

ВСТУП ДО КІБЕРБЕЗПЕКИ

Формат навчання

Курс побудовано на засадах активного навчання: лекції, практичні семінари, симуляції атак і захисту, аналіз кейсів, командні проєкти. Акцент робиться на застосуванні знань у реальному світі та міждисциплінарній взаємодії.

Типові дослідницькі питання курсу:

- Які основні типи кіберзагроз і як від них захищатися?
- Як забезпечити безпеку даних в особистому, корпоративному та державному контекстах?
- Як технології кібербезпеки можуть бути використані для захисту демократії та прав людини?
- Які соціальні, етичні та правові наслідки мають сучасні практики цифрової безпеки?

Оцінювання та підсумок

- Участь у заняттях та практиках (індивідуально; 20%).
- Командний проєкт – аналіз кіберінциденту або моделювання кіберзахисту (групова робота; 40%).
- Індивідуальне есе або дослідницький звіт (40%) – аналіз загроз, політики безпеки або етичні аспекти кібербезпеки.

Вимоги до учасників

Курс відкритий для студентів усіх спеціальностей, особливо корисний для тих, хто вивчає ІТ, право, соціальні науки або управління. Попередня технічна підготовка не є обов'язковою, але вітається.

Форма навчання

Курс «Вступ до кібербезпеки» поєднує теоретичні знання з практичним застосуванням. Він містить лекції, інтерактивні обговорення, симуляції реальних ситуацій, аналіз кейсів, а також групову проєктну роботу, пов'язану з розробкою елементів політик кіберзахисту або моделюванням інцидентів безпеки. Курс орієнтований на міждисциплінарний підхід і розв'язання практичних завдань у команді.

Орієнтовний бюджет часу

Це інтенсивний 10-тижневий курс обсягом 2,5 ECTS, що вимагає регулярного відвідування лекцій і практичних занять, а також активної участі у групових проєктах, які виконуються у позааудиторний час. Загальне навантаження складає близько 70 годин, з яких близько 30 – аудиторна робота і 40 – самостійна підготовка, дослідження і проєктна діяльність.

Результати навчання (згідно з дублінськими дескрипторами):

Після завершення курсу слухачі зможуть:

А. Знати основні поняття кібербезпеки, типи кіберзагроз, принципи захисту інформації та розуміти їх вплив на індивідуальному, організаційному та суспільному рівнях (знання та розуміння).

Б. Застосовувати базові інструменти кіберзахисту у повсякденній цифровій практиці, враховуючи як технічні, так і поведінкові аспекти безпеки (застосування знань і розуміння).

В. Аналізувати сучасні ризики та виклики у сфері кібербезпеки, приймати обґрунтовані рішення щодо цифрової безпеки, зважуючи технічні, етичні, правові й соціальні чинники (критичне мислення, формування суджень).

Г. Працювати в команді над проєктами з моделювання інцидентів, дослідженням кіберзагроз або розробкою елементів політики інформаційної безпеки, ефективно презентуючи результати (комунікативні та колаборативні навички).

Д. Розвинути здатність діяти відповідально у цифровому середовищі: (i) досліджувати виклики та рішення в умовах кіберризиків, (ii) враховувати етичні, правові та демократичні аспекти цифрової взаємодії, (iii) сприяти безпечній та етичній поведінці в Інтернеті (м'які навички, відповідальна цифрова поведінка, вирішення проблем).

Результати навчання за рамкою Луї:

Рамка Луї використовується в освіті EURIDICE для зміцнення загальних – вищого порядку – академічних та особистих результатів навчання. Він заснований на підході AAC&U-Value та прийнятий/адаптований для вищої освіти для впливу на суспільство Альянсом університетів Аврори.

- Критичне мислення
- Етична відповідальність
- Глобальна цифрова грамотність
- Активна участь у цифровому суспільстві

Команда лекторів

- **Марина Єсіна**, к.т.н., доцент, в.о. завідувача кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В.Н. Каразіна (Генеральний керівник курсу): m.v.yesina@karazin.ua.

- **Владислав Вілігура**, PhD, старший викладач кафедри кібербезпеки інформаційних систем, мереж і технологій Харківського національного університету імені В.Н. Каразіна: v.v.vilihura@karazin.ua.

Олена Миколенко (загальний менеджер курсу, olenamykolenko@karazin.ua).

Віртуальний клас

Усі заняття проходитимуть у змішаному форматі з використанням Zoom, Moodle та спеціалізованих кіберсимуляторів (де можливо).

Creative Commons

Усі матеріали цього курсу створюють Марина Єсіна та Владислав Вілігура.