Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(відповідно до постанови Кабінету Міністрів України від 11.10.2016 № 710 "Про ефективне використання державних коштів" (зі змінами))

1	**Назва предмета закупівлі**	Доступ до мережі Інтернет через захищений вузол інтернет доступу (ЗВІД). Код ДК 021:2015: 72410000-7: Послуги провайдерів. Ідентифікатор закупівлі UA-2024-12-13-018526-a.
2	**Обґрунтування технічних та якісних характеристик предмета закупівлі**	З метою забезпечення гарантованої якості підключення існуючих інформаційних ресурсів Комісії до мережі Інтернет, забезпечення їх доступності для користувачів та для впровадження нових сервісів та інформаційних систем, через захищений вузол Інтернет доступу (ЗВІД) із швидкістю підключення 1 Гбіт/с з 01 січня 2025 року. **Технічна специфікація** **Адреса адміністративної будівлі Замовника:** місто Київ, площа Лесі Українки, 1, 4 поверх. **Вимоги до Послуги:** 1. Наявність у Учасника (Виконавця) власних волоконно-оптичних ліній в адміністративній будівлі Замовника, які повинні забезпечити підключення інформаційної системи Замовника у синхронному симетричному режимі на гарантованій швидкості 1 Гбіт/с до власного захищеного вузла Інтернет-доступу Учасника (Виконавця). Точка підключення інформаційної системи Замовника – комутаційний вузол на 4 (четвертому) поверсі адміністративної будівлі за адресою м. Київ, площа Лесі Українки, 1. 2. Телекомунікаційна мережа, по якій надається Послуги, повинна забезпечувати безперебійну роботу Послуг. Для автономності роботи телекомунікаційна мережа має бути зарезервована додатковими засобами, що забезпечать працездатність точок взаємоз'єднання не менше 72 годин, при відключенні електроживлення, відповідно до рішення Ради національної безпеки і оборони України від 26 листопада 2022 року "Про забезпечення електронними комунікаційними послугами в умовах воєнного стану". 3. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через власний захищений вузол інтернет доступу (ЗВІД) Учасника (Виконавця), який повинен мати чинний атестат відповідності системи захисту інформації, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, та діючий експертний висновок до нього протягом строку надання Послуг. 3.1. Захищений вузол інтернет доступу (ЗВІД) – повинен являти собою сукупність програмно-технічних засобів та організаційних заходів для забезпечення доступу органів державної влади до мережі Інтернет із захистом інформаційних ресурсів відповідно до вимог законодавства України з функціональним профілем захищеності, який обов'язково має включати наступні функціональні профілі: {КА-2, КА-1, ЦА-1, ЦА-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НР-3, НИ-2, НК-1, НЦ-1, НТ-2, НВ-1} або не нижче за рівнем послуги безпеки, та рівнем гарантії оцінки коректності Г2 відповідно до НД ТЗІ 2.5-004-99. 3.2. Учасник (Виконавець) повинен мати наявність власного високошвидкісного підключення до вузла Української мережі обміну трафіком UA-IX, 1-IX, GIGANET, DTEL-IX. 3.3. Учасник (Виконавець) повинен забезпечити автономність роботи каналу по живленню – 24/7.

