Протокол про співробітництво між Українським державним університетом науки і технологій та Компанією «ДАІ Глобал Ел-ел-сі»	**Protocol of cooperation between the Ukrainian State University of Science and Technologies and the Company DAI Global LLC (DAI)**
м. Дніпро «____»_____2023 року	Dnipro «____»_____ 2023
Український державний університет науки і технологій, як Реципієнт (далі – Реципієнт), в особі в.о. ректора Величка Олександра Григоровича, який діє на підставі Статуту, з одного боку, та Компанія **«ДАІ Глобал Ел-ел-сі»** (Компанія «ДАІ»), як Виконавець Проєкту **Агентства міжнародного розвитку США (АМР США) «Кібербезпека критично важливої інфраструктури України»,** (далі – Проєкт), в особі Петра Матіяшека, який діє на підставі довіреності від 22 жовтня 2021 року року, з іншого боку, іменовані надалі - Сторони, керуючись положеннями Закону України "Про основні засади забезпечення кібербезпеки України", підтверджують, шляхом підписання цього Протоколу, угоду щодо цілей, завдань і очікуваних результатів Співробітництва, зазначених нижче.	**Ukrainian State University of Science and Technologies (hereinafter - the Recipient),** represented by Acting Rector Olexandr Velychko, acting on the basis of the Statute, on one hand, and **DAI Global LLC (DAI)**, as the Implementor of the Activity of the **United States Agency for International Development (hereinafter - USAID) "Cybersecurity of Critical Infrastructure of Ukraine", (hereinafter - the Activity),** represented by Petro Matiaszek, acting on the basis of a power of attorney on October 22, 2021, on the other hand, hereinafter referred to as the Parties, guided by the provisions of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", and, confirm by signing this Protocol an agreement on the goals, objectives and expected results listed below.
1. Цілі проєкту Проєкт фінансується АМР США та має двох Бенефіціарів - Міністерство цифрової трансформації України та Апарат Ради національної безпеки і оборони України. Метою Проєкту є посилення стійкості критичної інфраструктури країни до кібератак шляхом розвитку надійного партнерства між основними учасниками процесу підвищення рівня кібербезпеки у галузі державного управління, приватному секторі, а також представниками освітньої галузі і громадянського суспільства. Досягнення цієї мети передбачається шляхом виконання наступних завдань Проєкту: **Розвиток середовища, що сприяє підвищенню рівня кібербезпеки.** Зміцнення правової, регуляторної та інституційної основ кібербезпеки в Україні з метою посилення стійкості системи та її готовності до протидії викликам у відповідності до міжнародних стандартів. **Розвиток трудових ресурсів у галузі кібербезпеки в Україні.** Сприяння	**1.The Purpose** The Activity is funded by USAID and has two Beneficiaries - the Ministry of Digital Transformation of Ukraine and the Office of the National Security and Defense Council of Ukraine. The goal of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity is to strengthen the resilience of the country's critical infrastructure to cyberattacks by developing a reliable partnership between the main participants in the process of improving the level of cybersecurity in the field of public administration, the private sector, as well as representatives of the educational sector and civil society. Achieving this goal is envisaged by performing the following tasks the Activity (tasks the Activity). **Development of the environment that contributes to the improvement of the level of cybersecurity.** Strengthening the legal, regulatory and institutional foundations of cybersecurity in Ukraine in order to strengthen the resilience of the system and its readiness to counter challenges in accordance with international standards and best practices. **Development of human resources in the field of cybersecurity in Ukraine.** Assistance in

