***Державна митна служба України***

**ОБҐРУНТУВАННЯ**

технічних та якісних характеристик **закупівлі Послуги захищеного доступу до мережі Інтернет (основний канал, резервний канал),** розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))

**Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія: Держмитслужба м. Київ , вул. Дегтярівська, 11г, ЄДРПОУ 43115923.**

**Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі й частин предмета закупівлі (лотів) (за наявності):** ДК 021:2015 – 72410000-7 Послуги провайдерів.

**Вид та ідентифікатор процедури закупівлі:** UA-2023-02-06-007568-a .

**Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі:** **2 585 490,20** гривень. За два Лоти. Визначення очікуваної вартості предмета закупівлі обумовлено статистичним аналізом загальнодоступної інформації про ціну предмета закупівлі на підставі затвердженої центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері публічних закупівель, примірної методики визначення очікуваної вартості предмета закупівлі, а саме: згідно з пунктом 1 розділу ІІІ наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 із змінами.

**Розмір бюджетного призначення 2 585 490,20 гривень** згідно кошторису Держмитслужби на 2023 рік.

**Обґрунтування технічних та якісних характеристик предмета закупівлі.** Термін постачання — до  31 грудня 2023 року включно.

Якісні та технічні характеристики заявлених послуг визначені з урахуванням реальних потреб служби та оптимального співвідношення ціни та якості. Послуги повинен бути своєчасними, якісними та в повному обсязі.

Враховуючи зазначене, замовник прийняв рішення стосовно застосування таких технічних та якісних характеристик предмета закупівлі:

**ТЕХНІЧНІ ВИМОГИ**

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**(лот 1 - Послуги захищеного доступу до мережі Інтернет (основний канал);**

**лот 2 – Послуги захищеного доступу до мережі Інтернет (резервний канал))**

* + - 1. **Загальні вимоги:**
  1. Послуги захищеного доступу до мережі Інтернет повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:
* Закону України «Про електронні комунікації»;
* Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24 вересня 2001 р. № 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-комунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 7 липня 2008 р. за № 603/15294;
* Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11 квітня 2012 р. № 295, та інших нормативно-правових актів України у сфері електронних комунікацій.
  1. Відповідно до постанови Кабінету Міністрів України від 19 червня 2019 р.   
     № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» для забезпечення відмовостійкості об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно здійснюватися (для об’єкта критичної інфраструктури, які надають свої послуги через Інтернет) зв’язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами) (абзац сьомий пункту 38 Переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури додатку до Загальних вимог).

Учасники процедури закупівлі можуть подавати тендерні пропозиції за обома лотами, але у разі перемоги учасника за обома лотами – відхиляється тендерна пропозиція за другим лотом.

1. **Місце надання послуг:**

04119, м. Київ, вул. Дегтярівська, 11-Г;

03124, м. Київ, бул. В.Гавела, 8А;

88000, м. Ужгород, вул. Собранецька, 220.

1. **Вимоги до послуг:**
   1. **Тип послуг:** послуги захищеного доступу до мережі Інтернет через Захищений вузол Інтернет доступу Виконавця за технологією TCP/IP по виділеній оптично-волоконній лінії зв’язку:

лот 1 –

за адресою м. Київ, вул. Дегтярівська, 11-Г на швидкості 1 Гбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет;

за адресою м. Київ, вул. В.Гавела, 8А на швидкості 200 Мбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет;

за адресою м. Ужгород, вул. Собранецька, 220 на швидкості 200 Мбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет;

лот 2 - за адресою м. Київ, вул. Дегтярівська, 11-Г на швидкості 200 Мбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет.

