ОБҐРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення в межах закупівлі

UA-2023-12-15-014434-a

Замовник: Державна установа «Урядовий контактний центр» (далі-Центр) (ЄДРПОУ 36521731)

Місцезнаходження замовника: 01001, м. Київ, вул. Еспланадна, буд. 8/10

Категорія замовника: юридична особа, яка забезпечує потреби держави або територіальної громади.

Підстава для публікації: постанова Кабінету Міністрів України «Про ефективне використання державних коштів» від 11 жовтня 2016 р. № 710»

Предмет закупівлі: Послуги з надання доступу до мережі Інтернет за адресою м. Київ, вул. Бориса Грінченка, 3 другий та третій поверхи (ДК 021:2015: 72410000-7 Послуги провайдерів)

Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі та технічна специфікація до предмета закупівлі

<table>
<tr><td>1.</td><td>Завдання</td></tr>
<tr><td>1.1</td><td>Оператор електронних комунікаційних послуг (далі – Оператор) повинен надати Замовнику електронні комунікаційні послуги доступу до мережі Інтернет через захищений вузол (далі — Послуги) на 12 місяців, режим роботи, параметри та якість яких відповідають порядку та умовам, визначеним законодавством України.</td></tr>
<tr><td>2.</td><td>Місця розташування кінцевих користувачів послуг та вид послуги зазначено у Таблиці 1</td></tr>
<tr><td></td><td>Таблиця 1
<table>
<tr><th>№ п/п</th><th>Місце отримання послуги</th><th>Вид послуги</th><th>Швидкість Мбіт/с</th></tr>
<tr><td>1</td><td>м. Київ, вул. Бориса Грінченка, 3 другий та третій поверхи</td><td>Захищений доступ до мережі Інтернет (ЗВІД)</td><td>1 000</td></tr>
</table></td></tr>
<tr><td>3.</td><td>Вимоги до послуг.</td></tr>
<tr><td>3.1</td><td>Оператор повинен забезпечити постійне та безлімітне надання Послуги (24 годин на добу та 7 днів на тиждень) без обмеження обсягу трафіка з гарантованою швидкістю (українського та міжнародного трафіку).</td></tr>
<tr><td>3.2</td><td>Цілодобовий доступ до мережі Інтернет (п. 1, таблиця 1) повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Оператора, який повинен мати дійсний атестат відповідності системи захисту інформації (зареєстрований в Державній службі спеціального зв’язку та захисту інформації України) та експертний висновок до нього, за технологією TCP/IP по виділеній оптично-волоконній лінії зв’язку на швидкості 1 Гбіт/с. Перевірка чинності атестату відповідності систем захисту ЗВІД Оператора здійснюється Замовником на вебсайті Державної служби спеціального зв’язку та захисту інформації України, за посиланням: https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet</td></tr>
<tr><td>3.3</td><td>Оператор здійснює розміщення власного кінцевого (термінального) обладнання, необхідного для забезпечення надання Послуг на вузлі електронно комунікаційної мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для його розміщення та експлуатації обладнання Оператора.</td></tr>
</table>

3.4	Зона відповідальності Оператора при наданні Послуги – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання електронно комунікаційної мережі, надається, встановлюється, налагоджується Оператором в рамках надання Послуг, та не використовується для інших цілей.
3.5	Гарантована швидкість доступу до ресурсів мережі Інтернет:
3.5.1	для закордонних та українських ресурсів 1 Гбіт/с на прийом та 1 Гбіт/с, на передачу відповідно Таблиці 1, без обмеження трафіку;
3.5.2	значення джиттеру (коливання затримки передачі IP-пакетів) в мережі провайдера не повинне перевищувати 30 мілісекунд.
3.6	Підключення сервісу має буде здійснено в 3 денний строк з дати укладення договору.
3.7	Оператор повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик ліній електронних комунікаційних мереж, та у разі необхідності надавати ці відомості Замовнику.
3.8	Оператор повинен забезпечити технічну підтримку ліній електронних комунікаційних мереж, яка включає також постійний моніторинг сталості та якості каналу електронних комунікаційних мереж, діагностику причини відхилення від заданих технічних характеристик.
3.9	Інтерфейс для прийому послуг: GigabitEthernet (1000BASE-T).
3.10	Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Оператора із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.
3.11	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.
3.12	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; – система повинна знаходитись в режимі апаратної кластеризації, територіально розмежована між двома відмовостійкими майданчиками; – 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; – 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; – 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;

