Затверджено
на засіданні кафедри політики у сфері боротьби
зі злочинністю та кримінального права
протокол №2 від 31 серпня 2022 року

ПРОГРАМОВІ ВИМОГИ ДЛЯ ЗДАЧІ ЗАЛІКУ З ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КІБЕРБЕЗПЕКА ТА МІЖНАРОДНЕ ПРАВО»

І СЕМЕСТР
першого (бакалаврського) рівня вищої освіти
галузі знань 08 «Право», спеціальності 081 «Право»,
ОПП «Міжнародне та європейське право»
Навчально-науковий юридичний інститут

1. Сутність та підходи до визначення поняття «кібербезпека».
2. Ознаки кібербезпеки.
3. Напрямки кібербезпеки.
4. Суб'єкти забезпечення кібербезпеки.
5. Видова характеристика кібербезпеки (види кібербезпеки).
6. Сутність та підходи до визначення поняття «кіберзлочинність».
7. Ознаки кіберзлочинності.
8. Види та класифікації кіберзлочинності.
9. Заходи запобігання кіберзлочинності.
10. Феномен «кібертероризму» та історія його виникнення.
11. Кібертероризм та його поняття.
12. Види кібертероризму.
13. Ознаки кібертероризму.
14. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
15. Кібер-терористичний акт: поняття.
16. Види кібер-терористичних актів.
17. Запобігання кібертероризму.
18. Нормативно-правові документи світового масштабу щодо кібербезпеки.
19. Регіональні нормативно-правові документи (ЄС, Рада Європи, ІНТЕРПОЛ, НАТО) щодо кібербезпеки.
20. Нормативно-правове регулювання кібербезпеки країн Африканського континенту, Латинської Америки та держав Арабського регіону.
21. Історія становлення та формування кібербезпеки ЄС.
22. Нормативно-правові акти ЄС у сфері кібербезпеки (основні положення).
23. Стратегія кібербезпеки ЄС (2013 та 2021): основні положення.
24. Співробітництво у сфері кібербезпеки ЄС-НАТО.
25. Загальна характеристика міжнародно-правової боротьби з кіберзлочинністю.
26. Становлення та розвиток міжнародно-правового регулювання боротьби з кіберзлочинністю.
27. Міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні.
28. Міжнародно-правовий механізм боротьби з кіберзлочинністю на регіональному рівні.

29. Заходи міжнародного співробітництва боротьби з кіберзлочинністю.
30. Поняття та зміст кібербезпеки України.
31. Кібербезпека як складова національної безпеки.
32. Ознаки кібербезпеки України.
33. Види кібербезпеки України.
34. Нормативно-правова основа кібербезпеки в Україні.
35. Характеристика Закону України «Про основні засади забезпечення кібербезпеки в Україні»
36. Характеристика Стратегії кібербезпеки України.
37. Напрями кібербезпеки України.
38. Суб’єкти забезпечення кібербезпеки в Україні: види, повноваження.
39. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки.
40. Сучасний стан кіберзлочинності в Україні.
41. Кримінально-правова охорона кібербезпеки в Україні.
42. Загальна характеристика кримінальних правопорушень передбачених Розділом XVI Особливої частини Кримінального кодексу України.
43. Кваліфікація кримінальних правопорушень проти конфіденційності, цілісності і доступності комп'ютерних даних і систем.
44. Кваліфікація кримінальних правопорушень пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів.
45. Кваліфікація кримінальних правопорушень пов'язаних зі змістом інформації (зокрема, дитяча порнографія, расизм і ксенофобія).
46. Кваліфікація кримінальних правопорушень пов'язаних з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.
47. Методичні основи розслідування кіберзлочинів.
48. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.
49. Організаційно-тактичні основи розслідування кіберзлочинів.
50. Використання спеціальних знань під час розслідування кіберзлочинів.

Керівник навчальної дисципліни:
доктор філософії зі спеціальності 081 Право, асистент Яцина М. О.