрація пристроїв за моделлю, виробником або серійним номером. - Автоматичне блокування підозрілих пристроїв.
Захист поштового трафіку	- Інтеграція з поштовими клієнтами для перевірки POP3, IMAP, SMTP трафіку. - Вбудований антиспам-модуль із білими та чорними списками.
Фільтрація веб-трафіку	- Захист HTTP та HTTPS від фішингових атак, ботнет-серверів, командних серверів APT. - Фільтрація веб-ресурсів за категоріями (27 основних категорій, 100+ підкатегорій). - Блокування небезпечних сайтів та шкідливого контенту.
Функціональність брандмауера	- Персональний брандмауер для фільтрації мережевого трафіку. - Виявлення та блокування мережевих атак (IDS/IPS). - Контроль вхідного та вихідного трафіку додатків. - Автоматичне блокування підозрілих IP-адрес.
Оновлення та автоматизація	Регламентне оновлення вірусних баз не менше 24 разів на добу. Оновлення через локальне сховище в ізольованих мережах. Можливість відкату оновлень у разі виявлення проблем.

Підтримувані операційні системи

Тип ОС	Підтримувані версії
Windows	- Windows 11, 10, 8.1, 8, 7 (SP1). - Windows Server 2022, 2019, 2016, 2012, 2008 (R2 SP1).

	- Windows Storage Server 2016, 2012, 2008 (R2 SP1). - Windows MultiPoint Server 2012, 2011, 2010. - Windows Small Business Server 2011, 2008.
MacOS	- MacOS 10.9 та вище.
Мобільні ОС	- iOS 9 та вище. - Android 5 (Lollipop) та вище.
Linux	- Ubuntu Desktop 18.04 LTS 64-bit. - Ubuntu Server 16.04 LTS, 18.04 LTS 64-bit. - RedHat Enterprise Linux (RHEL) 7, 8. - CentOS 7, 8. - Debian 9, 10. - SUSE Linux Enterprise Server (SLES) 12 64-bit, 15 64-bit. - Oracle Linux 8. - Amazon Linux 2.

Система управління антивірусним програмним забезпеченням повинна відповідати наступним обов'язковим функціональним вимогам:

Категорія	Опис вимог
Централізоване управління та адміністрування	- Централізоване управління антивірусним захистом всієї міської мережевої інфраструктури. - Підтримка ієрархічної структури адміністрування з головним сервером та підпорядкованими серверами. - Віддалене встановлення та видалення антивірусного ПЗ на Windows, Linux та Mac. - Можливість інвентаризації обладнання та ПЗ, встановленого на робочих станціях і серверах. - Віддалене керування системами, включаючи перезавантаження, пробудження, відправку повідомлень і запуск команд. - Диспетчер користувачів з можливістю призначення різних рівнів доступу. - Аутентифікація адміністраторів за допомогою груп безпеки Active Directory. - Підтримка двофакторної аутентифікації для підвищеної безпеки адміністраторів. - Журнал аудиту для відстеження всіх змін у конфігурації та дій користувачів. - Автоматичний розподіл клієнтів за динамічними групами з відповідними політиками безпеки. - Підтримка імпорту користувачів та груп з Active Directory. - Використання вбудованих та користувацьких політик безпеки з можливістю імпорту/експорту.
Моніторинг та звітність	- Панель моніторингу з детальною інформацією про рівень безпеки інфраструктури. - Наявність 100+ шаблонів звітів для моніторингу та формування звітів у PDF, CSV. - Можливість створювати та редагувати власні шаблони звітів. - Підтримка інтеграції з SIEM через syslog для збору журналів. - Гнучке налаштування параметрів журналів та вибір з понад

