**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): Послуга з проведення випробувань інформаційних ресурсів та ІТС на вразливості за ДК 021:2015: 72810000-1 «Послуги з комп’ютерного аудиту»

**3. Ідентифікатор закупівлі: —** UA-2025-03-10-002823-а

## 4. Обґрунтування технічних та якісних характеристик предмета закупівлі: Послуга з проведення випробувань інформаційних ресурсів та ІТС на вразливості за ДК 021:2015: 72810000-1 «Послуги з комп’ютерного аудиту»

**ТЕХНІЧНІ ВИМОГИ**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Найменування**  | **Од. виміру** | **Кількість** |
| **1** | **Проведення випробувань інформаційних ресурсів та ІТС на вразливості** | **послуга** | **1** |

**Технічне завдання до**

**«Послуг з проведення випробувань інформаційних ресурсів та ІТС на вразливості»**

**І. Завдання до виконання**

Виконавець в рамках надання Послуг з проведення випробувань інформаційних ресурсів та ІТС на вразливості повинен забезпечити виконання таких завдань:

1.1. Надати послугу щодо проведення випробувань інформаційних ресурсів та ІТС на вразливості.

**Термін надання послуг:** до 01.05.2025 з дня підписання Договору.

**II. Вимоги до послуг**

**2.1 Вимоги до послуг щодо проведення випробувань інформаційних ресурсів на вразливості**

**Завдання:** Пошук вразливостей інформаційних систем Замовника.

**Об’єкти аналізу:** дані про об’єкти визначаються Замовником самостійно та надаються Виконавцеві.

**Кількість об’єктів аналізу:**

- щонайменше3 доменних імені (вебдодатків);

[https://ducit.gov.ua](https://ducit.gov.ua/)

[https://ca.ducit.gov.ua](https://ca.ducit.gov.ua/)

https://bdr.mvs.gov.ua

- щонайменше 43 IP-адреси.

91.197.4.254

91.227.69.79

91.227.69.80

91.227.69.78

91.227.69.76

193.109.11.171

91.227.69.212

193.109.10.2-5

193.109.10.48/29

94.131.252.196/30

193.109.9.178/28

94.131.251.232/30

Об’єкти аналізу надаються Виконавцю у відповідному запиті на надання послуг.

**Методи аналізу:** Випробування на проникнення інформаційної системи (тестування на проникнення) здійснюється по зовнішньому комунікаційному каналу за принципом чорного ящику.

Після проведення випробування Виконавець готує звіт та надає спеціалістам Замовника консультації (роз’яснення) щодо усунення виявлених недоліків.

**Періодичність перевірок:** 1 раз за всіма об’єктами аналізу.

**Порядок надання послуг:**

При здійсненні аналізу Виконавець може використовувати автоматизовану перевірку та обов’язково ручний пошук і експлуатацію вразливостей.

Виконавець повинен виконати оцінку можливості отримання несанкціонованого доступу в процесі моделювання атак.

Виконавець повинен знайти максимальну кількість вразливостей, виходячи з наявної інформації, знань і можливостей інструментальних засобів.

При проведенні тестування на проникнення Виконавець повинен провести випробування за принципом чорного ящику, тобто може отримувати від Замовника загальну інформацію щодо доменів та ІР-адрес.

При виконанні тестування спеціалісти повинні здійснити такі кроки:

 - збір інформації про інфраструктуру Замовника з відкритих джерел у пасивний та активний спосіб;

 - проведення сканування мереж та систем у інфраструктурі Замовника, що включено у перелік цілей для тестування;

 - випробування на вразливості знайдених активів і сервісів під час попередніх етапів тестування;

 - аналіз результатів випробувань з метою пріоритезації подальшого ходу тестування;

 - класифікація вразливостей і вибір неявних вразливостей для перевірки, оцінка вразливостей відповідно до галузевого стандарту CVSS;

 - документування вразливостей та збір доказів перевірки;

 - аналіз результатів перевірки вразливостей;

 - підготовка звіту з тестування з рекомендаціями, щодо усунення знайдених вразливостей та недоліків безпеки в ITC Замовника.

Усі послуги з тестування на проникнення повинні проводитись тільки після отримання Виконавцем від Замовника офіційного листа та/або електронного повідомлення на дозвіл таких послуг.

У випадку можливості виходу з ладу або погіршення показників роботи елементів інфраструктури Замовника в результаті виконання випробувань, такі випробування повинні бути припинені до отримання дозволу від Замовника на продовження саме такого виду випробувань.

У випадку отримання доступу до конфіденційної інформації в інформаційній системі Замовника, випробування відносно цієї системи повинні бути припинені до отримання дозволу від Замовника на продовження випробувань відносно цієї системи.

**Вимоги до оформлення результатів Послуг:**

За результатами аналізу Виконавець надає Замовнику звіт за результатами тестування.

Звіт повинен містити таку інформацію:

1. Резюме. Стисле викладення результатів випробувань.

2. Мета тестування. Опис цілей проведення випробувань.

3. Область дії. Визначення області дії випробувань.

4. Опис методики. Методики та інструменти, що були використані Виконавцем в ході тесту та його окремих етапів.

5. Результати випробувань. Детальні результати тестування та рекомендації, які повинні містити таку інформацію:

- назву вразливості;

- перелік вразливих систем (сервісів);

- статус вразливостей (дійсна / не дійсна / потенційна);

- рівень ризику;

- опис вразливостей;

- дії щодо перевірки вразливості (опис виконаних атак);

- докази перевірки;

- рекомендації з усунення.

Звіти з тестування повинні бути підготовлені в письмовій формі українською мовою.

Послуги повинні бути надані з урахуванням вимог, які викладені у таких документах:

 ISECOM OSSTMM 3 (Open Source Security Testing Methodology Manual);

 OWASP (OWASP Testing Guide v3.0) - індустріальний стандарт;

 Penetration Testing Model (BSI);

 ISACA IS auditing procedure "P8 Security Assessment - Penetration testing and vulnerability analysis;

 NIST 800-115 (Technical Guide to Information Security Testing and Assessment).

Звіти передаються Замовнику електронними поштовими повідомленнями та/або офіційним листом.

 **5. Обґрунтування розміру бюджетного призначення:** розмір бюджетного призначення визначено Законом України «Про Державний бюджет України на 2025 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 2025 рік.

**6. Очікувана вартість предмета закупівлі:** 840 000,00 грн. (вісімсот сорок тисяч гривень 00 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.