* 1. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (ЗВІД) Виконавця, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього.
  2. Виконавець 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 Виконавця.
  3. Зона відповідальності Виконавця при наданні Послуг – до інтерфейсу локального мережевого обладнання Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання, надається, встановлюється та налагоджується Виконавцем в рамках надання Послуг, та не використовується для інших цілей.
  4. Доступ до мережі Інтернет повинен здійснюватися за допомогою виділеного цифрового каналу передачі даних. Гарантована швидкість доступу до ресурсів мережі Інтернет:

Лот 1:

за адресою м. Київ, вул. Дегтярівська, 11-Г:

* для закордонних ресурсів 1 Гбіт/с на прийом та 1 Гбіт/с на передачу, без обмеження трафіку;
* для українських ресурсів 1 Гбіт/с на прийом та 1 Гбіт/с на передачу, без обмеження трафіку;

за адресою м. Київ, бул. В.Гавела, 8А:

* для закордонних ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку;
* для українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку

за адресою м. Ужгород, вул. Собранецька, 220:

* для закордонних ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку;
* для українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку

Лот 2:

за адресою м. Київ, вул. Дегтярівська, 11-Г:

* для закордонних ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку;
* для українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, без обмеження трафіку;
  1. Виконавець повинен забезпечити підключення Автономної Системи (AS) та IP адрес v4 Замовника до мережі Інтернет з використанням протоколу BGP.
  2. Виконавець повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналу передачі даних, та у разі необхідності надавати ці відомості Замовнику.
  3. Виконавець повинен забезпечити технічну підтримку каналу передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.
  4. Інтерфейс для прийому послуг за адресами: м. Київ, вул. Дегтярівська, 11-Г, м. Київ, бул. В.Гавела, 8А, м. Ужгород, вул. Собранецька, 220:

Gigabit Ethernet (1000BASE-T або 1000BASE-X).

* 1. Послуги надаються в режимі 24/7/365.
  2. Послуги повинні включати:
* використання при наданні послуг механізму захисту від DDoS атак з застосуванням програмно-апаратного комплексу операторського рівня.

1. **Вимоги до Захищеного вузлу Інтернет доступу**

Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Виконавця із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.

Захищений вузол Інтернет доступу **–** повиненявляти 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 (КСЗІ) з наступними функціями:

* застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;
* управління засобами захисту та функціями захисту активного мережевого обладнання що входить до складу ЗВІД;
* безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;
* приймання повідомлень щодо інцидентів щодо порушення безпеки від Комплексу засобів захисту (КЗЗ) серверів ЗВІД;
* приймання повідомлень щодо інцидентів з порушенням 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 рангу загрози;
* контроль за входом користувачів в систему та доступом до ресурсів;
* реєстрація дій користувачів по відношенню до ресурсів системи;
* забезпечення цілісності інформаційних ресурсів центру (у тому числі антивірусний захист);
* перевірка цілісності та функціонування системи захисту;
* контроль за інсталяцією програмного забезпечення на серверах ЗВІД;
* забезпечення необхідного рівня захисту технологічної інформації при її зберіганні, обробці, створенні та передачі за допомогою засобів системи;
* фізичний захист апаратно-програмних засобів ЗВІД від несанкціонованого доступу (НСД);
* контроль за цілісністю функціонального програмного забезпечення та даних;
* контроль за запуском процесів та їх виконанням;
* виявлення та реєстрацію спроб порушення прийнятих прав розмежування доступу;
* виявлення та блокування розповсюдження шкідливих програм;
* перевірки цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);
* забезпечення можливості повернення обчислювальної мережі ЗВІД у відомий захищений стан після відмов або переривання обслуговування.
* керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.
* за запитом надається деталізована інформація про весь вхідний та вихідний трафік, в узгоджений заздалегідь, обома сторонами, проміжок часу;
* здійснення разового налаштування вузла ЗВІД щодо блокування ресурсів, до яких обмежується доступ відповідно до рішень РНБО, що введені в дію указами Президента України.