	50 шаблонів.
Функціональність безпеки та управління захистом	- Віддалене керування модулями безпеки: брандмауер, захист у реальному часі, захист пошти, веб-контроль, антиспам. - Можливість імпортувати дерево комп'ютерів з Active Directory. - Контроль доступу до Інтернету та пристроїв через централізоване управління. - Виявлення незахищених робочих станцій для автоматичного розгортання антивірусного захисту. - Вбудований механізм створення та редагування інсталяційних пакетів для Windows, Linux та Mac з можливістю використання у відключених мережах.
Оновлення та керування ліцензіями	- Автоматичне оновлення агентів без втручання адміністратора. - Розподіл навантаження при оновленні для зменшення впливу на мережу. - Створення дзеркала оновлень на базі антивірусного продукту або стороннього HTTP-сервера. - Можливість керування ліцензіями навіть без використання сервера адміністрування. - Віддалена деактивація ліцензій навіть для пристроїв без фізичного або віддаленого доступу.
Розгортання та віртуалізація	- Встановлення сервера адміністрування на Windows та Linux. - Постачання сервера у вигляді готового розгортання для Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation). - Підтримка віртуалізації VMware Horizon 8.x та Citrix XenCenter/XenServer 8+. - Визначення джерела для копіювання або клонування в середовищах VDI. - Вбудований майстер налаштування для інтеграції з системами VDI. - Вибір параметрів шаблонів іменування VDI для миттєвих клонів та каталогів машин. - Автоматичне сповіщення про проблеми з ідентифікацією клонованих машин у VDI. - Можливість встановлення агента управління на ARM64-процесорах.
Масштабування та розподіл ресурсів	- Можливість створення майданчиків для різних філій компанії з окремими частинами ліцензій. - Функціонал для призначення адміністраторів конкретних філій або майданчиків.

Активація (подовження дії) ліцензій здійснюється автоматично момент припинення дії попередніх ліцензій – 06.11.2025 р.

4.2. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

Не застосовуються.

4.3. Вимоги до безпеки

Підтримка політик безпеки, що відповідають міжнародним стандартам інформаційної безпеки та управління ризиками.

Підтримка централізованого управління захистом у відповідності до вимог інформаційної безпеки Київської міської ради, структурних підрозділів виконавчого органу Київської міської

ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва згідно законодавства та нормативно-правових актів у сфері захисту інформації.

Використання загальноприйнятих протоколів шифрування та безпечного обміну даними для захисту трафіку.

Автоматизоване оновлення баз загроз та захист у режимі реального часу на всіх підключених пристроях.

4.4. Вимоги до ергономіки та технічної естетики;

Не застосовуються.

4.5. Вимоги до захисту інформації

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

4.6. Вимоги до стандартизації та уніфікації

Дотримання вимог стандартів ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою.

4.7. Вимоги до надійності засобу інформатизації та збереженості інформації

Централізоване управління безпекою всіх кінцевих пристроїв, серверів та віртуальних середовищ.

Автоматичне створення резервних копій політик безпеки та конфігурацій із можливістю швидкого відновлення.

Вбудована система антивірусного сканування та виявлення загроз із використанням машинного навчання та поведінкового аналізу.

Високий рівень продуктивності завдяки оптимізованому використанню ресурсів пристроїв.

4.8. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи

Шифрування з'єднань між керуючим сервером та клієнтами для забезпечення конфіденційності переданих даних.

Підтримка автоматичної аутентифікації пристроїв та адміністраторів перед встановленням з'єднання.

4.9. Вимоги до режимів функціонування засобу інформатизації

Гнучке керування політиками безпеки, включаючи режими моніторингу, адаптації та активного блокування загроз.

Підтримка автоматичного оновлення антивірусних баз без потреби в ручному втручанні адміністратора.

Здійснення контролю активності додатків, файлів та процесів у реальному часі з можливістю миттєвого реагування.

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

Виявлення вразливостей та оцінка рівня ризиків для кожного пристрою в корпоративній мережі.

Автоматизоване управління карантином та ізоляцією заражених пристроїв.

Фільтрація веб-трафіку, що дозволяє блокувати шкідливі та небезпечні веб-сайти.

Централізоване управління оновленням програмного забезпечення та аналіз наявності застарілих компонентів.

Інтеграція з системами логування та моніторингу безпеки (SIEM) для централізованого аналізу загроз.

