Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі
(відповідно до пункту 4[1] постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів»)

Ідентифікатор закупівлі: UA-2026-04-06-013084-a
Процедура закупівлі: Відкриті торги з особливостями
Назва закупівлі: Послуги з підключення та надання захищеного доступу до мережі Інтернет (ДК 021:2015: 72410000-7 — Послуги провайдерів)

Очікувана вартість предмета закупівлі: 850 000,00 грн

Обґрунтування технічних та якісних характеристик предмета закупівлі:

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 24.09.2001 №891;
- 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, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 №94, зареєстрованого в Міністерстві юстиції України 7 липня 2008 року за №603/15294;
- Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 25.06.2025 № 761 та інших нормативно-правових актів України у сфері телекомунікацій.
- Постанова Кабінетом Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».

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 26.11.2022 року «Про забезпечення електронними комунікаційними послугами в умовах воєнного стану» на виконання Розпорядження Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ) від 27.06.2025 № 424/3225 «Про забезпечення сталості електронних комунікаційних мереж в умовах воєнного стану».

- Час роботи в Інтернет та обсяг передачі інформації не обмежується, доступ до Інтернет 24 години на добу, транзит трафіку Замовника до Міжнародних з’єднань Учасника - не лімітований.
- Наявність кваліфікованої цілодобової технічної підтримки та моніторингу, надання консультативної та технічної допомоги Замовнику по забезпеченню керування доступом до ресурсів Інтернет, маршрутизації електронної пошти, поштових служб та інтерфейсу web-mail

Загальні вимоги до захисту каналів від DDoS:

1. Послуги захисту Замовника від розподілених атак типу “відмова в обслуговуванні” (DDoS-атак) повинні забезпечувати доступність послуги у випадку цілеспрямованих атак,

направлених на блокування легітимного трафіку внаслідок вичерпання мережних та серверних ресурсів Замовника, які зазначені у Додатку 2.

Послуги повинні надаватися за допомогою власного програмно-апаратного комплексу (далі – Системи захисту), що здійснює фільтрацію Інтернет-трафіку в центрі очищення Інтернет-трафіку з єдиним централізованим механізмом керування. Програмно-апаратний комплекс має належати безпосередньо Учаснику.

Системи захисту мають складатись з гібридної комбінованої моделі захисту, включаючи первинну ланку захисту з використанням ресурсів хмарного сервісу для запобігання атак за об'ємом, що перевищують спроможність відбиття лише ресурсами систем Учасника.

Фізичне розташування Систем захисту Учасника, а саме технічні засоби програмно-апаратних комплексів по захисту ресурсів повинні знаходитись на території України. Учасник повинен мати 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 з терміном дії не менше терміну дії договору.

Технічні параметри роботи Системи захисту. Загальні параметри:

- пропускна спроможність Системи захисту сайту Замовника: 1 (один) канал не менше 3000 Mbps;

- 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 за гібридною схемою роботи не менш ніж 200 Mbps з можливістю обробки не менш ніж 100 Mpps мережевих IP пакетів у секунду;

- потужність Системи захисту по відбиттю L4/L7 атак не менш ніж 10 Gbps з можливостю обробки не менш ніж 28 Mpps мережевих IP пакетів у секунду без обмежень на кількість одночасних сесій та нових сесій за секунду;

- відсутність потреби Системи в будь-якому створенні профілю легітимного трафіку (створення еталонної моделі поведінки трафіку) для унеможливлення залежності поведінки Системи захисту від зміни профілю трафіку.

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 країн (геолокація);
- для окремих мережевих протоколів;
- для окремих типів мережевих пакетів;
- мінімально допустиму бітову та/або пакетну швидкість для TCP та/або HTTP 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, тощо);

- для покращення рівня захисту від паразитного трафіку Система захисту має бути підключена до всесвітньо відомих баз даних DDoS атак та отримувати дані в режимі on-line щодо:

- відомих ботнет-мереж,
- репутацій IP адрес,
- сигнатур відомих атак та відповідно превентивно блокувати паразитний трафік, базуючись на отриманих даних.

