8/05/21-2

Протокол про наміри та співпрацю між ХАРКІВСЬКИМ НАЦІОНАЛЬНИМ УНІВЕРСИТЕТОМ РАДІОЕЛЕКТРОНІКИ та компанією DAI Global LLC

м. Київ, 24 травня 2021 року

Харківський національний університет радіоелектроніки (далі – Університет), як Сторона-реципієнт, та компанія DAI Global LLC (далі – DAI), як Сторона-виконавець, в рамках проєкту Агентства США з міжнародного розвитку (далі – USAID) «Кібербезпека критично важливої інфраструктури України» (далі – «Проєкт»), які надалі разом іменуються як «Сторони», підписали цей Протокол про наміри та співпрацю і тим самим виразили намір співпрацювати над цілями Проєкту, завданнями та очікуваними результатами, що наведені нижче.

1. Цілі та завдання Проєкту

Проєкт «Кібербезпека критично важливої інфраструктури України» – це Проєкт, що фінансується USAID та реалізується за допомогою DAI. До групи партнерів, що залучені до реалізації Проєкту, належать: компанія з дистрибуції передових технологій безпеки «Catalisto», Флоридський міжнародний університет, міжнародна спеціалізована компанія з кібербезпеки «Information Systems Security Partners», компанія «Schweitzer Engineering Laboratories», українська технологічна громадська організація «SocialBoost» та компанія зі стратегічних IT-рішень «Veterans First Initiative».

Метою Проєкту є зробити критично важливу інфраструктуру України стійкішою до кібератак через формування взаємовідносин довіри та співпраці між основними зацікавленими сторонами у сфері кібербезпеки, які представляють органи влади, приватний бізнес, наукову спільноту та громадянське суспільство. Задля досягнення зазначеної мети, в Проєкті передбачено виконання наступної цілі:

- **формування кадрового потенціалу**

Memorandum of Understanding (MoU) Between KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS and DAI Global LLC

Kyiv, May 24, 2021

Kharkiv National University of Radio Electronics (University), as Recipient, and DAI Global LLC (DAI), as Implementer, within the United States Agency for International Development (USAID) Cybersecurity for Critical Infrastructure in Ukraine Activity (the "Project"), who are hereinafter collectively referred to as the "Parties", hereby affirm, by signing this MoU, their intent to cooperate within the Project objectives, tasks, and expected results included below.

1. Project goal and objectives

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity is a Project funded by USAID and implemented by DAI. Additional implementing partners include Catalisto, Florida International University, Information Systems Security Partners, Schweitzer Engineering Laboratories, SocialBoost, and Veterans First Initiative.

The purpose of the Project is to strengthen the resilience of Ukraine's critical infrastructure from cyberattacks by establishing trusted collaboration between key cybersecurity stakeholders in the government, private sector, academia, and civil society. Pursuant to this goal, one of the Project's objectives is to:

- **develop Ukraine's cybersecurity**

України у сфері кібербезпеки: Спрямування зусиль на усунення прогалин у підготовці фахівців задля розвитку нових талантів у сфері кібербезпеки та розбудови потенціалу професіоналів, які вже працюють у сфері кібербезпеки. Керуючись цими цілями, Компонент з розвитку кадрового потенціалу збільшить можливості та якість вищої оствіти у сфері кібербезпеки додатково до покращення знань вже у працюючих професіоналів.

workforce, addressing workforce gaps to develop new cybersecurity talent and build the capacity of existing cybersecurity professionals. Aligned with this objective, the Activity's workforce development component will be increasing the capacity and quality of cybersecurity higher education in addition to upskilling industry professionals.

2. Терміни проведення літніх тренінгів

Сторони виражають намір співпрацювати до 01 вересня 2024 року.

2. Summer Training implementation term

The Parties intend to cooperate over an estimated period of three years from May 2021 to September 01, 2024.

3. Завдання Проєкту

Особливістю компонента з розвитку професійних навичок є співпраця Проєкту з закладами вищої освіти, щоб підвищити спроможність українських університетів викладати програми з кібербезпеки, включаючи надання можливості тренувати практичні навички у віртуальних тренінгових лабораторіях з кібербезпеки.

3. Project tasks

Specific to the workforce development component, the Project's higher education program will expand capacity among Ukrainian universities to deliver cybersecurity courses and degree programs, including practical training opportunities via experiential training virtual Cybersecurity Training Labs.

