**Звіт про участь у проекті USAID “Cybersecurity for Critical Infrastructure in Ukraine”**

**КПІ імені Ігоря Сікорського (НН ФТІ, кафедра інформаційної безпеки)**

В рамках співробітництва Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" з USAID в рамках проекту “Cybersecurity for Critical Infrastructure in Ukraine” було досягнуто наступних результатів:

1. Вдосконалено практичну складову програм бакалаврського та магістерського рівня спеціальностей 125 Кібербезпека завдяки інтеграції кіберполігону RangeForce у базові курси професійного циклу. За новими програмами підготовлено більше 430 студентів, отримали професійні навички захисту критичної інфраструктури у складі blue team команд, SOC 1 і 2 рівня.
2. Удосконалено практичну складову програм спеціальності 125 Кібербезпека завдяки інтеграції кіберполігону (Enterprise Dedicated Labs) та академії (Academy) Hack The Box в якості додаткової підготовки за напрямами активної безпеки, тестування на проникнення у складі red team команд. Підготовку проходять більше 40 студентів, успішно здано 6 екзаменів (сертифікації CPTS, CBBH).
3. Підвищено професійний рівень викладачів в рамках серії літніх шкіл проекту -- щорічно приймали участь більше 10 викладачів університету (серед них – викладачі кафедри Ільїн М., Родіонов А., Ільїн К., Стьопочкіна І., Якобчук Д.), а також здобувачі бакалаврських, магістерських освітніх програм та PhD (). Отримані матеріали використані для вдосконалення курсів університету.
4. Університет спільно з USAID та Amazon Web Services провів всеукраїнське змагання з кібербезпеки Sikorsky CTF 2023, в якому прийняло участь більше 260 шкільних та університетських команд (870+ учасників, 156 команд мають ненульовий результат). Це найбільший CTF України за історію існування держави, задав нові стандарти якості завдань, підготовки і організації подібних змагань. Результатом проведення є популяризації професії спеціаліста з кібербезпеки, профорієнтація абітурієнтів, вступників до магістратури та аспірантури. Зокрема, не зважаючи на активні бойові дії на території країни, набір абітурієнтів-випускників шкіл поточного року збільшився на спеціальність 125 Кібербезпека в КПІ імені Ігоря Сікорського, і є найбільшим в країні. У сукупності з сучасними удосконаленими програмами підготовки дає якісний крок підвищення загальнонаціонального рівня кіберстійкості інформаційних систем.
5. В рамках проекту було передано серверне обладнання, що застосовується для проведення практичних занять з цифрової криміналістики (технічний аналіз інцидентів комп'ютерної безпеки), безпеки корпоративних систем на базі Windows Active Directory (тестування на проникнення, аналіз загроз в рамках кіберполігону GOADv2), аналіз шкідливого програмного забезпечення (розгорнуто Cuckoo Sandbox та CAPEv2). Підготовлено більше 100 студентів-учасників гуртка з інформаційної безпеки dcua-school та в рамках курсів підвищення кваліфікації державних службовців-операторів критичної інфраструктури.
6. В рамках проекту передано обладнання Cisco, що заплановано для використання в рамках курсів з безпеки об'єктів критичної інфраструктури -- цикл підготовки аспірантів спеціальності 125 Кібербезпека та курси підвищення кваліфікації для державних структур-операторів критичної інфраструктури.

В довгостроковому форматі проект дав можливість покращити навчальні програми спеціальності 125 Кібербезпека провідного технічного ЗВО країни. Здобуті за допомогою проекту кваліфікації викладачів КПІ імені Ігоря Сікорського дозволяють підвищити рівень підготовки на всіх освітніх рівнях (бакалаврату, магістратури та аспірантури), а також безпосередньо курсах підвищення кваліфікації співробітників компаній-операторів критичної інфраструктури. Надане обладнання забезпечує технічну можливість практичної підготовки спеціалістів на протязі щонайменше 5 років.

Все вищезазначене дозволяє зробити висновок про системний ефект підвищення кіберстійкості критичної інфраструктури на державному рівні, в результаті розвитку кадрового потенціалу операторів та суміжних спеціалістів з кібербезпеки.