Інформація що до виконання вимог пункту 4^{-1} постанови Кабінету Міністрів України від 11 жовтня 2016 №710 «Про ефективне використання державних коштів».

1	Найменування замовника	**ТУ БЕБ у Волинській області**
2	Найменування предмету закупівлі, згідно з класифікатором ДК021:2015	ДК 021:2015: 72410000-7 – Послуги провайдерів (*Послуги надання доступу до мережі Інтернет, технічної підтримки та комплексного обслуговування із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки (захист від DoS та DDoS – атак) з резервуванням за адресою: м. Луцьк)*
3	Посилання на реквізити оголошення про проведення конкурентної процедури закупівлі, оприлюдненої в електронній системі Прозоро чи повідомлення про намір укласти договір для переговорної процедури	**https://prozorro.gov.ua/tender/ UA-2023-01-25-015657-a**
4	Обґрунтування технічних та якісних характеристик предмета закупівлі	З метою забезпечення безперебійного *доступу до мережі Інтернет, технічної підтримки та комплексного обслуговування із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки (захист від DoS та DDoS – атак) з резервуванням* ТУ БЕБ у Волинській області необхідно у відповідності до вимог Закону та Постанови № 1178 провести процедуру відкритих торгів (з особливостями). Технічні та якісні характеристики предмету закупівлі визначені відповідно до потреб замовника з урахуванням вимог законодавства та внутрішніх нормативно-розпорядчих документів БЕБ України, а саме: - Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу; - Доступ до мережі Інтернет здійснюється за допомогою виділеного цифрового каналу передачі даних. Гарантована швидкість доступу до ресурсів мережі Інтернет становить 100 Мбіт/с на передачу, без обмеження трафіку - Захист від атак класу «розподілені атаки відмови у обслуговуванні» (надалі - DDoS-атак) засобами власних систем Захисту; - Захист від Dos та DDos атак Виконавець повинні забезпечувати наступні функції протидії кібер-загрозам: *– підсистема очищення повинна підтримувати можливість побудувати дворівневу модель захисту, дозволяючи користувачам самостійно вмикати і вимикати захист через відповідне кінцеве обладнання (CPE);* *– підсистема очищення повинна використовувати поведінкові методи аналізу трафіку для блокування атак, включаючи атаки нульового дня;* *– підсистема очищення повинна блокувати некоректні пакети (включно з перевіркою коректності заголовків, повноцінності фрагмента, коректності контрольної суми IP, дубліката фрагмента, довжини фрагмента, довжини пакета*