4. Очікувані результати від реалізації Проєкту (представлені відповідно до Сторони-реципієнта)

За умов наявності фінансування, співпраці та домовленостей із Стороною-реципієнтом,в рамках данного Протоколу про наміри та співпрацю,Проєктом очікується досягти наступні результати в рамках поставлених задач:

- Викладачі з кібербезпеки пройшли підготовку (підвищення кваліфікації), яка дасть їм змогу організувати та проводити навчальний процес у сфері кібербезпеки відповідно до передового досвіду, що також дасть нагоду українським ЗВО збільшити кількість студентів, які навчаються за освітніми програмами з кібербезпеки, розширити масштаби та якість кваліфікаційних та

4. Expected results of the Project implementation (specific to Recipient)

Subject to the availability of funds, cooperation, and agreements with Recipient, the following results of the tasks implemented by the Project under this MoU are expected:

- Cybersecurity instructors prepared for teaching best practice cybersecurity coursework that will allow Ukrainian HEIs to expand the number, scale, and quality of cybersecurity degree and certificate programs capable of developing a talented pool of human capital.

сертифікаційних навчальних програм з кібербезпеки, здатних забезпечити країну талановитими резервами людського капіталу.

- Українські ЗВО перейшли від традиційної педагогіки на основі проведення лекцій до експериментального навчання шляхом затвердження практичних навчальних (тренінгових) програм, що ґрунтуються на наданні студентам доступу до навчальних лабораторій (кіберполігонів), які дадуть їм змогу навчатися та водночас активно розвивати свої навички з визначення та протидії реальному шкідливому програмному забезпеченню в широкому діапазоні мереж з моделюванням реальних ситуацій.

- Ukrainian HEIs transformed from their traditional lecture-based pedagogy to experiential learning through the adoption of practical training programs based on access to academic cyber ranges that allow students to learn while actively identifying and countering real malware in a broad range of simulated networks.

5. Кількісні та/або якісні критерії досягнення ефективності Проєкту

Проєкт має намір створити надійну систему моніторингу та оцінки з метою вимірювання результатів, належного управління заходами Проєкту та розробкою робочого плану. Ключові індикатори стосовно програми вищої освіти включають:

- 4 (чотири) регіональні практичні навчальні лабораторії для підтримки відповідних освітніх програм в рамках вищої освіти з кібербезпеки;
- Кількість університетів, що готують фахівців з кібербезпеки в рамках відповідних навчальних дисциплін та сертифікаційних програм.

5. Quantitative and/or qualitative criteria of achieving the project effectiveness

The Project intends to put in place a robust monitoring and evaluation system to measure results and guide Project activities and work plan development. Key indicators related to the higher education program include:

- Four (4) regional educational labs to support higher education programs on cybersecurity;
- Number of universities offering cybersecurity courses and certifications.

6. Перелік активів, робіт та послуг, прав інтелектуальної власності, інших ресурсів, які планується придбати та забезпечити в рамках Проєкту

За умов наявності фінансування, співпраці та домовленостей із Стороною-реципієнтом, Проєкт має наміри щодо закупівлі товарів та послуг на підтримку:

- Шеститижневої літньої практичної навчальної (тренінгової) програми для

6. Lists of assets, works and services, intellectual property rights, other resources to be purchased and provided under the Project

Subject to the availability of funds, cooperation, and agreements with Recipient, the Project should procure goods and services in support of:

- Six-week summer training program for cybersecurity instructors over three years.

підготовки викладачів (інструкторів) з кібербезпеки, яка проводитиметься протягом трьох років.

- Навчання науково-педагогічних працівників та вдосконалення наявних навчальних дисциплін.
- Проведення регіональних командних змагань студентів із кібербезпеки (так званих змагань із захопленням прапора або CTF змагань) / хакатонів серед ЗВО, які є учасниками навчальної мережі з доступом до практичних навчальних лабораторій (кіберполігонів), запропонованої в рамках програми.
- Проведення будь-яких додаткових регіональних заходів з кібербезпеки, які погоджені обома Сторонами.

- Training of additional faculty and refining of existing courses.
- Hosting of regional student capture the flag (CTF)/hackathon competitions among HEIs participating in a cyber range training network offered by the program.
- Hosting of any additional regional cybersecurity events, as agreed to by both Parties.

7. Очікуваний вплив Проєкту на розвиток економіки та регіону

Очікується, що досягнення цілей Проєкту покращить кіберстійкість України в короткостроковому контексті, а також створить міцну основу для довгострокової незалежності та лідерства країни в сфері кібербезпеки. В рамках визначеного у даному Протоколі компоненту, Проєкт має намір забезпечити Україну фахівцями з кібербезпеки, які зможуть заповнити прогалини у забезпеченні країни талановитими резервами людського капіталу, та зможуть грамотно виявляти і визначати кібератаки, захищати від них, реагувати на них та відновлювати систему після них як в операційних секторах, так і в секторі інформаційних технологій.

