ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ:

**ПОСЛУГИ ЗАХИЩЕНОГО ДОСТУПУ ДО МЕРЕЖІ ІНТЕРНЕТ**

**КОД ДК 021:2015 72410000-7 ПОСЛУГИ ПРОВАЙДЕРІВ**

(відповідно до пункту 41 постанови Кабінету Міністрів України 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами)

|  |  |  |
| --- | --- | --- |
| 1 | Ідентифікатор закупівлі | UA-2024-02-28-011051-a |
| 2 | Технічні та якісні характеристики предмета закупівлі | 1. Предмет закупівлі: Послуги захищеного доступу до мережі Інтернет за кодом ДК 021:2015 72410000-7 (послуги провайдерів).  Строк надання послуг: з моменту укладення договору до 31.12.2024 року.  Кількість послуг – 1.  Місце надання послуг:  65078, м. Одеса, вул. Лип Івана та Юрія, 21А.  **2. Тип послуг:** послуги підключення та користування захищеного доступу до мережі Інтернет за кодом ДК 021:2015 – 72410000-7 «прослуги провайдерів» мають надаватися через Захищений вузол Інтернет доступу Учасника за технологією TCP/IP по виділеній оптично-волоконній лінії зв’язку на швидкості 500 Мбіт/с (з резервуванням на швидкості 200 Мбіт/с основного каналу) без урахування обсягів прийнятої та переданої інформації з операторським та технічним супроводженням доступу до мережі Інтернет.  **3. Загальні вимоги:**  3.1. Послуги підключення та користування захищеного доступу до мережі Інтернет (далі – Послуги) повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:  – Закону України «Про електронні комунікації» від 16.12.2020 №1089-ІХ;  – Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 № 891/2001;  – Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;  – Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11.04.2012 № 295 та інших нормативно-правових актів України у сфері телекомунікацій.  3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Учасника, який повинен мати чинний атестат відповідності системи захисту інформації та експертний висновок до нього.  3.3. Учасник здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлі мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Учасника.  3.4. Зона відповідальності Учасника при наданні Послуг – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання вузлів мережі, надається, встановлюється та налагоджується Учасником в рамках надання Послуг, та не використовується для інших цілей.  3.5. Доступ до мережі Інтернет повинен здійснюватися за допомогою виділених цифрових каналів передачі даних – основного та резервного. Гарантована швидкість доступу до ресурсів мережі Інтернет по основному каналу:  – для закордонних та українських ресурсів 500 Мбіт/с на прийом та 500 Мбіт/с на передачу, без обмеження трафіку;  – значення джиттеру (коливання затримки передачі IP-пакетів) в мережі провайдера не повинно перевищувати 30 мілісекунд.  Гарантована швидкість доступу до ресурсів мережі Інтернет по резервному каналу:  – для закордонних та українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку;  – значення джиттеру (коливання затримки передачі IP-пакетів) в мережі провайдера не повинно перевищувати 30 мілісекунд.  3.6. Учасник повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналів передачі даних, та у разі необхідності надавати ці відомості Замовнику.  3.7. Учасник повинен забезпечити технічну підтримку каналів передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.  3.8. Інтерфейс для прийому послуг: GigabitEthernet (1000BASE-T або 1000BASE-X).  3.9. Послуги надаються в режимі 24/7.  3.10. Послуги повинні включати:  – виділення окремої підмережі з 64 IPv4 адрес мережі Інтернет;  – можливість автоматичного переключення на резервний канал зв’язку у разі відмови основного каналу із збереженням роботи виділеної Замовнику окремої підмережі з 64 IPv4 адрес мережі Інтернет.  3.11. Підключення до мережі Інтернет має бути забезпечено у синхронному симетричному режимі з пропускною здатністю:  – основного каналу – 500 Мбіт/с (з можливістю поетапного збільшення швидкості з 500 Мбіт/с до 1 Гбіт/с за вимогою Замовника);  – резервного каналу – 200 Мбіт/с (з можливістю поетапного збільшення швидкості з 200 Мбіт/с до 500 Мбіт/с за вимогою Замовника).  3.12. Підключення основного та резервного каналів має бути здійснено по окремих виділених оптично-волоконних лініях зв’язку за різними маршрутами.  3.13. Підключення до мережі Інтернет у відповідності до всіх визначених технічних вимог має бути здійснено не пізніше 5 робочих днів після укладення Договору.  **4. Вимоги до Захищеного вузла Інтернет доступу:**  Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Учасника із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.  Захищений вузол має бути розташований в м. Одеса (дозволяються також підключення до резервних або магістральних вузлів, які є частиною побудованої інформаційно-телекомунікаційної системи захищеного доступу) та бути частиною створеної Комплексної системи захисту інформації та присутній в експертному висновку Атестату відповідності (ЗВІД).  Захищений вузол Інтернет доступу 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.  Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі ЗВІД повинен мати створену Комплексну систему захисту інформації з наступними функціями:  – застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;  – управління засобами захисту та функціями захисту активного мережевого обладнання, що входять до складу ЗВІД;  – безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;  – приймання повідомлень про інциденти щодо порушення безпеки від комплексу засобів захисту серверів ЗВІД;  – приймання повідомлень про інциденти щодо порушення безпеки від активних мережевих засобів захисту та обладнання;  – визначення правил проходження інформаційних потоків між активним мережевим обладнанням;  – захист програмно-апаратних засобів від несанкціонованого доступу;  – моніторинг та аналіз поточного стану безпеки ЗВІД;  – аналіз прийнятих повідомлень та сортування згідно з рангом загрози;  – керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.  **5. Вимоги до міжмережевого екрану як частини інформаційно-телекомунікаційної системи захищеного вузла:**  Для забезпечення необхідного рівня захисту міжмережевий екран Учасника повинен відповідати таким умовам:  – мінімум 2 інтерфейси 10 Гб/с або більше;  – Пропускна здатність міжмережевого екрану IPv4 не менше 10 Гб/с;  – Затримка міжмережевого екрану (UDP-пакет на 64 байта) – не більше 2,2 мкс;  – Пропускна здатність інспекції трафіку SSL (IPS, avg HTTPS) не менше 1,5 Гб/с;  – Пропускна здатність міжмережевого екрану наступного покоління (NGFW) не менше 1,5 Гб/с.  **6. Вимоги до операторського та технічного супроводження:**  6.1. Учасник повинен мати власний Центр технічної підтримки, що працює в режимі: 24х7 (цілодобово (00:00-24:00) з понеділка по неділю включно) з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail);  6.2. Учасник має надати Замовнику контактні дані (службовий, мобільний телефон, електронна пошта, тощо) фахівців (не менше двох) відповідальних за надання послуг (у тому числі невідкладних).  6.3. Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Виконавця, та світових ресурсів.  6.4. Учасник повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.  6.5. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.  6.6. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо моніторингу протидії інцидентам з інформаційної безпеки на захищеному вузлі Учасник у реальному часі та за попередній період з моменту початку надання послуг.  6.7. Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 8 годин.  **7. Порядок та строки усунення інцидентів:**  7.1. Відсутність надання послуг протягом 30 хвилин вважається інцидентом.  7.2. У випадку виникнення інцидентів Учасник негайно повідомляє про це представників технічної підтримки Замовника по телефону або за електронною поштою (e-mail).  7.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Учасника по телефону або через веб-сайт, або електронну пошту (e-mail).  7.4. Початком періоду інциденту вважається виявлена Учасником або Замовником відсутність надання послуг.  7.5. Строк усунення інцидентів, які виникли з вини Учасника, не повинен перевищувати 1-у годину.  7.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.  7.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.  7.8. Про факт відновлення Послуг Учасник повідомляє Замовника по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Учасника Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.  7.9. Замовник зобов’язується надавати персоналу Учасника доступ до приміщень Замовника, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.  7.10. Для отримання необхідного доступу до приміщень Замовника, Учасник надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред’являє Замовнику службові посвідчення та направлення на виконання робіт.  7.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Учасника.  7.12. При надходженні заявки про інцидент (відсутність Послуги з вини Учасника), при перевищені строку відновлення надання Послуги понад нормований час, повинно бути припинене нарахування абонентської плати за період з моменту подачі заявки до відновлення надання Послуги у повному обсязі. |
| 3 | Розмір бюджетного призначення | Розмір бюджетного призначення, визначений відповідно до розрахунку до кошторису Одеської митниці на 2024 рік, становить 246 000,00 грн. |
| 4 | Очікувана вартість предмета закупівлі | Очікувана вартість – 161 000,00 грн.  Визначення очікуваної вартості предмета закупівлі проведено у відповідності до порядку пункту 1 Розділу ІІІ Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275.  Керуючись вищевказаною Методикою, для визначення очікуваної вартості предмета закупівлі здійснювався розрахунок методом порівняння ринкових цін, а саме було проведено моніторинг цін, шляхом здійснення пошуку, збору та аналізу загальнодоступної інформації про ціну послуг (тобто інформація про ціни, що містяться в мережі Інтернет у відкритому доступі, спеціалізованих торгівельних майданчиках, в електронних каталогах, в електронній системі закупівель «Прозоро» тощо). |