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

(відповідно до пункту 41 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

**1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, його категорія:** ДЕРЖАВНА УСТАНОВА "ЦЕНТР ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ"; 03151, Україна, м. Київ, вул. Володимира Сікевича, 28; категорія замовника – бюджетна неприбуткова установа.

## 2. 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 і частин предмета закупівлі (лотів) (за наявності): Закупівля програмних, програмно-апаратних засобів криптографічного захисту за кодом CPV за ЄЗС ДК 021:2015: 48730000-4 - Пакети програмного забезпечення.

**3. Ідентифікатор закупівлі: —** UA-2024-03-12-009150-а

**4. Обґрунтування технічних та якісних характеристик предмета закупівлі**: Закупівля програмних, програмно-апаратних засобів криптографічного захисту за кодом CPV за ЄЗС ДК 021:2015: 48730000-4 - Пакети програмного забезпечення.

**ТЕХНІЧНІ ВИМОГИ**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Назва**  | **Одиниця виміру** | **Кількість** |
| **1** | **Система криптографічного захисту інформації «Шифр-X.509» версія 2 у комплектації для обслуговування до 1 тис. сертифікатів, для VPN у основному ЦОД із встановленням, налаштуванням, проведення навчання та технічною підтримкою протягом року** | **шт** | **1** |
| **2** | **Програмний комплекс криптографічного захисту мережевих з’єднань «Шифр-VPN», для захисту каналу зв’язку між ЦОД МВС та ЦОД 112 (Київ) із встановленням, налаштуванням, проведення навчання та технічною підтримкою протягом року** | **шт** | **2** |
| **3** | **Програмний комплекс криптографічного захисту мережевих з’єднань «Шифр-VPN», для віддаленого адміністрування. Комплект включає 1 серверний шлюз і 15 клієнтів VPN (Windows, Linux) із встановленням, налаштуванням, проведення навчання та технічною підтримкою протягом року** | **шт** | **1** |
| **4** | **Програмний комплекс криптографічного захисту TLS-з’єднань «Шифр-Web» із встановленням, налаштуванням, проведення навчання та технічною підтримкою протягом року** | **шт** | **1** |

***У ціну мають бути включені прямі, загальновиробничі та адміністративні витрати з урахуванням витрат, у тому числі, але не виключно: транспортні витрати, доплати працівникам у зв’язку з втратою часу в дорозі, зв’язок, страхування, спецзасоби, а також економічно обґрунтований прибуток, який Постачальник планує отримати в результаті продажу, кошти на покриття ризиків та/або додаткових витрат, пов’язаних з інфляційними процесами, усі податки і збори, обов’язкові платежі, що сплачуються або мають бути сплачені Постачальником для поставки Товару, зокрема податок на додану вартість, інші витрати, необхідні для виконання проєкту Договору до моменту його повного завершення.***

Характеристики товару повинні відповідати вимогам або бути кращими тих, які наведені в таблиці (характеристики будуть порівнюватися із характеристиками на зазначений товар в Специфікації). У разі відсутності зазначених вимог, Замовник залишає право відхилити пропозицію запропонованого товару.

1. Товар повинен бути новим. Упаковка, в якій постачається товар, повинна відповідати загальноприйнятим стандартам та технічним умовам, забезпечувати зберігання товару, та/або його неушкодженість при транспортуванні.

2. Технічні та якісні характеристики повинні відповідати вимогам та стандартам відповідних діючих нормативних документів.

3. Доставка товару здійснюється за рахунок та силами Постачальника, у терміни попередньо узгоджені, і визначається в кожному випадку замовленням Замовника.

4. Приймання товарів проводиться при наявності товаро супроводжуючих документів, видаткової накладної та копії документів, що підтверджують якість товарів.

5. Учаснику необхідно зазначити конкретну назву, марку, модель Товару, що пропонується для визначення замовником технічних характеристик Товару, що пропонується Учасником.

У разі, якщо характеристики товару, що пропонується Учасником до постачання, відрізняються від характеристик, які вимагаються Замовником, такий учасник у складі тендерної пропозиції надає таблицю відповідності за нижченаведеною формою.