Контроль доступу до змінних носіїв та зовнішніх пристроїв, забезпечення розмежування прав доступу.

Підтримка політик контролю використання програмного забезпечення та блокування небажаних застосунків.

Багаторівневий захист від цільових атак, зловмисного ПЗ та фішингових загроз.

5. Вимоги до розробки та передачі послуг

5.1. Вимоги до розробки

Відсутні

5.2. Вимоги до передачі

Забезпечення відображення примірників ПЗ у кабінеті адміністратора на порталі виробника.

Код активації у електронному форматі, який надсилається на поштову скриньку користувача.

5.3. Вимоги до гарантійної підтримки

На період дії ліцензійної угоди.

6. Висновки.

Призначення та цілі інформатизації відповідно до цих Технічних вимог забезпечують якісну реалізацію визначених планових потреб Замовника та забезпечення функціонування засобу інформатизації і гарантує відповідність набору критеріїв, які описують засіб інформатизації.

7. Додатки.

Відсутні.

8. Заявка на модернізацію (модифікацію, розвиток).

Не передбачена.

**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.*

Начальник відділу обслуговування програмних та апаратних комплексів **Реут Д.Л.**

Засідання в онлайн режимі
із використанням Microsoft Teams

ПРОТОКОЛ № 56

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 «28» травня 2025 року

ПРИСУТНІ:

Члени робочої групи:
А. Жежера
В. Жучков
М. Клюєва
С. Осіпов
О. Поліщук
Т. Самойленко
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Цифровий Київ» на 2024-2027 роки, затвердженої рішенням Київської міської ради від 07.12.2023 № 7516/7557 (у редакції рішення Київської міської ради від 12.12.2024 № 449/10257) (далі – Програма), у 2025 році, а саме:

1.1. проєкт технічних вимог до закупівлі «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.2. проєкт технічних вимог до закупівлі «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 «Розвиток комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.3. проєкт технічних вимог до закупівлі «Послуги по встановленню засобів, обладнання та матеріалів для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 «Розвиток

комплексної системи відеоспостереження міста Києва, систем забезпечення безпеки, відеоаналітики із розширенням зони функціонування на території Київської області» переліку завдань і заходів Програми);

1.4. доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для захисту від вірусів» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми) у частині уточнення кількості продукції;

1.5. доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для захисту DNS» (пункт 6.5 «Впровадження, розвиток та дооснащення центру моніторингу та кібербезпеки міських сервісів, закупівля обладнання та програмного забезпечення кібербезпеки, створення, проведення державних експертиз та модернізація комплексних систем захисту інформації» переліку завдань і заходів Програми) у частині перерозподілу обсягу ліцензій.

2. Різне.

По пунктах 1.1-1.3 питання 1

СЛУХАЛИ:

С. Осіпова, який повідомив, що для створення безпечного простору в столиці здійснюється розвиток комплексної системи відеоспостереження міста Києва, зокрема шляхом розширення зони контрольованого покриття системами відеоспостереження об'єктів, будівель та прилеглих територій станцій Київського метрополітену, тому є необхідність придбання обладнання та матеріалів, послуг з їх встановлення та представив проєкти технічних вимог до закупівель «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки», «Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуги по встановленню засобів, обладнання та матеріалів для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми).

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

УХВАЛИЛИ:

Рекомендувати комунальному підприємству «Інформатика» виконавчого органу Київської міської ради (Київської міської державної адміністрації) під час процедури закупівель «Обладнання та матеріали для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки»,

«Засоби для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» та «Послуги по встановленню засобів, обладнання та матеріалів для розвитку комплексної системи відеоспостереження та систем забезпечення безпеки» (пункт 2.1 переліку завдань і заходів Програми) використовувати проєкти технічних вимог, розглянуті на засіданні робочої групи.

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

По пункту 1.4 питання 1

СЛУХАЛИ:

О. Поліщука, який повідомив про необхідність захисту від вірусів електронних інформаційних ресурсів, серверної інфраструктури та автоматизованих робочих місць працівників Київської міської ради, структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, шляхом використання відповідної програмної продукції та представив доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для захисту від вірусів» (пункт 6.5 переліку завдань і заходів Програми) у частині уточнення кількості продукції.