		TCP / UDP / ICMP), коректності контрольної суми TCP / UDP, коректності TCP-прапорів) і забезпечувати статистику для відкинутих пакетів; *− підсистема очищення повинна виявляти і блокувати повільні атаки (Slowloris, Slow read і т.д.);* *− підсистема очищення повинна з використовувати поведінкові методи захисту від атак на 3-м, 4-м, 5-м і 7-м рівнях моделі OSI, забезпечуючи пропуск тільки легітимного трафіку і блокування нелегітимного;* *− підсистема очищення повинна виявляти і блокувати підозрілий трафік;* *− підсистема очищення повинна виявляти і блокувати пульсуючі атаки, які полягають в короткочасному (кілька секунд) сплеску нелегітимного трафіку. Легітимний трафік при цьому повинен пропускатися без втрат;* *− підсистема очищення повинна самостійно (без втручання оператора) виявляти і реагувати на зміну вектора атаки з часом реакції до 30 сек;* *− підсистема очищення повинна обмежувати кількість одночасних TCP-з'єднань по кожному хосту;* *− підсистема очищення повинна мати можливість виявляти і блокувати HTTPS атаки (або мати можливість модернізуватися до такої функціональності без заміни апаратної платформи або залучення додаткових апаратних засобів) і при цьому бути сумісна з вимогами PCI DSS;* *− підсистема очищення повинна мати можливість виявляти і блокувати HTTPS page flood атаки з використанням SSL / TLS без дешифрування трафіку, використовуючи поведінкові моделі (або мати можливість модернізуватися до такої функціональності без заміни апаратної платформи або залучення додаткових апаратних засобів);* *− при роботі в режимі inline підсистема очищення повинна блокувати атаки перебору піддоменів на DNS сервер, повністю пропускаючи легітимні запити і блокуючи нелегітимні;* *− підсистема очищення повинна мати можливість обмежувати кількість DNS, HTTP і SIP-запитів в секунду з кожного джерела відповідно до налаштованим порогом;* *− підсистема очищення повинна забезпечувати можливість конфігурувати регулярні вирази в кількості не менше 100 для відкидання певного трафіку як текстових, так і бінарних протоколів;* *− підсистема очищення повинна з використовувати поведінкові методи захисту від атак на DNS, що забезпечують пропуск тільки легітимного трафіку;* *− підсистема очищення повинна мати можливість здійснювати обмеження (rate limiting) трафіку по його географічним властивостями, тобто на базі країни походження трафіку;* *− підсистема очищення повинна виявляти ботів, які не мають можливість розпізнавати і слідувати командам HTTP 302 redirect;* *− підсистема очищення повинна виявляти ботів, які не мають можливість розпізнавати і слідувати redirect-командам, закодованим в JavaScript;* *− підсистема очищення повинна мати можливість автоматично або у ручному режимі активувати нові захисні техніки за допомогою регулярного оновлення сигнатур атак, що забезпечуються дослідницькою командою виробника обладнання, яка здійснює моніторинг Інтернету 24x7, ідентифікуючи найсуттєвішу і недавню активність ботнетів і стратегії нападу. Підсистема аналізу ботнетів і поточних атак повинна здійснювати глобальний моніторинг Інтернет-трафіку з метою виявлення нових методів атаки і вироблення способів протидії їм;*

		− *підсистема очищення повинна дозволяти змінювати параметри захисту під час її роботи. Такі зміни не повинні викликати переривання трафіку;* − *підсистема очищення повинна мати вбудований пакетний аналізатор і декодер, який повинен бути здатний захопити не менше 50000 пакетів, відповідно фільтру, який сконфігурований користувачем, забезпечуючи декодування для заголовків протоколів IP, TCP, UDP, ICMP, HTTP, SSL / TLS, SIP та DNS. Користувач повинен мати можливість скачати PCAP файл для його подальшого аналізу;* − *при історичному аналізі атак, відображених системою очищення, повинна бути можливість отримання зразка відкинутого трафіку в форматі PCAP;* − *підсистема очищення повинна забезпечувати можливість агрегації інтерфейсів Ethernet з використанням стандартних протоколів LAG або навпаки, прозоро пропускати LAG PDU в залежності від налаштувань, зроблених адміністратором;* − *підсистема повинна мати можливість горизонтального розширення. Розширення повинно здійснюватися без заміни використовуваної апаратної платформи або віртуалізації;* − *підсистема повинна підтримувати автоматичну дворівневий захист спільно з flowspec або blackhole (при перевищенні певного порогу трафік перестає проходити через систему очищення і включається flowspec або blackhole на маршрутизаторах);* − *підсистема очищення повинна мати можливість інтеграції на рівні сигналізації з системами WAF;* − *в системі захисту повинна бути реалізована рольова модель управління доступом (RBAC);* − *підсистема очищення повинна оновлювати інформацію, що стосується джерел, нещодавніх Dos та DDoS-атак, для запобігання атак зловмисників, перш ніж вони націлюються на мережу Замовника;* − *рішення, що пропонується, не повинно передавати, обробляти, аналізувати або зберігати трафік Замовника за межами України.* - Забезпечення резервування як каналів зв'язку, по яким організоване підключення до ЗВІД, так і резервування системи захисту від DDoS-атак; - Підтримка протоколу маршрутизації BGP.
5	Обґрунтування очікуваної вартості предмета закупівлі	**140 000,00 (сто сорок тисяч грн.. 00 коп.) в тому числі ПДВ;** Очікувана вартість закупівлі визначена шляхом моніторингу ринку послуг провайдерів, комерційних пропозицій від провайдерів, що мають відповідні Ліцензії.