Науково-практична конференція молодих вчених «Кібернетика: теорія та практика» Київського національного економічного університету імені Вадима Гетьмана, присвячена 100-річчю з дня народження В.М. Глушкова

Принцип проведення конференції – робота на практичних секціях з IT-спеціалістами, які вже реалізували себе, розвиваються або тільки починають цікавитися сферою IT.

Основна практична частина.

Для студентів доступні секції (воркшопи, віладжі), в яких надаються можливості для перевірки своїх навичок на практиці, а саме:

1. **Індивідуальний CTF** (англ.Capture the flag) – це змагання, які спрямовані на тестування та підвищення навичок в області кібербезпеки та інформаційної безпеки. У цих змаганнях учасники повинні шукати, знаходити та експлуатувати різні вразливості в комп'ютерних системах та мережах із метою здобуття «прапорців», які підтверджують їх успішний доступ до системи або вирішення завдання.

Завдання: CTF включають в себе такі типи завдань:

a. Web-exploitation: учасники повинні шукати та використовувати вразливості в веб-додатках.
a. Reverse Engineering: учасники аналізують та зворотно розробляють програми, щоб знайти «прапорці» або вразливості.
b. Crypto: розкриття шифрів, розшифровка повідомлень та інші криптографічні виклики.
c. Forensics: відновлення втрачених або видалених даних, аналіз файлових форматів та слідів.
d. Steganography: виявлення прихованих повідомлень в медіафайлах (зображеннях, аудіо тощо).
e. Binary Exploitation: пошук та використання вразливостей у бінарних програмах.

2. **Командний CTF** (Team-based CTF) - це змагання, в яких учасники об'єднуються в команди, щоб спільно розв'язувати завдання з кібербезпеки та інформаційної безпеки.

Склад команди: команди можуть бути з різною кількістю учасників, але не більше чотирьох. Важливо, щоб учасники команди доповнювали один одного з точки зору навичок та вмінь. Зазвичай команди складаються зі спеціалістів із різних областей, таких як: веб-захист, реверс-інженерія, криптографія, програмування тощо.

Час і бали: командні CTF мають обмежений час, після закінчення якого бали нараховуються командам або учасникам у залежності від кількості «прапорців», які вони знайшли та подали.

Правила та етика: у CTF існують правила, що визначають допустимі методи отримання «прапорців».

Безпека та збереження конфіденційності: організатори CTF забезпечують, щоб жодні реальні системи чи дані не були вразливими під час змагань. Усі вразливості створюються спеціально для гри та оберігаються від реального зловмисного використання.

0. **Фізичний хакінг** (англ. Hardware hacking) – робота з друкованими платами, конекторами тощо, для дослідження фізичних вразливостей і впливу відкритих контролерів та з’єднань на платі.

Учасники конференції за допомогою фізичного доступу до макетів матимуть змогу дослідити їх функціонал. Додатково буде надана можливість регулювати роботу макетів за допомогою відкритого коду та віддаленого керування за допомогою протоколу MQTT, ІЧ-передавачів та інших технологій бездротового зв’язку, зокрема, запрограмувати системи різного типу, що розроблені на платформах Arduino, Raspberry PI, ESP.

Учасникам конференції буде надана можливість створювати власні системи та проєкти. Серед досліджуваних проєктів конференції є:

- «Роботизована рука»
- «Клімат-контроль»
- «Пожежна безпека»
- «Охоронна система»
- «Фонтан»
- «Система пропуску»
- «Автоматизована система поливу»
- «Автоматизована система освітлення»
- «Система світлофорів»

- «Метелик-переможець»

Реєстрація може бути проведена через сайт конференції за допомогою kneu.edu.ua акаунтів (наразі проведення планується тільки для студентів ЗВО):

https://docs.google.com/forms/d/10qzmMRtOy9Fe461cIP_O4rSuNJnXcvrXO2b8ZGaqld4/edit?usp=drivesdk

Загальний принцип організації такий, як і у американського DEF CON або OWASP Ukraine, що веде за собою вільне спілкування між «спікерами» та гостями, що надає більше можливостей для обговорення та творчих ідей.

На конференції будуть організовані майстер-класи аспірантами, викладачами та запрошеними фахівцями.

Теми доповідей

№	Тема	Доповідачі
1.	Вступне слово	**Джалладова Ірада Агаверді-кизи**, доктор фізико–математичних наук, професор кафедри системного аналізу та кібербезпеки
2.	Штучний інтелект і його реалізація у прикладних задачах	**Матвійчук Андрій Вікторович**, доктор економічних наук, професор кафедри математичного моделювання та статистики
3.	Мовні моделі LLM	**Дербенцев Василь Джоржович**, кандидат економічних наук, професор кафедри інформатики та системології
4.	Розвиток інформаційних систем та мереж в умовах обмежених ресурсів	**Безкоровайний Віталій Сергійович**, кандидат економічних наук, доцент кафедри інформатики та системології
5.	Популяризація науки в коміксах	**Мамонова Ганна Валеріївна**, кандидат фізико-математичних наук,

		доцент кафедри системного аналізу та кібербезпеки
6.	Забезпечення аутентифікації та авторизації користувачів у клієнт-серверних застосунках	**Лозовик Юрій Миколайович**, кандидат економічних наук, доцент кафедри інформаційних систем в економіці
7.	Вступ до промпт-інжинірингу	**Скіцько Володимир Іванович**, кандидат економічних наук, доцент кафедри математичного моделювання та статистики
8.	Кібервійна: спадок	**Синицький Ростислав Костянтинович**, аспірант кафедри інформаційних систем в економіці

Регламент проведення: 10 хвилин доповіді з ілюстративними матеріалами + 5 хвилин на відповіді на запитання від аудиторії.

Регламент роботи конференції

Час	***Подія***
10^{00} - 10^{15}	Відкриття конференції
10^{15} - 12^{30}	Виступи доповідачів
12^{30} - 13^{00}	Шорт-брейк
13^{00} - 15^{00}	Робота основної практичної частини HACK CON
15^{00} - 15^{30}	Нагородження переможців

Конференція відбудеться 26.10.2023 року в офлайн-режимі у 4-ому корпусі КНЕУ (Наукова бібліотека імені М.В. Довнар-Запольського)
Адреса: м. Київ, вул. Дегтярівська, 49-г, ауд. 201, 604, 605.