ЗАПРОШЕННЯ ДО ВИCЛОВЛЕННЯ ЗАЦІКАВЛЕНОСТІ

(КОНСУЛЬТАЦІЙНІ ПОСЛУГИ – ВІДБІР ІНДИВІДУАЛЬНОГО КОНСУЛЬТАНТА)

**Країна**: Україна

**Проект**: Програма підтримки управління державними фінансами в Україні

**Грант №:**  TF0B6630

**Назва завдання:** Cтарший технічний радник з питань ІТ-безпеки.

**Ідентифікаційний №** **(згідно з Планом закупівель):** NACS-IC-2/2-2

Україна отримала фінансування від Міжнародного банку реконструкції та розвитку (далі – «Банк» або МБРР) у вигляді гранту на реалізацію проєкту «Програма підтримки управління державними фінансами в Україні» (далі – «Проєкт») та має намір використати частину цих коштів на здійснення правомочних платежів за консультаційні послуги, для закупівлі яких випущено це запрошення до висловлення зацікавленості.

Консультаційні послуги (далі – «Послуги») передбачають надання НАДС послуг щодо ІТ-безпеки для впровадження та використання HRMIS. Детальне Технічне завдання наведено нижче.

Національне агентство України з питань державної служби (далі – НАДС) запрошує правомочних консультантів (надалі – «Консультанти»), висловити свою зацікавленість у наданні зазначених Послуг. **Зацікавлені Консультанти мають надати інформацію, що підтверджує наявність у них кваліфікації та досвіду, необхідних для виконання Послуг, а також заповнити форму для визначення відповідності кваліфікаційним критеріям, що наведена нижче.**

Відбір найбільш кваліфікованого та досвідченого консультанта для виконання завдання здійснюватиметься на основі наступних критеріїв:

Обов'язкові вимоги:

1. Вища освіта в галузі комп’ютерних наук, інформаційної безпеки або еквівалентної суміжної галузі;
2. Щонайменше 6 років професійного досвіду в адмініструванні засобів ІТ-безпеки (принаймні антивірусне програмне забезпечення, брандмауер, система запобігання вторгнень);
3. Вільне володіння українською мовою,
4. Поглиблене знання найновіших рішень, інструментів і технологій з ІТ-безпеки, методів атак і вразливостей;
5. Наявність сертифікату спеціаліста з безпеки інформаційних систем (CISSP) або еквівалентного сертифікату;
6. Досвід роботи з архітектурою ІТ-безпеки у великому ІТ-середовищі, включаючи досвід виявлення слабких місць безпеки архітектури на рівні програми, ОС і мережі;
7. Досвід проектування та впровадження рішень з IT-безпеки;

Бажані вимоги:

1. Досвід роботи з адміністрування ІТ або засобів ІТ-безпеки в центральних органах виконавчої влади буде вважатися перевагою;
2. Практичні навички адміністрування широкого спектру ІТ-систем будуть вважатися перевагою;
3. Досвід підготовки інфраструктури та отримання позитивного висновку на Комплексну систему захисту інформації буде вважатися перевагою.

Звертаємо увагу зацікавлених Консультантів на Розділ ІІІ пункти 3.14, 3.16 та 3.17 Посібника Світового банку «Правила закупівель Світового банку для позичальників ФІП», датованого вереснем 2023 року (далі – «Правила закупівель»), який містить політику Світового Банку стосовно конфлікту інтересів.

Консультанта буде обрано за допомогою методу відбору індивідуальних консультантів (ІК), що детально описаний у Правилах закупівель. З Консультантом буде підписано договір, в якому він виступатиме у якості фізичної особи-підприємця, з поденною формою оплати за ставкою, погодженою при підписанні договору.

Додаткову інформацію можна отримати за адресою електронної пошти, що вказана нижче, з 10:00 до 17:00 години за місцевим часом.

Резюме та заповнена форма мають бути доставлені у письмовій формі **українською** мовою за зазначеною нижче адресою електронної пошти **до 17:00 за київським часом 19 березня 2025 року**. Резюме необхідно подавати із зазначенням наступної теми: **«NACS-IC-2/2-2: Висловлення зацікавленості».**

Адреси, що згадуються вище, наступні:

Ел. пошта: i\_fedorenko@nads.gov.ua, **обов’язково копія** на procurement.nacs@ukr.net, hrmis\_zagal@nads.gov.ua

