

**Затверджено на засіданні
кафедри правоохоронної діяльності
Протокол №5 від 21 січня 2025 р.**

Тематика індивідуальних завдань з навчальної дисципліни:

«Державна політика в сфері кіберзахисту»

Презентації:

1. Підготуйте презентацію на тему «Співвідношення національної безпеки, інформаційної безпеки та кібербезпеки».
2. Підготуйте презентацію на тему «Кримінологічний портрет кіберзлочинця» або «Типи кіберзлочинців».
3. Підготуйте презентацію на тему «Види кіберзлочинів».
4. Підготуйте презентацію на тему «Роль міжнародних організацій (таких як ООН, ЄС, НАТО, АСЕАН, Інтерпол) у розробці нормативно-правових актів і стандартів для забезпечення кібербезпеки».
5. Підготуйте презентацію на тему «Європейські регламенти та директиви щодо кібербезпеки».

Реферати/есе/аналітичні повідомлення:

1. Здійсніть аналіз сучасних кіберзагроз, які можуть становити небезпеку для національної безпеки України. Розгляньте основні типи кіберзагроз (кібератаки, шкідливе програмне забезпечення, фішинг, інсайдерські загрози) і визначте їхній вплив на стратегічні сфери (енергетика, телекомунікації, фінансовий сектор).
2. Проаналізуйте реальний або гіпотетичний кіберінцидент, що стався в Україні (наприклад, кібератака на енергетичну інфраструктуру чи державні органи). Оцініть його вплив на національну безпеку України та можливі юридичні наслідки для держави та організацій, які постраждали.
3. Оцініть правові аспекти кіберзахисту інфраструктури критичного значення (енергетика, водопостачання, транспорт), яка є важливою для національної безпеки України. Розгляньте питання забезпечення її захисту від кіберзагроз, відповідальності держави та приватних компаній.
4. Здійсніть аналіз поняття кібертероризму в контексті сучасної правової теорії та практики. Як це поняття визначається в міжнародному праві і національному законодавстві України? Розгляньте основні характеристики кібертероризму.
5. Дослідження видів кібертероризму та їх вплив на державну безпеку. Розгляньте такі форми кібертероризму, як кібератаки на інфраструктуру критичного значення, поширення пропаганди та дезінформації через Інтернет, кібернапади на державні органи влади.
6. Дослідження міжнародних зусиль у боротьбі з кібертероризмом, зокрема через Організацію Об'єднаних Націй (ООН), Європейський Союз та інші міжнародні організації. Як міжнародні правові механізми можуть бути використані для протидії кібертероризму?
7. Проаналізуйте національне законодавство України щодо боротьби з кібертероризмом. Як Україна реагує на кібертероризм на рівні державних органів,

правозахисних структур та міжнародної співпраці? Які кроки можна зробити для посилення законодавчої та практичної боротьби з кібертероризмом?

8. Оцініть роль міжнародних організацій (наприклад, ЄС, ООН, НАТО) у забезпеченні кібербезпеки України. Як міжнародні зобов'язання можуть сприяти підвищенню національної безпеки в кіберпросторі? Розгляньте юридичні аспекти співпраці України з міжнародними організаціями в цій сфері.

9. Проаналізуйте організаційну структуру забезпечення кібербезпеки в Україні. Розгляньте роль державних органів, таких як Державна служба спеціального зв'язку та захисту інформації України, Національний координаційний центр кібербезпеки, а також інших органів у сфері забезпечення кіберзахисту.

10. Проаналізуйте нормативно-правове забезпечення кібербезпеки в декількох країнах світу (наприклад, США, Європейський Союз, Китай, Індія, Україна). Визначте основні відмінності в підходах до регулювання кібербезпеки.

**Викладач кафедри політики у сфері боротьби
зі злочинністю та кримінального права**

Максим ЯЦИНА