**Таблиця відповідності**

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Характеристика | Опис технічних вимог, які визначені Замовником | Опис технічних вимог, які пропонуються Учасником |

Товар повинен відповідати вимогам:

- Закону України від 14.08.2014р. № 1644-VІІ «Про санкції»,

- Указу Президента України від 15.05.2017р. № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»,

- Постанови КМУ від 16.12.2015р. № 1035 «Про обмеження поставок окремих товарів(робіт, послуг) з тимчасово окупованої території на іншу територію України та/або з іншої території України на тимчасово окуповану територію»,

- п/п. 4 п.2 частини першої Розпорядження Кабінету Міністрів України від 11.09.2014 р. №829-р «Про пропозиції щодо застосування персональних спеціальних економічних та інших обмежувальних заходів», згідно з якими заборонено здійснення державних закупівель товарів, робіт і послуг у юридичних осіб - резидентів Російської Федерації державної форми власності та юридичних осіб, частка статутного капіталу яких перебуває у власності Російської Федерації, а також у інших суб’єктів господарювання, що здійснюють продаж товарів, робіт і послуг походженням з Російської Федерації, крім випадків, коли заміщення таких предметів закупівлі іншими неможливе, що підтверджено Міністерством економічного розвитку і торгівлі.

Вимоги до програмних, програмно-апаратних чи апаратних засобів захисту інформації, які можуть бути використані відповідно до технічного завдання Служби 112 і технічного завдання до КСЗІ ІКС 112:

|  |  |  |
| --- | --- | --- |
| № | Підсистема та вимоги до неї | Деталізація вимог |
| **1. Підсистема захисту інформації, що передається між ЦОД МВС та ЦОД Служби 112 (Київ)**Забезпечує захист інформації, що передається магістральними каналами зв’язку між двома ЦОД: (один) ЦОД МВС і (один) ЦОД Служби 112 (Київ). Вважається, що у кожному ЦОД розгорнуто не менше одного шлюзу |
| 1.1 | Реалізація шлюзів у вигляді образу віртуальної машини (virtual appliance) з попередньо налаштованими операційною системною та програмним забезпеченням у віртуальній інфраструктурі ЦОД МВС і ЦОД Служби 112 (Київ) | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware |
| 1.2 | Забезпечення пропускної здатності захищеного каналу між ЦОД МВС і ЦОД Служби 112 (Київ) | Не менше 1 Гбіт/с |
| 1.3 | Можливість горизонтального масштабування пропускної здатності за рахунок збільшення кількості шлюзів (Virtual Appliance) | Можливість збільшення до 4 шлюзів |
| 1.4 | Використання сучасних криптографічних алгоритмів для забезпечення конфіденційності через симетричне шифрування та автентичності інформації через імітовставку, як національних, так і міжнародних | * ГОСТ 34.311-95+ДСТУ ГОСТ 28147:2009;
* ДСТУ 7564:2014+ДСТУ 7624:2014;
* ДСТУ 7564:2014+ДСТУ 8845:2019 (бажано);
* SHA-256+AES
 |
| 1.5 | Використання сучасних механізмів стиснення трафіку (дані, що передаються базуються на форматах XML, JSON) | * LZO;
* LZ4;
* Інші
 |
| 1.6 | Засоби КЗІ повинні мати відповідний діючий позитивний експертний висновок (сертифікат відповідності) Держспецзв’язку України | Обов’язково |
| 1.7 | Кількість Virtual Appliance з шлюзами засобів КЗІ | 2 шт, з можливістю масштабування до 4 шт |
| **2. Підсистема захисту віддаленого адміністративного доступу** |
| 2.1 | Реалізація шлюзів у вигляді образу віртуальної машини (virtual appliance) з попередньо налаштованими операційною системною та програмним забезпеченням у віртуальній інфраструктурі ЦОД МВС | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware |
| 2.2 | Використання сучасних механізмів стиснення трафіку (дані, що передаються базуються на форматах XML, JSON) | * LZO;
* LZ4;
* Інші
 |
| 2.3 | Агрегація трафіку з кількох мережних інтерфейсів на VPN шлюзі | До 3-х шлюзів |
| 2.4 | Забезпечення пропускної здатності між клієнтом VPN і VPN шлюзом у ЦОД МВС | * не менше 800 Мбіт/с, для каналу Інтернет у 1 Гбіт/с;
* не менше 90 Мбіт/с, для каналу Інтернет у 100 Мбіт/с
 |
| 2.5 | Гарантоване забезпечення якісним обслуговуванням одночасних клієнтських підключень до одного VPN шлюзу | Не менше 15  |
| 2.6 | Аналізувати статус сертифікату за протоколом OCSP | Обов’язково |
| 2.7 | Ведення списків доступу для користувачів та груп користувачів | Обов’язково |
| 2.8 | Використання сучасних криптографічних алгоритмів для забезпечення конфіденційності через симетричне шифрування та автентичності інформації через імітовставку, як національних, так і міжнародних стандартів | * ГОСТ 34.311-95+ДСТУ ГОСТ 28147:2009;
* ДСТУ 7564:2014+ДСТУ 7624:2014;
* ДСТУ 7564:2014+ДСТУ 8845:2019 (бажано);
* SHA-256+AES
 |
| 2.9 | Використання протоколів мережного рівня TCP чи UDP для організації захищеного з’єднання за протоколом TLS v1.2 (чи SSL VPN) | Обов’язково |
| 2.10 | Підтримка віртуальних мереж | Обов’язково |
| 2.11 | Підтримка маршрутизації пакетів на рівні L3, що дозволяє відмовитись від додаткових маршрутизаторів | Обов’язково |
| 2.12 | Віддалене управління VPN шлюзами через web-інтерфейс, в тому числі і управлінням клієнтськими VPN підключеннями | Обов’язково |
| 2.13 | Віддалений централізований моніторинг навантаження за SNMP | Обов’язково |
| 2.14 | Автоматизація реєстрації користувачів – клієнтів VPN для доступу до мережі на VPN шлюзі | Обов’язково |
| 2.15 | Створення каналу між клієнтською робочою станцією та VPN шлюзом, без необхідності додаткових налаштувань з боку мережевих екранів та маршрутизаторів. Користувачі, що будуть використовувати клієнти VPN будуть знаходитись у різних мережах, з різними специфічними налаштуваннями, слід забезпечити їм можливість підключення до Служби 112 МВС з мінімальним втручанням з боку адміністраторів ЦОД МВС | Обов’язково |
| 2.16 | Можливість роботи через HTTP-proxy | Обов’язково |
| 2.17 | Клієнтське програмне забезпечення VPN повинно мати зручний користувацький інтерфейс і підтримувати наступні апаратні платформи | * Microsoft Windows x86, x86-64;