вирішенню наявних проблем кадрового забезпечення шляхом залучення компетентних фахівців та професійного розвитку наявних фахівців. **Розбудова стійкої галузі кібербезпеки.** Зміцнення довіри і розвиток співпраці між державним і приватним секторами з метою розробки інноваційних рішень, які обумовлюватимуть виклики у майбутньому. Сприяння розвитку зростанню широкого ринку кібербезпеки в Україні.	solving existing problems of personnel support by involvement of competent specialists and professional development of existing staff. **Building a sustainable cybersecurity industry.** Building trust and developing cooperation between the public and private sectors in order to develop innovative solutions that will be challenged in the future and promote the growth of a broad cybersecurity market in Ukraine.
2. Термін реалізації Проєкту З січня 2023 року по вересень 2025 року.	**2.Term of the Activity** From January 2023 to September 2025.
3. Цілі та напрямки співробітництва Проєкту з Реципієнтом Співробітництво відбувається в рамках завдань Проєкту та фокусується на таких ключових цілях: • підвищення спроможності Реципієнта викладати програми з кібербезпеки, • надання можливості тренувати практичні навички студентів на віртуальних тренінгових платформах із кібербезпеки. Задля забезпечення досягнення поставленої мети співробітництво здійснюється в наступних напрямках: 1) Розвиток технічної спроможності Реципієнта; 2) Надання Реципієнту програмного та апаратного забезпечення за результатами оцінки потреб після повномасштабного вторгнення; 3) Розвиток компетенцій співробітників Реципієнта; 4) Проведення регіональних командних змагань студентів із кібербезпеки; 5) Тренінги з використання технічних платформ та інструментів.	**3. Objectives and directions of cooperation of the Activity with the Recipient** Cooperation takes place within the framework of the main objectives of the Activity and focus on the following key objectives: • increasing the capacity of the Recipient to teach cybersecurity programs; • providing access for students to practice their skills on virtual cybersecurity training platforms. To ensure the achievement of this goal, cooperation is carried out in the following areas: 1) Development of the Recipient's technical capacity; 2) Providing the Recipient with the software and hardware based on the results of needs assessment after the full-scale invasion; 3) Development of the Recipient's employees competencies; 4) Conducting regional student team competitions in cybersecurity; 5) Trainings on effective combined use of technical platforms and tools.
4.Очікувані результати реалізації Співробітництва Проєкту з Реципієнтом • підвищення спроможності співробітників Реципієнта; • підвищення рівня співробітників з питань кібербезпеки і розвиток технічних навичок фахівців Реципієнта; • підвищення кваліфікації викладачів з кібербезпеки; • посилення технічної бази Реципієнта для	**4.Expected results of cooperation implementation of the Activity and the Recipient** • increasing the Recipient's employees capacities; • raising awareness of cybersecurity issues and developing the technical skills of the Recipient's specialists; • refresher courses for trainers on cybersecurity; • strengthening the Recipient's technical capacities for training purposes; • and other short-term and long-term measures in

викладацької діяльності; • інші короткострокові і довгострокові заходи з метою реалізації пріоритетних завдань, визначених спільно Реципієнтом та Проєктом.	order to implement the priority tasks identified jointly by the Recipient and the Activity.
5. Критерії ефективності Співробітництва Проєкт забезпечує створення надійної і ефективної системи моніторингу та оцінювання з метою вимірювання результатів роботи, спрямування подальшої діяльності і забезпечення ефективного планування. Зокрема, Сторони забезпечують моніторинг таких показників: • кількість одиниць обладнання, наданого Реципієнту для навчального процесу; • кількість студентів, які мали змогу навчатися завдяки посиленню технічної бази Реципієнта; • інші показники, визначені спільно Реципієнтом та Проєктом.	**5. Criteria for achieving effectiveness of Cooperation** The Activity ensures the creation of a reliable and effective monitoring and evaluation system in order to measure the results of work, direction further activities and ensuring effective planning. In particular, the Parties shall monitor the following indicators: • number of equipment units provided to the Recipient for training purposes; • number of students had an opportunity to go for training as a result of the Recipient's technical capacities strengthened; • and other indicators defined jointly by the Recipient and the Activity.
6.Активи, роботи, послуги, права інтелектуальної власності та інші ресурси, що придбаватимуться і надаватимуться у рамках Проєкту В рамках співробітництва Проєкт надаватиме послуги щодо покращення технічної бази, підвищення професійної спроможності науково-педагогічних працівників Реципієнта, вдосконалення наявних навчальних дисциплін, та залучення до освітніх програм, курсів підвищення кваліфікації з метою покращення знань, вмінь і навичок у цій сфері.	**6.Assets, works, services, intellectual property rights and other resources to be acquired and provided within the framework of the Activity** As part of the cooperation, the Activity provides assistance to strengthen the Recipient's technical capacities, increase the professional capacity of trainers personnel, improve current study programs, involve in educational programs and refresher courses to improve knowledge, skills and abilities in this area.
7.Очікуваний вплив Проєкту на розвиток економіки і регіону Виконання зазначених завдань покращить підготовку фахівців з кібербезпеки, які зможуть заповнити прогалини у забезпеченні країни талановитими резервами людського капіталу, та зможуть професійно 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.The expected impact of the Activity on the development of the economy and the region** Fulfillment of these tasks will help 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. As a result of the strengthening of the Recipient's cybersecurity, a gradual improvement of the overall cyber instability of the state is ensured, which corresponds to the goals and objectives of the

Цей Протокол складено у 2 (двох) примірниках, кожен з яких має однакову юридичну силу.	This Protocol is drawn up in 2 (two) copies, each of equal legal force.
Цей Протокол набирає чинності з дня його підписання і залишається в силі до вересня 2025 року.	This Protocol shall enter into force on the date of its signing and shall remain in force until September, 2025.
Компанія «ДАІ Глобал Ел-ел-сі», Проєкт «Кібербезпека критично важливої інфраструктури України» (АМР США) _____ Петро Матіяшек Директор Проєкту **Дата**_____ **Український державний університет науки і технологій** _____ Олександр Величко В.о. ректора Дата: 17.04.2023	DAI Global LLC (DAI), USAID Cybersecurity for Critical Infrastructure in Ukraine Activity _____ Petro Matiaszek Chief of Party Date: _____ **Ukrainian State University of Science and Technologies** _____ Olexandr Velychko Acting Rector Date : 17.04.2023