1. **Вимоги до програмно-апаратного комплексу захисту від DDoS атак.** 
   1. Захист діапазону IP-адрес закріпленої за Замовником автономної системи (блоку провайдеро-незалежних IP-адрес) найбільш відповідальних ресурсів Системи.
   2. 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 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 (Volumetric), L4 (Infrastructure) та L7 (Application) мережевої моделі OSІ).
  1. Віддалений доступ до веб порталу контролю параметрів роботи Системи захисту, статистики, звітів, аналізу параметрів трафіку й виявлених аномалій.
  2. Можливість самостійного керування Замовником власним захистом за допомогою віддаленого порталу Системи захисту – зміна параметрів захисту, зупинка та поновлення захисту тощо без залучення Постачальника Послуги.
  3. Можливість збору та збереження мережевого трафіку під час атаки для подальшого аналізу та розслідування.
  4. Забезпечення додаткової аналітики по вимірюваному трафіку та маршрутизації трафіку глобальної мережі.
  5. Безперервну роботу в режимі 24х7 із забезпеченням автоматичного реагування;
  6. Ефективне очищення асиметричного трафіку для забезпечення можливої роботи систем Замовника з декількома провайдерами доступу в Інтернет;
  7. Ведення та зберігання журналів реєстрації подій протягом мінімум 1-го (одного) місяця;
  8. Побудову звітів про роботу Системи захисту, зміну параметрів її роботи, наявності атак на захищені ресурси.

Інтеграція 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.

Загальні параметри:

* система має бути реалізована із основного та резервного програмно-апаратних комплексів по захисту ресурсів, на базі яких реалізується рішення по захисту інформаційних ресурсів в мережі Інтернет від DDoS-атак (з детальним описом роботи даних систем, схеми, функціоналу тощо);
* у разі необхідності, надавач послуги 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;
* відсутність потреби аналізу зворотнього трафіку для ефективного захисту від DDoS-атак при роботі систем Замовника з декількома провайдерами доступу в Інтернет.

Гарантована функціональність у режимі очищення трафіку під час атаки:

* система захисту повинна пропускати трафік від адресатів, включених Замовником в “білий список”;
* система захисту повинна блокувати трафік від адресатів, включених Замовником в ”чорний список“;
* система захисту повинна забезпечувати можливість ведення “чорного” та “білого” списків, а також керування станом захисту;
* система захисту повинна забезпечувати можливість повної заборони та/або обмеження швидкості бітової та/або пакетної для адресатів за наступними характеристиками:
  + - * для окремих мережевих протоколів;
      * для окремих типів мережевих пакетів.
* система захисту повинна забезпечувати можливість обмежувати для адресатів наступні характеристики:
  + - * кількість TCP та/або НТТР сесій;
      * тривалість TCP та/або НТТР сесій;
      * мінімально допустиму бітову та/або пакетну швидкість для TCP та/або НТТР сесій.
* захист від атак з використанням протоколів поза специфікацією (Invalid Packets);
* захист від нелегітимного трафіку на незатребуваний протокол та/або порт (Flood Attacks: TCP, UDP, ICMP, DNS, SSDP, NTP, SNMP, тощо);
* захист від посилених атак (Amplification Attacks: Chargen Amplification, DNS Amplification, NTP Amplification, SNMP Amplification, SSDP Amplification, тощо);
* захист від атак з використанням фрагментованих пакетів (Fragmentation Attacks: Teardrop, Targa3, Jolt2, Nestea, тощо);
* захист від атак на виснаження TCP стеку (TCP Stack Attacks: SYN, FIN, RST, SYN ACK, URG-PSH, TCP Flags, тощо);
* відмова в обслуговуванні сервісу/ресурсу атакою за протоколом HTTP шляхом відправлення даних:
  + - * поза специфікацією протоколу;
      * за специфікацією протоколу, але з використанням Slow-rate HTTP GET/POST/READ (Resource exhaustion attacks: Slowloris, Pyloris, LOIC, тощо).
* фільтрація трафіку в умовах наявності великої кількості легітимних користувачів ресурсу з генерацією трафіку з різними характеристиками;
* інші типи атак (Application Attacks: HTTP GET ﬂoods, SIP Invite ﬂoods, DNS attacks, HTTPS protocol attacks, тощо).