**ФОРМА ДЛЯ ЗАПОВНЕННЯ**

**у рамках відбору консультанта за позицією «Cтарший технічний радник з питань ІТ-безпеки»**

**(№ NACS-IC-2/2-2)»**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Критерій, передбачений Технічним завданням** | **Відповідність критерію** |
| **Обов'язкові вимоги:** |
|  | Вища освіта в галузі комп’ютерних наук, інформаційної безпеки або еквівалентної суміжної галузі; |  |
|  | Щонайменше 6 років професійного досвіду в адмініструванні засобів ІТ-безпеки (принаймні антивірусне програмне забезпечення, брандмауер, система запобігання вторгнень); |  |
|  | Вільне володіння українською мовою, |  |
|  | Поглиблене знання найновіших рішень, інструментів і технологій з ІТ-безпеки, методів атак і вразливостей; |  |
|  | Наявність сертифікату спеціаліста з безпеки інформаційних систем (CISSP) або еквівалентного сертифікату; |  |
|  | Досвід роботи з архітектурою ІТ-безпеки у великому ІТ-середовищі, включаючи досвід виявлення слабких місць безпеки архітектури на рівні програми, ОС і мережі; |  |
|  | Досвід проектування та впровадження рішень з IT-безпеки; |  |
| **Бажані вимоги:** |
|  | Досвід роботи з адміністрування ІТ або засобів ІТ-безпеки в центральних органах виконавчої влади буде вважатися перевагою; |  |
|  | Практичні навички адміністрування широкого спектру ІТ-систем будуть вважатися перевагою; |  |
|  | Досвід підготовки інфраструктури та отримання позитивного висновку на Комплексну систему захисту інформації буде вважатися перевагою. |  |

**ТЕХНІЧНЕ ЗАВДАННЯ**

на консультаційні послуги (відбір індивідуального консультанта)

**Cтарший технічний радник з питань ІТ-безпеки**

(позиція у плані закупівель: NACS-IC-2/2-2)

**1. ЗАГАЛЬНА ІНФОРМАЦІЯ**

Україна отримала фінансову допомогу від Міжнародного банку реконструкції та розвитку та Міжнародної асоціації розвитку («Банк»), які діють як адміністратор грантових коштів, наданих Європейською Комісією від імені Європейського Союзу («Донор») у рамках Програми партнерства ЄС та Світового банку, Частина ІІІ для програм Європи та Центральної Азії Цільовий фонд єдиного донора (TF073423) у сумі три мільйони вісімсот дев’ять тисяч євро (3 809 000, 00 євро) («Грант») на фінансування Програми підтримки управління державними фінансами в Україні. Лист-Угода щодо гранту TF0B6630 була підписана між Україною та Світовим банком 09.02.2022 («Лист-Угода»).

Проект спрямований на покращення управління державними ресурсами. Це має бути досягнуто, серед іншого, за допомогою впровадження Фази 2 Інформаційної системи управління людськими ресурсами в державних органах (HRMIS), як це передбачено у частині A «Запровадження HRMIS в межах всієї країни» (Частина A Проекту). Національне агентство України з питань державної служби (НАДС) відповідає за реалізацію заходів Частини А Проекту. Частина D Проекту «Управління проектом та підтримка впровадження» покриває відповідні витрати НАДС та Міністерства економіки України, іншого виконавця Проекту.

Розробка та впровадження HRMIS передбачено Стратегіями реформування державного управління на 2016-2021 та 2022-2025 роки та іншими постановами Уряду[[1]](#footnote-1). Європейська Комісія у партнерстві з Банком надає фінансову та технічну підтримку цим заходам у рамках проектів технічної допомоги. Впровадження HRMIS відбувається за двоетапним підходом з поступовим функціональним та інституційним охопленням і розширенням.

Фаза 1 HRMIS, яка охоплює проектування та розробку основних функціональних можливостей HRMIS та обмежений запуск системи на рівні міністерств, була завершена в рамках Проекту «Зміцнення управління державними ресурсами» (Угода про грант № TF0A5324 між Україною та Світовим банком, що фінансувалася Програмою ЄС для Реформи державного управління та фінансів в Україні (EURoPAF) протягом серпня 2017 р. – березня 2021 р. НАДС здійснила закупівлю на міжнародних торгах рішення HRMIS як комерційного готового рішення, яке було налаштовано постачальником відповідно до технічної та функціональної системи НАДС. За результатами Фази 1 HRMIS була розроблена за основними функціями (*Управління державними органами; Управління посадами; Ведення особистих справ працівників; Конкурсний прийом на вакантні посади державної служби; Стаж державної служби; Вступ на державну службу та її припинення; Офіційна кар'єра; Переведення; Відрядження; Час роботи та відпочинку; Документи; Розрахунок заробітної плати; Звіт із заробітної плати; Публічний портал, Кабінет самообслуговування*) та впроваджена в 19 центральних органах виконавчої влади (включаючи територіальні) з охопленням 20 973 кінцевих споживачів. [Публічний портал](https://public.nads.gov.ua/) надає основну інформацію про HRMIS та її поточний стан розгортання серед державних установ.