* Linux x86-64;
 |
| 2.18 | Засоби КЗІ повинні мати відповідний діючий позитивний експертний висновок (сертифікат відповідності) Держспецзв’язку України | Обов’язково |
| 2.19 | Кількість Virtual Appliance з шлюзами засобів КЗІ |  шт |
| 2.20 | Кількість клієнтських програмних засобів КЗІ | Не менше 15 шт |
| **3. Підсистема захисту інформації між користувачами Служби 112 МВС**(без використання VPN клієнта) |
| 3.1 | Реалізація шлюзів у вигляді образу віртуальної машини (virtual appliance) з попередньо налаштованими операційною системною та програмним забезпеченням у віртуальній інфраструктурі ЦОД МВС | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware |
| 3.2 | Завдання на захист конфіденційності і автентичності трафіку між ЦОД МВС та користувачами Служби 112 МВС покладається на web-сервери, для побудови HTTPS з’єднання  | Обов’язково з використанням TLS v1.2+ |
| 3.3 | Можливість горизонтального масштабування пропускної здатності за рахунок збільшення кількості серверів (virtual appliance). | Без обмежень на кількість |
| 3.4 | Забезпечення пропускної здатності захищеного каналу між користувачами та Служби 112 МВС (за умови наявності якісного Інтернет з’єднання між web-браузером користувача і web-серверами Служби 112 МВС) | Не менше 100 Мбіт/с між користувачем і web-серверами Служби 112 МВС |
| 3.5 | Можливість роботи через HTTP-proxy | Обов’язково |
| 3.6 | Засоби КЗІ, які використовуються для побудови TLS v1.2 на боці web-серверів Служби 112 МВС повинні мати відповідний діючий позитивний експертний висновок Держспецзв’язку України. | Обов’язково |
| 3.7 | Кількість Virtual Appliance з засобами КЗІ | 1 шт, з можливістю масштабування до 4 шт |
| **4. Підсистема генерації ключів та відповідних сертифікатів відкритих ключів VPN користувачів Системи 112 МВС на основі стандартів X.509**(технологічний надавач електронних довірчих послуг НЕДП) |
| 4.1 | Реалізація у вигляді образу віртуальної машини з попередньо налаштованими операційною системною та програмним забезпеченням (virtual appliance) у віртуальній інфраструктурі ЦОД МВС | Постачання у вигляді Virtual Appliance для середовищ віртуалізації VMware |
| 4.2 | Розгортання власного технологічного НЕДП для управляння сертифікатами відкритих ключів, які надаються користувачам для забезпечення віддаленого підключення при передачі відкритими каналами між клієнтом і Служби 112 МВС | Обов’язково |
| 4.3 | Забезпечення ефективного управління активними сертифікатами | не менше 1000 шт. |
| 4.4 | Використання сучасних криптографічних алгоритмів ЕП, як національних, так і міжнародних | * ДСТУ 4145-2002+ГОСТ 34.311-95+ДСТУ ГОСТ 28147:2009+ISO/IEC 15946-3:2006.
* ДСТУ 4145-2002+ДСТУ 7564:2014+ДСТУ 7624:2014+ISO/IEC 15946-3:2006.
* ECDSA+SHA-256+AES+ISO/IEC 15946-3:2006.
* RSA+SHA-256+AES+ISO/IEC 15946-3:2006.
 |
| 4.5 | Максимально використовувати інфраструктурне програмне забезпечення з відкрити вихідним кодом та операційні системи сімейства Linux, для зменшення вартості володіння | Обов’язково |
| 4.6 | Використання протоколу OCSP для визначення статусу сертифікату користувачів | Обов’язково |
| 4.7 | Використання протоколу TSP для отримання позначок часу користувачами | Обов’язково |
| 4.8 | Можливість функціонувати технологічного НЕДП у одному ЦОД МВС (з подальшим розгортанням, у майбутньому, у резервному ЦОД Служби 112) | Обов’язково |
| 4.9 | Реалізовувати механізми автоматичного формування сертифікатів відкритих ключів за PKCS#10 запитом | Обов’язково |
| 4.10 | Можливість додавання власних розширень до PKCS#10 та до сертифікату відкритих ключів | Обов’язково |
| 4.11 | Виконувати пошук сертифікатів і запитів PKCS#10, PKCS#7 за власними розширеннями | Обов’язково |
| 4.12 | Підтримувати роботу віддалених пунктів реєстрації (ВПР) клієнтів, як у централізованому | Обов’язково |
| 4.13 | ПТК технологічного НЕДП повинен відповідати основним вимогам, які висуваються до ПТК КНЕДП | Обов’язково |
| 4.14 | Засоби КЗІ повинні мати відповідний діючий позитивний експертний висновок (сертифікат відповідності) Держспецзв’язку України | Обов’язково |
| 4.15 | Кількість комплектів ПТК НЕДП (один екземпляр активний) | 1 шт, у ЦОД МВС |
| 4.16 | Кількість сертифікатів, що видаються НЕДП (не враховуючи сертифікати адміністраторів НЕДП) | до 1000 шт. |