1. **Вимоги до операторського та технічного супроводження.** 
   1. Виконавець повинен мати власний Центр технічної підтримки що працює в режимі: 24х7х365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік з можливістю звернення по телефону, через веб-сайт або електронну пошту (e-mail);
   2. Виконавець повинен надати Замовнику перелік телефонів, веб-сайт та електронну пошту (e-mail) Центру технічної підтримки протягом 2-х календарних днів з моменту підписання Договору.
   3. Звернення (повідомлення) Замовника повинно обов’язково включати: найменування Замовника; ім'я, прізвище, контактний телефон особи, що звертається; причину звернення.
   4. На підставі звернення (повідомлення) Замовника Виконавець формує заявку, що включає всі відомості, повідомлені Замовником.
   5. Виконавець повинен здійснювати постійний моніторинг каналу передачі даних, виявлення та усунення причин відхилення від заданих технічних характеристик.
   6. У разі виявлення кіберінцинденту (кібератаки) на ресурси або трафік Замовника Виконавець повинен негайно повідомити про це представників технічної підтримки Замовника по телефону та засобами електронної пошти (e-mail).
   7. Виконавець повинен щомісячно надавати статистичну інформацію про послуги, що надаються.
   8. Виконавець повинен забезпечити усунення пошкоджень каналу передачі даних та відновлення доступу до глобальної мережі у термін (далі - нормований час) відповідно до Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 28.12.2012 № 803, зареєстрованого в Міністерстві юстиції України 21.01.2013 №135/22667.
2. **Порядок та строки усунення інцидентів:**
   1. Відсутність надання послуг протягом 30 хвилин вважається інцидентом.
   2. У випадку виникнення інцидентів Виконавець негайно повідомляє про це представників технічної підтримки Замовника по телефону та засобами електронної пошти  
      (e-mail).
   3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Виконавця по телефону та засобами електронної пошти (e-mail).
   4. Початком періоду інциденту вважається отримання Виконавцем від Замовника повідомлення про інцидент або повідомлення Виконавцем Замовника по телефону та засобами електронної пошти (e-mail).
   5. Строк усунення інцидентів, які виникли з вини Виконавця не повинен перевищувати 2-х годин.
   6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.
   7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.
   8. Про факт відновлення Послуг Виконавець повідомляє Замовника по телефону та дублює повідомлення на електронну пошту (e-mail). На повідомлення Виконавця Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.
   9. Замовник зобов’язується надавати персоналу Виконавця доступ до приміщень Замовника, електронного комунікаційного обладнання, яке встановлено у Замовника відповідно п. 6.9, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.
   10. Для отримання необхідного доступу до приміщень Замовника, Виконавець надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред’являє Замовнику службові посвідчення та направлення на виконання робіт.
   11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Виконавця.
   12. При надходженні заявки про інцидент (відсутність Послуги з вини Виконавця) 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. **На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, Учасником у складі тендерної пропозиції надається:**

8.1. Довідка (форма довільна) щодо можливості надання послуг відповідно до вимог.

8.2. Довідку в довільній формі про організацію цілодобової технічної підтримки послуги (телефони «гарячої лінії», e-mail адреси, сайти технічної підтримки тощо). Інформація зазначена у довідці повинна бути підтверджена інформацією з офіційного сайту Учасника (за наявності).

8.3. Документ, який підтверджує внесення Учасника до реєстру постачальників електронних комунікаційних мереж та послуг Національною комісією, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку.

8.4. На підтвердження відповідності системи захисту інформації Захищеного вузла Інтернет доступу (ЗВІД) встановленим вимогам у сфері захисту інформації учасник повинен надати копію дійсного Атестату відповідності виданого Державною службою спеціального зв’язку та захисту інформації України та Експертного висновку до нього.

8.5. Довідка (форма довільна), яка має містити інформацію про наявність програмно-апаратного комплексу захисту від DDoS атак, що відповідає вимогам указаним у пункті 5 Технічних вимог.

8.6. Документ (документи), що підтверджує (підтверджують) право власності   
або користування програмно-апаратним комплексом захисту від DDoS атак промислового рівня (основний та резервний) від постачальника відповідних послуг.

8.6.1. Довідка про реалізацію програмно-апаратного комплексу по захисту ресурсів, на базі якого реалізується рішення по захисту інформаційних ресурсів в мережі Інтернет від DDoS-атак (з детальним описом роботи даних систем, схеми, функціоналу тощо).

8.7. Копії документів, що підтверджують відповідність системи менеджменту інформаційної безпеки вимогам стандарту ISO/IEC 27001.

8.8. Довідка (форма довільна) щодо застосування заходів із захисту довкілля.