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

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для захисту від вірусів» (пункт 6.5 переліку завдань і заходів Програми) використовувати доопрацьований проєкт технічних вимог, розглянутий на засіданні робочої групи.

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

По пункту 1.5 питання 1

СЛУХАЛИ:

О. Поліщука, який поінформував, що з метою організації ефективного захисту від зовнішнього несанкціонованого втручання в роботу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем структурних підрозділів виконавчого органу Київської міської ради (Київської міської державної адміністрації), районних в місті Києві державних адміністрацій, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, є

необхідність придбання для центру моніторингу та кібербезпеки міських сервісів визначеної програмної продукції та представив доопрацьований проєкт технічних вимог до закупівлі «Програмна продукція для захисту DNS» (пункт 6.5 переліку завдань і заходів Програми) у частині перерозподілу обсягу ліцензій.

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

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Програмна продукція для захисту DNS» (пункт 6.5 переліку завдань і заходів Програми) використовувати доопрацьований 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 075-1205
Дата реєстрації 28.05.2025
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 28.05.2025 (Протокол № 56 від 28.05.2028)

Кількість файлів: 6
Кількість ЕП: 42

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
28.05.2025 № 075-1205

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 6	29.05.2025 14:50:28 ; 29.05.2025 14:50:29 ; 29.05.2025 14:50:30 ; 29.05.2025 14:50:31 ; 29.05.2025 14:50:32 ; 29.05.2025 14:50:34 ;	29.05.2025 14:50:34 Погодив;	29.05.2025 14:50:34 Погодив
Жучков Василь Анатолійович **Кількість ЕП:** 6	29.05.2025 13:17:48 ; 29.05.2025 13:17:50 ; 29.05.2025 13:17:52 ; 29.05.2025 13:17:54 ; 29.05.2025 13:17:56 ; 29.05.2025 13:17:59 ;	29.05.2025 13:18:00 Погодив;	29.05.2025 13:17:59
ЖЕЖЕРА АРТЕМ СЕРГІЙОВИЧ **Кількість ЕП:** 6	28.05.2025 16:25:16 ; 28.05.2025 16:25:17 ; 28.05.2025 16:25:18 ; 28.05.2025 16:25:19 ; 28.05.2025 16:25:21 ; 28.05.2025 16:25:23 ;	28.05.2025 16:25:23 Погодив;	28.05.2025 16:25:23 Погодив
Поліщук Олег Федорович **Кількість ЕП:** 6	28.05.2025 15:46:35 ; 28.05.2025 15:46:41 ; 28.05.2025 15:46:42 ; 28.05.2025 15:46:44 ; 28.05.2025 15:46:45 ; 28.05.2025 15:46:46 ;	28.05.2025 15:46:47 Погодив;	28.05.2025 15:46:46
ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 6	28.05.2025 15:20:52 ; 28.05.2025 15:20:53 ; 28.05.2025 15:20:55 ; 28.05.2025 15:20:56 ; 28.05.2025 15:20:58 ;	28.05.2025 15:21:00 Погодив;	28.05.2025 15:21:00 Погодив

	28.05.2025 15:21:00 ;		
КЛЮЄВА МАРІЯ ПАВЛІВНА **Кількість ЕП:** 6	28.05.2025 15:18:44 ; 28.05.2025 15:18:46 ; 28.05.2025 15:18:47 ; 28.05.2025 15:18:49 ; 28.05.2025 15:18:51 ; 28.05.2025 15:18:52 ;	28.05.2025 15:18:53 Погодив;	28.05.2025 15:18:52
Самойленко Тамара Анатоліївна **Кількість ЕП:** 6	28.05.2025 15:16:37 ; 28.05.2025 15:16:38 ; 28.05.2025 15:16:39 ; 28.05.2025 15:16:40 ; 28.05.2025 15:16:40 ; 28.05.2025 15:16:41 ;	28.05.2025 15:16:41 Погодив;	28.05.2025 15:16:41 Погодив