Реагування на інциденти:

- час реагування (годин, робочий час): протягом 1-2 годин після звертання (по електронній пошті або телефону).

Вирішення інцидентів:

Початком періоду інциденту вважається отримання Учасником від Замовника повідомлення про інцидент або повідомлення Учасником Замовника по телефону або через веб-сайт, або за електронною поштою (e-mail).

Строк усунення інцидентів, які виникли з вини Учасника не повинен перевищувати 2-х годин.

Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.

Виконання планових ремонтних робіт з впливом на надання послуг допускається проводити тільки з 23:00 до 8:00 години.

Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг. Термін зберігання інформації – 1 місяць.

Вимоги до технічного супроводу.

Служба технічного супроводу повинна забезпечувати обробку запитів уповноважених осіб Замовника та передбачати:

- приймання запитів, їх реєстрацію, класифікацію й маршрутизацію на наступні рівні підтримки;
- контроль ходу виконання робіт за запитом, прискорення у випадку виникнення проблем з виконанням запиту, інформування уповноважених осіб Замовника про хід виконання робіт, закриття запиту;
- моніторинг Учасником та Замовником роботи системи захисту online з можливістю формування звітів про атаки;
- інформування уповноважених осіб Замовника про зміни, регламентні та технологічні роботи.

Постачальник повинен мати експлуатаційні бригади служби технічної підтримки для забезпечення функціонування послуг у режимі 24 години на добу, 7 днів на тиждень. Точкою демаркації вважається порт обладнання Замовником у кожній точці підключення. Точка демаркації – зона відповідальності Замовника за працездатність каналу, що закінчується інтерфейсним портом на мережевому обладнанні Замовника за умови оренди мережевого обладнання Замовника.

Обґрунтування розміру бюджетного призначення:

Кошторисні призначення на 2026 рік Територіального управління Державної судової адміністрації України в Полтавській області за бюджетною програмою КПКВК 0501020 «Забезпечення здійснення правосуддя місцевими, апеляційними судами та функціонування органів і установ системи правосуддя» по КЕКВ 2240 «Оплата послуг, крім комунальних»

Обґрунтування очікуваної вартості предмета закупівлі:

Міністерством розвитку економіки, торгівлі та сільського господарства України затверджена примірна методика визначення очікуваної вартості предмета закупівлі від 18.02.2020 №275, якою передбачені методи визначення очікуваної вартості предмета закупівлі, а саме: 1) здійснення пошуку, збору та аналіз загальнодоступної інформації про ціну товару (тобто інформація про ціни, що містяться в мережі інтернет у відкритому доступі, спеціалізованих торгівельних майданчиках, в електронних каталогах, в електронній системі закупівель «Прозоро», тощо; 2) отримання комерційних (цінових) пропозицій від виробників, офіційних представників (дилерів), постачальників; 3) у разі обмеження конкуренції на ринку певних товарів та враховуючи їх специфіку при розрахунку використовуються ціни попередніх закупівель аналогічного товару та/або минулих періодів (з урахуванням індексу інфляції, зміни курсів іноземних валют). Відповідно до вказаної методики, при визначені очікуваної вартості предмету закупівлі товарів, робіт та послуг використовується один із методів формування очікуваної вартості предмету закупівлі та проведення моніторингу цін для подальшого укладення договорів.

Очікувана вартість предмета закупівлі визначена методом здійснення пошуку, збору та аналіз загальнодоступної інформації про ціну послуг (тобто інформація про ціни, що містяться в мережі інтернет у відкритому доступі, в електронній системі закупівель «Прозоро», вартість послуг інтернет-провайдерів Полтавської області), ціну за одиницю послуг у попередньому році з урахуванням кількості приміщень місцевих загальних судів Полтавської області та територіального управління в межах кошторисних призначень на 2026 рік.