<table>
<tr><td></td><td>− контроль за цілісністю функціонального програмного забезпечення та даних;
− перевірка 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.
− надання власного Приватного кабінету на вузлі ЗВІД з можливістю переглядів інцидентів інформаційної безпеки та атак, для подальшого аналізу та прийняття відповідних рішень. 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;
− надання Замовнику доступу до вузла ЗВІД для самостійного керування політиками доступу для сайтів, ресурсів та додатків;</td></tr>
<tr><td>4.</td><td>Рівень якості послуги (SLA)</td></tr>
<tr><td>4.1.</td><td>Наявність Послуги протягом місяця розраховується, виходячи з загального часу протягом даного місяця, коли погоджені параметри забезпечувалися. Розрахунок відбувається у такий спосіб:
$$\text{Наявність послуги} = \frac{[\ D \times 24 - TN\ ]}{D \times 24} \times 100\%$$
де:
Наявність послуги — період, коли Послуга повинна надаватися в даному місяці, виражається у відсотках, округлених до двох знаків після коми;
D — кількість днів в розрахунковому місяці;
D x 24 — загальний час надання послуги в розрахунковому місяці;
TN = ∑ [TC – T0] — загальний час відсутності Послуги. Це період від загального часу надання Послуги в даному місяці, коли Сторона, що замовила цю Послугу, не могла нею користуватися.
Обчислюється шляхом підсумовування тривалості всіх простоїв за місяць і округленням до цілої кількості годин.
T0 — час одержання повідомлення про несправність (відкриття trouble ticket)
TC — це час, коли Оператор робить першу спробу (по телефону, факсу чи електронною поштою) повідомити Замовника про відновлення послуги (час закриття trouble ticket).
Відсутністю послуги вважається неможливість обміну інформаційними пакетами за протоколом ICMP, TCP, UDP з портами маршрутизаторів операторів вищого рівня, поточні IP-адреси яких визначаються за допомогою утиліти traceroute.
Виникненням несправності визначається той момент, коли одна Сторона повідомляє Службу технічної підтримки іншої Сторони про те, що виявлені невірні робочі параметри чи відбувається переривання надання Послуги (T0).
Час ремонту — це період між одержанням повідомлення про несправність (T0) і усуненням несправності.
Параметри якості послуги Оператора визначаються як час проходження 64-бітного пакета даних між центральним вузлом магістральної мережі Оператора (у м. Київ) та вузлами операторів вищого рівня.
Метою є наступні середньомісячні значення:
<table><tr><td>Час затримки пакетів (max):</td><td>40ms</td></tr><tr><td>Кількість втрачених пакетів:</td><td>< 1%</td></tr><tr><td>Наявність послуги:</td><td>99,5%</td></tr></table></td></tr>
<tr><td>5.</td><td>Вимоги до програмно-апаратного комплексу захисту від DDoS атак:</td></tr>
<tr><td>5.1.</td><td>Реалізацію комплексу механізмів виявлення паразитного трафіку з можливістю оперативного розширення переліку цих механізмів на вимогу Замовника та застосування наступних механізмів фільтрації:</td></tr>
</table>

	– 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, L4 та L7); – віддалений доступ 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 Постачальника Послуги; – 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; – ефективне очищення асиметричного трафіку для забезпечення можливої роботи систем Замовника з декількома провайдерами доступу в Інтернет; – 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.
5.2.	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, регіонально розмежованих один від одного, 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 зворотного трафіку для ефективного захисту від DDoS-атак при роботі систем Замовника з декількома провайдерами доступу в Інтернет.
5.3.	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 HTTP сесій; • тривалість TCP та/або HTTP сесій; • 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, HTTPS protocol attacks, тощо).
6	**Додаткові умови надання Послуги**
	– послуги повинні надаватися через власні оптичні лінії надавача послуг, або із залученням партнерів для організації «останньої милі» (учасник повинен надати відповідні підтверджуючі документи); – автономність по електроживленню, майданчиків з яких надаються послуги повинна бути ультимативною, тобто безперервною, при умові наявності можливості довоза пального до майданчика, з якого вона підключена. – на вимогу Замовника Оператор, у термін, що не повинен перевищувати 2 дні, повинен, надати послугу по забезпеченню захисту від DDoS-атак на базі власного програмно-апаратного комплексу з можливістю використати сервісу хмарної очистки паразитного трафіку.

Обґрунтування очікуваної вартості предмета закупівлі, розміру бюджетного призначення: Очікувана вартість закупівлі формувалась із середніх цін комерційних пропозицій, наданих суб'єктами господарювання.

Очікувана вартість 137 300, 00 грн. (сто тридцять сім тисяч триста грн. 00 коп.) з ПДВ