**4. Вимоги до підтримки**

В рамках постачання програмних, програмно-апаратних чи апаратних засобів захисту інформації, які можуть бути використані відповідно до технічного завдання Служби 112 і технічного завдання до КСЗІ ІКС 112, Виконавець повинен передбачити такі послуги:

**4.1 Послуги з встановлення та налаштування СПЗ**

Виконавець повинен здійснити постачання та налаштування програмних, програмно-апаратних чи апаратних засобів захисту інформації у відповідності до розроблених політик та наявної документації в Замовника.

**4.2 Проведення навчання для обслуговуючого персоналу по кожному ПЗ**

Навчання по для

1. «Підсистеми захисту інформації, що передається між ЦОД МВС та ЦОД Служби 112 (Київ)»;
2. Підсистема захисту віддаленого адміністративного доступу;
3. Підсистема захисту інформації між користувачами Служби 112 МВС
4. Підсистема генерації ключів та відповідних сертифікатів відкритих ключів VPN користувачів Системи 112 МВС на основі стандартів X.509
	1. **Налаштування обладнання**

В рамках розгортання програмного забезпечення, Виробник має надати рекомендації щодо налаштування обладнання замовника (серверного обладнання, мережевого обладнання, пристроїв захисту інформації, тощо) для коректного та документованого функціонування програмного забезпечення.

Супроводити роботи з налаштування обладнання замовника (серверного обладнання, мережевого обладнання, пристроїв захисту інформації, тощо) для коректного та документованого функціонування програмного забезпечення, здійснити тестування коректності та документованого функціонування програмного забезпечення.

Під тестування функціонування програмного забезпечення мається на увазі тестування серверних компонентів (серверного програмного забезпечення), клієнтських компонентів (клієнтського програмного забезпечення), підключень користувачів.

**4.4 Підтримка від виробника**

Протягом дії ліцензії виробник має забезпечувати:

* сервісну підтримку з режимом роботи 8х5 (робочі дні, з 10:00 до 18:00) з питань роботи програмного забезпечення;
* надавати можливість для завантаження нових версій програмного забезпечення, оновлень з безпеки, вразливостей і виправлень виявлених помилок, розширення функціональності ПЗ;

для вирішення проблем під час експлуатації програмного забезпечення Виробник повинен надавати електронний сервіс (веб-портал, спеціальну email-адресу, мобільний додаток тощо) для створення заявок від Замовника або його представників з автоматичною реєстрацією таких заявок в системі підтримки Виробника. Робота з таким сервісом та комунікація з представниками Виробника повинна бути доступна англійською або українською мовою.

*У разі, якщо у цій тендерній документації (у тому числі у технічній специфікації) міститься посилання:*

*- на стандартні характеристики, технічні регламенти та умови, вимоги, умовні позначення та термінологію, пов’язані з товарами, роботами чи послугами, що закуповуються, передбачені існуючими міжнародними, європейськими стандартами, іншими спільними технічними європейськими нормами, іншими технічними еталонними системами, визнаними європейськими органами зі стандартизації або національними стандартами, нормами та правилами – вважати, що міститься вираз «або еквівалент»;*

*- на конкретні марку чи виробника або на конкретний процес, що характеризує продукт чи послугу певного суб’єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва – вважати, що міститься вираз «або еквівалент».*

*У випадку надання учасником еквіваленту він має надати порівняльну таблицю запропонованих товарів з товарами, які вимагаються Замовником. Якщо Учасник пропонує товар, технічні характеристики якого відрізняються від наведених вище, він повинен обов’язково надати порівняльну таблицю щодо відповідності технічних характеристик запропонованого товару наведеним Замовником характеристикам. Товар має бути з технічними та якісними характеристиками рівноцінними, або покращеними, ніж визначені Замовником.*

**5. Обґрунтування розміру бюджетного призначення:** розмір бюджетного призначення визначено Законом України «Про Державний бюджет України на 2024 рік» за КПКВК 1001050 «Забезпечення діяльності органів, установ та закладів Міністерства внутрішніх справ України, підготовка кадрів закладами вищої освіти із спеціальними умовами навчання» відповідно до бюджетного запиту на 2024 рік.

**6. Очікувана вартість предмета закупівлі:** 1 491 164,60 грн. (один мільйон чотириста дев’яносто одна тисяча сто шістдесят чотири гривні 60 коп.) з ПДВ.

**7. Обґрунтування очікуваної вартості предмета закупівлі:** Очікувана вартість визначена відповідно до частини 1 та 2 пункту 1 Розділу ІІІ «Методи визначення очікуваної вартості» Примірної методики визначення очікуваної вартості предмета закупівлі затвердженої Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 18.02.2020 № 275 та розрахована, як середньоарифметичне значення масиву отриманих даних, що розраховується за такою формулою: Цод = (Ц1 +… + Цк) / К.

**8. Процедура закупівлі:** Застосовується процедура відкритих торгів з особливостями.