		4. Учасник (Виконавець) повинен надати Замовнику пул статичних публічних IP адрес з 32 (тридцять дві) шт. 5. Учасник (Виконавець) повинен забезпечити підтримку доменів "cvk.gov.ua" та "drv.gov.ua". 6. Учасник (Виконавець) повинен мати можливість оптимізувати пропускну здатність мережі для підтримки гарантованої якості вихідного потокового відео та аудіо Замовника 7. Учасник (Виконавець) повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг. 8. Учасник (Виконавець) гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 4 годин. 9. У складі вузла доступу Виконавця має бути наявна власна система захисту від атак класу «розподілені атаки відмови у обслуговуванні» (надалі - DDoS-атак). 9.1. Система має бути власним основний та додатковий програмно-апаратним комплексом (далі - Система захисту), що здійснює фільтрацію Інтернет-трафіку в центрі очищення Інтернет-трафіку з єдиним централізованим механізмом керування. Програмно-апаратний комплекс (основний та додатковий) має належати безпосередньо Учаснику (Виконавцю). 9.2. Учасник (Виконавець) повинен мати діючі ліцензії на програмне забезпечення зі складу програмно-апаратного комплексу по захисту ресурсів в обсягах, необхідних для надання послуг згідно цих Вимог та ліцензії на технічну підтримку. 9.3. Система захисту Учасника (Виконавця) має бути реалізована із основного та резервного програмно-апаратних комплексів по захисту ресурсів, територіально розмежованих між собою, на базі яких реалізується рішення по захисту інформаційних ресурсів в мережі Інтернет від DDoS-атак (з детальним описом роботи даних систем, схеми, функціоналу тощо). 9.4. Система захисту повинна забезпечувати: - захист діапазону IP-адрес закріпленої за Замовником; - реалізацію комплексу механізмів виявлення паразитного трафіку з можливістю оперативного розширення переліку цих механізмів на вимогу Замовника та застосування наступних механізмів фільтрації: • фільтрацію на основі “чорних і білих” списків IP-адрес, з можливістю редагування їх Замовником у режимі on-line; • фільтрацію за географічною ознакою (за місцем розташування джерела трафіку), як з можливістю блокування або пропуску окремих країн та регіонів з можливістю редагування їх Замовником у режимі on-line; • фільтрацію на основі аналізу коректності використання протоколів; • пропуск трафіку тільки за визначеним Замовником списком протоколів; • фільтрацію на засадах контрзаходів, що дозволяють відокремлювати й блокувати паразитний трафік з атаками мережевого, транспортного та прикладного рівнів (L3, L4 та L7); - віддалений доступ Замовника до веб порталу контролю параметрів роботи Системи захисту, статистики, звітів, аналізу параметрів трафіку й виявлених аномалій; - можливість самостійного керування Замовником власним захистом за допомогою віддаленого порталу Системи захисту – зміна параметрів захисту, зупинка та поновлення захисту тощо без залучення Виконавця; - можливість збору та збереження мережевого трафіку під час атаки для подальшого аналізу та розслідування; - забезпечення додаткової аналітики по вимірюваному трафіку та маршрутизації трафіку глобальної мережі; - безперервну роботу в режимі 24x7 із забезпеченням автоматичного реагування; - відсутність обмежень у тривалості захисту при довготривалих DDoS-атаках;

		- ефективне очищення асиметричного трафіку - автоматичні повідомлення про початок/завершення DDoS атак шляхом відправлення по електронній пошті, так і миттєві повідомлення; - ведення та зберігання журналів реєстрації подій протягом мінімум 1-го (одного) місяця; - побудову звітів про роботу Системи захисту, зміну параметрів її роботи, наявності атак на захищені ресурси. 9.5. Вимоги та параметри до роботи Системи захисту: - ємність отриманого очищеного трафіку через Систему захисту - 1000 Mbps; - у разі необхідності, Виконавець повинен мати можливість застосування сервісу хмарної очистки паразитного трафіку; - час реакції на початок атаки: до 30 секунд (при автоматичному спрацюванні системи); - потужність Системи захисту по відбиттю L3 атак не менш ніж 100 Gbps з можливістю обробки не менш ніж 100 Mpps мережевих IP пакетів у секунду; - потужність Системи захисту по відбиттю L4/L7 атак не менш ніж 20 Gbps з можливостю обробки не менш ніж 36 Mpps мережевих IP пакетів у секунду без обмежень на кількість одночасних сесій та нових сесій за секунду; - система захисту має мати Інтеграцію з хмарним сервісом (рівня ATLAS Intelligence Feed або аналог) для отримання в реальному часі інформації про атаки, що відбуваються в світі, і засоби захисту від них. 10. Учасник (Виконавець) має забезпечити, на період дії Договору надання послуг протягом 24 годин на добу 7 днів на тиждень. 11. Учасник (Виконавець) повинен мати власний Центр технічної підтримки що працює в режимі: 24x7x365 (цілодобово (00:00-24:00) з понеділка по неділю включно, з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail). Водночас Учасник (Виконавець) повинен забезпечити можливість інформування про інциденти шляхом створення резервних засобів зв'язку, а саме за допомогою використання електронної пошти та миттєвих повідомлень. 12. Режим роботи служби експлуатації Учасника (Виконавця) має бути - 24x7x365. 13. Учасник (Виконавець) бере на себе зобов'язання з дати укладання Договору забезпечити безперервність обміну даними між локальною мережею Замовника та Інтернет через захищений вузол інтернет доступу (ЗВІД). 14. Учасник (Виконавець) повинен виконати підключення у відповідності до всіх означених технічних вимог з дати укладання Договору, але не пізніше 01.01.2025 року. 15. Строк надання послуг – щомісячно, з 01 січня 2025 року до 31 грудня 2025 року.
3	**Обґрунтування очікуваної вартості предмета закупівлі, розміру бюджетного призначення**	Розрахунок ОВ складено відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року № 275, з урахуванням порівняння ринкових цін згідно наданих цінових пропозицій від ТОВ "ІНТЕР-ТЕЛЕКОМ", ТОВ "КОСМОНОВА", ТОВ "ГІГА ТРАНС". Очікувана вартість розрахована відповідно до середньоринкового рівня цін та складає 498 648,00 грн. з ПДВ.

Начальник управління
адміністрування та захисту інформації
Секретаріату Комісії **Листровий С.О.**

16.12.2024 р.