DAITEKS
сучасні IT рішення

21021, Вінницька обл., Вінницький р-н,
м. Вінниця, просп. Юності, буд. № 14-Б
E-mail: info@dtt.com.ua
Тел.: +380 (432) 50-80-88

Поштова адреса: 21050, м. Вінниця, а/с: 8174
ЄДРПОУ 43054384, **ІПН** 430543802285
АТ КБ "ПРИВАТБАНК",
П/р UA793052990000026004036101949

Вих. № 10062025-1
від «10» червня 2025 року

СКП «Київтелесервіс»
Олександру ВОЛОЩУКУ

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

На постачання ПЗ

У відповідь на Ваш запит № 200-2025 від 30.05.2025, просимо розглянути нашу комерційну пропозицію на постачання антивірусів:

Таблиця №1

№	Артикул	Найменування	К-ть	Од.	Ціна без ПДВ	Сума без ПДВ
1		Програмне забезпечення ESET PROTECT Entry On-prem/13 200 об'єктів./1 рік.	1	шт.	4 882 944,00	4 882 944,00

Разом: **4 834 114,33**
Сума ПДВ: **966 822,87**
Всього із ПДВ: **5 800 937,20**

Загальна вартість: 5 800 937,20 грн. з ПДВ

(П'ять мільйонів вісімсот тисяч дев'ятсот тридцять сім гривень 20 копійок)

З повагою та сподіванням на плідну співпрацю,

Генеральний директор
ТОВ «ДАЙТЕКС» **Сергій КОСТЮК**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 146/2025
Від 10.06 2025р.

ТОВ «Датастрім»
01011, Україна, м.Київ, Печерський узвіз, 19
тел: +38 044 4953415
info@datastream.com.ua, www.datastream.com.ua

Вих. №250609-14
"09" червня 2025 р.

СКП "КИЇВТЕЛЕСЕРВІС"

Цінова пропозиція

Шановний Замовник!

Товариство з обмеженою відповідальністю «ДАТАСТРІМ» у відповідь на лист-запит надає цінову пропозицію на закупівлю необхідної програмної продукції:

Найменування товарів/послуг	Кількість	Ціна без ПДВ, грн.	Сума без ПДВ, грн.
Програмна продукція ESET PROTECT Entry On-prem/13200 obj./1 у.	1	4 882 944,00	4 882 944,00
		Всього без ПДВ, грн:	**4 882 944,00**
		ПДВ, грн:	**976 588,80**
		Всього з ПДВ, грн:	**5 859 532,80**

- Строк поставки – до 10 календарних днів
- Фінансові умови: за договором, післяплата 100%
- Поставка за рахунок постачальника

Менеджер, відповідальний за проект:
Мішутін Андрій
Менеджер з розвитку бізнесу ТОВ «ДАТАСТРІМ»
Тел: +380505790979, (telegram, viber, whatsup)
e-mail: a.mishutin@datastream.com.ua

Директор
ТОВ «ДАТАСТРІМ»

Стеценко Світлана Вікторівна

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 14/2025
Від 09.06. 2025 р.

SOFTNET GROUP

Вих. №004/06-03062025
від 03 червня 2025 року

В.о. Директора
СКП "КИЇВТЕЛЕСЕРВІС"
О. Волощуку

Щодо надання цінової пропозиції

Шановний пане Олександре!

ТОВ «СОФТНЕТ ГРУП» висловлює свою повагу і дає відповідь на ваш запит від 30.05.2025 року №199-2025 щодо надання орієнтовної вартості закупівлі ліцензійного програмного забезпечення, 48760000-3 «Закупівля антивірусного програмного забезпечення для захисту від вірусів» за ДК 021:2015 Єдиного закупівельного словника.

У відповідності до наданих Технічних вимог орієнтовна вартість антивірусного програмного забезпечення наведена у Таблиці 1.

Таблиця 1.