7. Expected impact of the project on the development of the economy and region

It is expected that accomplishing the Project objectives should improve short-term cybersecurity resilience in Ukraine and establish a solid foundation for long-term cybersecurity independence and leadership. Specific to this component, the Project intends to equip Ukraine with cybersecurity specialists who can fill in talent gaps, and can competently identify, detect, protect, respond and recover to attacks across both operational and information technology sectors.

8. Зобов'язання Сторони-реалізатора в рамках надання допомоги

За умови наявності коштів, співпраці та домовленостей із реципієнтом, DAI виражає наміри щодо:

- Забезпечення викладачів (інструкторів) та надання навчальної

8. Commitments of the Implementer regarding assistance

Subject to the availability of funds, cooperation, and agreements with recipient, DAI intends to:

- Provide instructors and the learning management platform for conducting online

управлінської платформи для проведення онлайн та офлайн-навчання в літній період протягом наступних трьох років.

- Надання Університету опису навчальної програми із зазначенням дисциплін, які буде запропоновано, та узгодження точної кількості викладачів (інструкторів), які братимуть участь у цьому етапі практичної навчальної програми принаймні за один місяць до початку літніх навчальних модулів.
- Призначення Координатора практичної навчальної програми для вищої освіти, який відповідатиме за координацію Сторін в рамках надання підтримки / проведення заходів.
- Розробки моделі проведення оцінки до та після практичного навчання, спрямованої на інформування / вдосконалення навчання наступного року.
- Покриття витрат на подорожі для студентів, відібраних для участі у регіональних CTF-змаганнях / хакатонах.
- Підтримки інших типів співробітництва на основі регіональних лабораторій, що будуть погоджені обома Сторонами.

or in-person training over the next three summers.

- At least 1 month before the start of the summer training sessions, provide University with a description of the courses that will be offered and agree to the exact number of instructors who will take part in that iteration of the training program.
- Designate a Higher Education Training Coordinator responsible for coordinating the Parties' support/activities.
- Develop pre- and post-training assessments aimed at informing/refining the following year's training.
- Cover travel costs for students selected to compete in the regional CTF/hackathon events.
- Support other types of cooperation based at the regional lab subject to agreement between both Parties.

9. Зобов'язання Сторони-одержувача

Університет виражає наміри щодо:

- Визначення та відбору викладачів (інструкторів) з Університету, які братимуть участь у кожній з трьох запланованих літніх практичних навчальних програм, щонайменше за 2 (два) місяці до початку навчання.
- Призначення відповідального працівника, який буде контактною особою, і, відповідно, координуватиме та організовуватиме направлення на навчання викладачів (інструкторів) з Університету, які братимуть участь у літніх практичних навчаннях.
- Забезпечення здійснення виплат та відшкодувань викладачам (інструкторам) з Університету за час

9. Obligations of the Recipient

University intends to:

- Identify and select the University instructors who will take part in each of the three contemplated summer training programs at least 2 months prior to the start of the training.
- Assign an employee as point of contact (POC) to coordinate and organize the delegation of instructors from University who will take part in the summer training.
- Compensate participating University instructors for the time (6 weeks) they dedicate to the contemplated training.

запланованого практичного навчання (6 тижнів).

- Забезпечення науково-педагогічним працівникам адміністративної та оперативної підтримки для впровадження навчальної методології, що ґрунтується на практиці, про яку наголошуватимуть під час запланованих літніх шкіл.
- Надання допомоги в оновленні навчальної програми та компоненту з практичної підготовки студентів у рамках освітніх програм з кібербезпеки в Університеті.
- Забезпечення інших типів співробітництва, за умови їх погодження Сторонами.

- Provide the administrative and operational support needed for faculty to apply the practice-based learning methodology emphasized in the contemplated summer courses.
- Assist with updating the curriculum and practical-based component of University cybersecurity degree programs.
- Ensure other types of cooperation subject to agreement between the Parties.

Цей Протокол набирає чинності з дня його підписання, виражає наміри Сторін щодо їхньої співпраці та діятиме до 01 вересня 2024 року чи до моменту припинення/відкликання.

This MoU takes effect on the day of its signing, reflects the intentions of the Parties relating to their cooperation, and shall be effective until September 1, 2024, or the moment of termination/withdrawal.

Харківський національний університет радіоелектроніки

підпис / signature

Валерій Семенець
Ректор

Дата: 24.05.21

Kharkiv National University of Radio Electronics

Valerii Semenets
Rector

Date: 24.05.21

DAI / Проєкт USAID «Кібербезпека критично важливої інфраструктури України»

підпис / signature

Тімоті Дубел
Директор Проєкту

Дата: 24.05.21

DAI/USAID Cybersecurity for Critical Infrastructure in Ukraine Activity

Timothy Dubel
Chief of Party

Date: 24.05.21