Фаза 2 впровадження HRMIS, яка охоплює нову Програму підтримки управління державними фінансами в Україні, включає: i) функціональне розширення HRMIS з оцінкою ефективності, розвитком професійних компетенцій та модулями аналізу та звітності; ii) розгортання системи по всій країні; iii) навчання кінцевих користувачів; iv) удосконалення політики та методологічної основи впровадження та використання HRMIS («Проект»). Крім того, Фаза 2 впровадження HRMIS включатиме підтримку агенцій Фази 1, які ще не відповідають вимогам щодо переходу на HRMIS та вдосконалення розробок Фази 1 для усунення прогалин у функціональності».

Розгортання HRMIS по всій країні передбачає два етапи. Етап 2а включатиме державні установи зі 100-відсотковим охопленням персоналу, включаючи державних службовців та інших працівників, на яких поширюється дія Кодексу законів про працю. Етап 2b має охоплювати державні установи зі змішаним штатом (включаючи як державних службовців, так і інших державних службовців в установах державної служби, які не регулюються Законом України «Про державну службу»), і буде залежати від рішень Наглядового комітету Проекту. Заходи 2 фази HRMIS мають бути завершені до 11 червня 2025 року.

*Для зміцнення своєї спроможності впровадження та забезпечення ефективного виконання фази 2 HRMIS НАДС за конкурсним відбором забезпечить найм групи окремих консультантів – спеціалістів з технічної підтримки та підтримки HRMIS, а також спеціалістів з управління проектами та фідуціарних процедур – до команди НАДС з впровадження Проекту. Групу індивідуальних консультантів очолюватиме керівник групи, призначений або законтрактований НАДС. Наразі НАДС шукає досвідченого та кваліфікованого Старшого технічного радника з питань ІТ-безпеки («Консультант») для забезпечення ефективного та надійного налаштування та обслуговування ІТ-безпеки системи HRMIS. Це Технічне завдання («ТЗ») визначає мету, обсяг і тривалість необхідних консультаційних послуг, а також кваліфікаційні вимоги до Консультанта.*

**2. МЕТА**

Метою цього завдання є надання НАДС послуг щодо ІТ-безпеки для впровадження та використання HRMIS. Забезпечення ІТ-безпеки HRMIS здійснюватиметься, в тому числі шляхом адміністрування систем ІТ-безпеки НАДС, які використовуються або впливають на рівень ІТ-захисту HRMIS, та вказані нижче.

**3. ОБСЯГ ПОСЛУГ**

Обсяг послуг, які надає Технічний радник з питань ІТ-безпеки для підтримки впровадження HRMIS, включає (але не обмежується) наступне:

1. Консультація Адміністратора Інформаційної безпеки по виконанню робіт згідно річного плану захисту інформації КСЗІ HRMIS.
2. Контроль за впровадженням оновлень операційних систем HRMIS та баз даних в частині IT-безпеки;
3. Надання попередження про відомі вразливості щодо ІТ-безпеки для всього Проекту, включно для HRMIS;
4. Надання рекомендацій щодо покращення ІТ-безпеки, в тому числі для HRMIS;
5. Оперативне реагування на інциденти для мінімізації потенційних операційних ризиків, а також проведення розслідувань порушень безпеки, і за потреби надання допомоги у правових питаннях, пов'язаних з такими інцидентами.
6. Нагляд за відновленням і відбудовою після інцидентів, пов'язаних із безпекою.
7. Планування та проведення тестування та моніторингу безпеки для забезпечення дотримання політики та операційних гарантій.
8. Тестування вебсервісів ІТ для виявлення загроз безпеці.
9. Тестування інформаційних ресурсів на вразливості безпеки.
10. Співпраця з іншими консультантами Проекту та структурними підрозділами НАДС щодо ІТ-безпеки, в тому числі для HRMIS та координація діяльності технічного радника з питань ІТ-безпеки;
11. Виконання інших завдань Координатора проекту та Керівника групи, що пов’язані з безпекою HRMIS.

**4. ТРИВАЛІСТЬ ТА МІСЦЕ НАДАННЯ ПОСЛУГ**

Послуги будуть надаватися до 11 червня 2025 року включно.

Консультант надає свої послуги на умовах часткової зайнятості.

Послуги можуть надаватися НАДС дистанційно та/або безпосередньо в приміщенні НАДС, лише якщо це дозволяють умови безпеки.

У разі потреби в додаткових послугах та наявності відповідних ресурсів і правових підстав, а також за умови задовільного виконання роботи Консультантом, обсяг послуг, передбачений в розділі 3 ТЗ, може бути переглянуто та/або завдання може бути продовжено за взаємною письмовою згодою між НАДС та Консультантом.