№ з/п	Найменування	Од. виміру	Кількість ліцензій	Термін дії	Всього без ПДВ, грн
1	Програмна продукція ESET PROTECT Entry з локальним управлінням. На 1 рік. Для захисту 13200 об'єктів – 1шт*	шт	1	12 місяців	4 792 480,00
				Всього без ПДВ, грн:	4 792 480,00
				ПДВ, грн:	958 496,00
				Всього з ПДВ, грн:	5 750 976,00

Орієнтовна вартість антивірусного програмного забезпечення в 2025 році складає 5 750 976,00 грн (п'ять мільйонів сімсот п'ятдесят тисяч дев'ятсот сімдесят шість грн 00 копійок) з ПДВ.

Директор **Тихонов М. В.**

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 1431/2025
Від 03.06. 2025 р.

ТОВ "СОФТНЕТ ГРУП"
ЄДРПОУ: 42952398
ІПН: 429523926500

БАНКІВСЬКІ РЕКВІЗИТИ
Р/р: UA333052990000026004036703983
в АТ КБ "ПриватБанк", МФО 380775

ЮРИДИЧНА/ФАКТИЧНА АДРЕСА
м.Київ, вул. О. Пироговського, буд. 19/4.
Тел. +38 044 393 93 23

softnetgroup.com.ua

Додаток №3

Кваліфікаційні критерії, вимоги та документи, які вимагаються для підтвердження відповідності пропозиції учасника кваліфікаційним критеріям та іншим вимогам замовника

Для участі у процедурі закупівлі учасники повинні відповідати кваліфікаційним критеріям та іншим вимогам, наведеним у таблиці.

Вимога	**Підтвердження відповідності (перелік документів, що вимагаються від учасника)**
1. Кваліфікаційні критерії до учасника та спосіб їх документального підтвердження	
Кваліфікаційні критерії, встановлені відповідно до статті 16 Закону	**Документальне підтвердження наявності кваліфікаційних критеріїв**
1. Наявність документально підтвердженого досвіду виконання аналогічного договору *В цій тендерній документації під аналогічним договором слід розуміти договір на поставку з аналогічного предмету закупівлі, який зазначено в даній документації	Довідка у довільній формі про наявність досвіду виконання аналогічного договору за період з 2014 року по теперішній час із зазначенням найменування контрагента, предмету договору, строку дії договору. Разом з довідкою учасник повинен надати копію договору, зазначеного у довідці з усіма наявними додатками, зазначеними у договорі, на який надано лист-відгук (рекомендацію тощо), від контрагента (контрагентів), зазначеного у довідці із зазначенням в ньому дати укладання і номеру договору, на який надано лист-відгук (рекомендацію тощо).
2. Підтвердження можливості постачання продукції у відповідності з технічними вимогами	Учасник повинен надати інформаційний лист або довідку в довільній формі про можливість поставки товару відповідно до технічної специфікації із зазначенням конкретної назви програмної продукції та терміну її дії, що пропонується учасником
3. Наявність експертних висновків.	Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог викладених нижче), зареєстрованих в Адміністрації Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.

- Запропоноване ПЗ забезпечується в Україні технічною підтримкою через українську службу технічної підтримки, яка працює в режимі 24×7×365 - цілодобово, з можливістю зв'язку з технічними спеціалістами по місцевому телефону (без використання послуг міжнародного телефонного зв'язку), на підтвердження чого у складі своєї тендерної пропозиції учасником надається лист від виробника або його ексклюзивного дистриб'ютора щодо наявності в Україні авторизованого центру технічної підтримки.

- З метою встановлення джерела постачання та наявності гарантій виробника на програмне забезпечення, що пропонується учасником до постачання, учасником у складі тендерної пропозиції надається авторизаційний або інформаційний лист від виробника або його офіційного представника на території України відповідного ліцензійного програмного забезпечення, яке пропонується Учасником до постачання, що адресований на ім'я Замовника із посиланням на цю процедуру закупівлі.

Начальник відділу обслуговування програмних та апаратних комплексів **Реут Д.Л.**