Анотація до курсу «Дії в кіберпросторі»

Під час навчання студенти опановують базові знання про основні дії сучасної людини у кіберпросторі. Зокрема, про основні загрози, які у цифрову добу постають перед нами. Для студентів-медійників важливо також уміти критично оцінювати журналістські матеріали про кіберзлочини у ключі дотримання професійних та етичних стандартів у висвітленні цієї проблематики.

Дисципліна покликана розвивати навички абстрактного мислення, аналізу та синтезу, конкретизувати розуміння комунікаційної мети в кіберпросторі, виявляти та вирішувати проблеми в реалізації медіапроєктів, присвяченим кіберзлочинам, проводити дослідницьку та/або інноваційну діяльність, а також точно і зрозуміло доносити власні висновки.

Завдання (навчальні цілі):

- сформувати поняття про дії людини в кіберпросторі як основу життя та роботи сучасної цифрової людини;
- опанувати базові знання про різновиди кіберзлочинів, їхню еволюцію та їхній вплив на появу, скажімо, антивірусної галузі як критично важливого елемента у системі протидії кіберзлочинності;
- здатність усебічно аналізувати журналістські матеріали про кіберзлочини, пояснювати сильні та слабкі сторони кожного матеріалу у контексті дотримання професійних стандартів журналістики;
- розуміння сучасних механізмів інформаційних шпигунства, тероризму та війни та особливості ведення цих видів діяльності в Інтернеті.

Мета вивчення курсу: сформувати систему знань про основні загрози інформаційній безпеці, кіберзлочинність, способи протидії цим загрозам, а також про те, як висвітлюють поважні медіа проблематику кіберзлочинності.

Структура курсу.

В першому модулі студенти розглядають Загальні питання інформаційної безпеки. *Безпека та конфіденційність користувача в мережі. Війна в кіберпросторі: сучасні стратегії і тактики.*

В другому модулі студентам пропонується опанувати види інформаційних загроз та способи їм протидіяти. *Комп'ютерні віруси та специфіка антивірусних програм: як висвітлюються в медіа. Кібершпигунство та кібертероризм. Даркнет та безпека електронних фінансів.*

Вивчення курсу передбачає систематизацію **знань** про:

Розуміти історичний контекст виникнення кіберзлочинів та основних стадій їх еволюції.

Знати основні види кіберзлочинів та їхні особливості.

Знати механізм здійснення шпигунства, тероризму та комунікативної війни в Інтернеті.

Опанування практичними аспектами курсу передбачає оптимізацію **вмінь** щодо:

Вміти визначати фахову основу кожного журналістського матеріалу про кібер-злочини.

Презентувати результати проведеного проєкту в колективі (робота над порівняльним аналізом двох журналістських розслідувань про кіберзлочини).

Вміння аргументовано відстоювати висновки власного проєкту.

Критично оцінювати й аналізувати джерела, в яких викладені різні стратегії донесення інформації про кіберзлочини, використовувати здобуті знання у професійній діяльності.

Корисні джерела:

1. Митник, К. (2019). Мистецтво залишатись непоміченим. Хто ще читає ваші імейли? Київ: Наш Формат.

2. Гудмен, М. (2019). Злочини майбутнього. Київ: Наш Формат.

3. Senker, C. (2017). Cybercrime and the Darknet. London, UK: Arcturus.