**5. ЗВІТНІСТЬ ТА УМОВИ ВИКОНАННЯ ЗАВДАННЯ**

Консультант повинен вести облік часу, витраченого на виконання цього завдання, і звітувати перед Координатором проекту НАДС у вигляді щомісячних звітів. Ці звіти за формою та деталями, узгодженими із Замовником, містять короткий опис завдань, виконаних Консультантом протягом звітного періоду, та досягнутих результатів і повинні бути подані протягом 5 (п’яти) робочих днів після закінчення звітного періоду. Звіти Консультанта та табелі обліку робочого часу, за відсутності обґрунтованих зауважень зі сторони Замовника, є основою для оплати Консультанту за надані послуги.

Документи, підготовлені Консультантом, можуть бути додані до місячних звітів або надані за запитом Керівника групи або Координатора проекту НАДС. Керівник групи розглядатиме та коментуватиме документи, підготовлені Консультантом, включаючи звіти, перед тим, як вони будуть подані Координатору проекту НАДС.

Консультант готує звітні та інші документи за формою та деталями, які задовольняють вимоги НАДС, українською та англійською мовами (за потреби), у двох примірниках, у друкованому та електронному вигляді. Під час дії воєнного стану всю звітність та інші документи можна подавати лише в електронному вигляді. Тексти електронних документів подаються у форматах Word або PDF.

Консультант працюватиме під керівництвом Керівника групи та в тісній координації з усією командою впровадження Проекту НАДС, консультантами Проекту, а також підтримуватиме контакти з командою проекту Банку. Консультант підпорядковується безпосередньо Координатору проекту НАДС.

Будь-які зауваження та/або претензії до Консультанта щодо наданих послуг повинні бути висловлені НАДС у письмовій формі не пізніше 5 (п’яти) робочих днів з дати подання звітної документації Консультантом. У разі відсутності коментарів та претензій з боку НАДС Сторони підписують Акт прийому-передачі Послуг за цим Договором.

Документи щодо надання послуг за цим ТЗ, підготовлені Консультантом під час виконання завдання, підлягають обговоренню з посадовими особами НАДС, відповідальними за реалізацію Проекту.

**6. ОБОВ’ЯЗКИ ЗАМОВНИКА**

НАДС у межах своєї компетенції надає Консультанту всю необхідну підтримку для виконання Консультантом цього завдання. Зокрема, під час виконання завдання НАДС надасть Консультанту наступне:

1) регламентований доступ до документів, що стосуються підготовки та реалізації Проекту та контракту HRMIS, та інших інформаційних матеріалів, пов’язаних із завданням, якщо це буде потрібно;

2) доступ до приміщень та системи HRMIS (за потреби);

3) робоче місце в приміщенні НАДС з комп’ютером, доступом до мережі Інтернет, принтером, копіювальним апаратом, сканером, витратними матеріалами та канцтоварами;

**7. КВАЛІФІКАЦІЙНІ ВИМОГИ**

Консультант повинен відповідати таким кваліфікаційним вимогам**:**

Обов'язкові вимоги:

1. Вища освіта в галузі комп’ютерних наук, інформаційної безпеки або еквівалентної суміжної галузі;
2. Щонайменше 6 років професійного досвіду в адмініструванні засобів ІТ-безпеки (принаймні антивірусне програмне забезпечення, брандмауер, система запобігання вторгнень);
3. Вільне володіння українською мовою,
4. Поглиблене знання найновіших рішень, інструментів і технологій з ІТ-безпеки, методів атак і вразливостей;
5. Наявність сертифікату спеціаліста з безпеки інформаційних систем (CISSP) або еквівалентного сертифікату;
6. Досвід роботи з архітектурою ІТ-безпеки у великому ІТ-середовищі, включаючи досвід виявлення слабких місць безпеки архітектури на рівні програми, ОС і мережі;
7. Досвід проектування та впровадження рішень з IT-безпеки;

Бажані вимоги:

1. Досвід роботи з адміністрування ІТ або засобів ІТ-безпеки в центральних органах виконавчої влади буде вважатися перевагою;
2. Практичні навички адміністрування широкого спектру ІТ-систем будуть вважатися перевагою;
3. Досвід підготовки інфраструктури та отримання позитивного висновку на Комплексну систему захисту інформації буде вважатися перевагою.
1. Концепція впровадження HRMIS та План заходів (розпорядження Кабінету Міністрів України від 01 грудня 2017 р. № 844-р «Про схвалення Концепції впровадження інформаційної системи управління людськими ресурсами в державних органах та затвердження плану заходів щодо її реалізації» (зі змінами, внесеними від 20 травня 2020 р.); розпорядження Кабінету Міністрів України від 28 грудня 2020 р. № 1343 «Про затвердження Положення про інформаційну систему управління людськими ресурсами в державних органах» (зі змінами, внесеними від 16 вересня 2022 р.). [↑](#footnote-ref-1)