Затверджено
на засіданні кафедри політики у сфері боротьби зі злочинністю та кримінального права
протокол №1 від 28 серпня 2023р.

Програмові вимоги
для здачі заліку з навчальної дисципліни
«Кіберзлочинність»
для студентів денної та заочної форм навчання

1. Види запобігання кіберзлочинності:
2. Види кримінальних правопорушень, які посягають на конфіденційність, цілісность та доступність інформації, даних і систем.
3. Видова характеристика кіберзлочинності та її структура.
4. Використання спеціальних знань під час розслідування кіберзлочинів.
5. Державна політика у сфері забезпечення кібербезпеки.
6. Детермінанти кіберзлочинності.
7. Загальна характеристика кіберзлочинів пов’язаних з контентом.
8. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
9. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісность та доступність інформації, даних і систем.
10. Загально-соціальне запобігання кіберзлочинності.
11. Запобігання кібертероризму.
12. Індивідуальне запобігання кіберзлочиннам.
13. Кібер-терористичний акт: поняття та види.
14. Кібербезпека України в умовах дії правового режиму воєнного часу.
15. Кіберзлочини що посягають на громадський порядок та моральність.
16. Кіберзлочини які посягають на авторитет органів державної влади.
17. Кіберзлочини, які вчиняються службовими особами.
18. Кіберзлочинність неповнолітніх.
19. Кіберзлочинність під час правового режиму воєнного стану.
20. Кіберзлочинність у сфері економіки.
21. Кіберзлочинність у сфері національної безпеки.
22. Кіберзлочинність як соціально-правове явище сучасного світу, її поняття та ознаки.
23. Кібертероризм: поняття та ознаки, види.
24. Корисливий кіберзлочини.
25. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особоивої частини Кримінального кодексу України.

26. Кримінально-правова хзарактеристика та види кіберзлочинів пов’язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).

27. Кримінально-правова хзарактеристика та види кіберзлочинів пов’язаних з контентом: порнографії, ненависті, жорстокості, расизу і ксенофобії; авторських та суміжних прав.

28. Методичні основи розслідування кіберзлочинів.

29. Міжнарожне співробітництво у запобіганні кіберзлочинності.

30. Місце кіберзлочинності у структурі системі злочинності, її показники.

31. Напрями кібербезпеки України.

32. Наукове і практичне значення вивчення особистості кіберзлочинців.

33. Нормативно-правова основа кібербезпеки в Україні.

34. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.

35. Організаційно-тактичні основи розслідування кіберзлочинів.

36. Особливості кібершахрайства.

37. Поняття і система запобігання кіберзлочинності.

38. Поняття кібершпигунства.

39. Поняття особи кіберзлочинця.

40. Причини та умови кримінальних праопорушень проти конфеденційності цілісності та доступності інформації, даних і систем.

41. Спеціально кримінологічне запобігання кіберзлочинності.

42. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).

43. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки.

44. Структура особистості кіберзлочинця (соціально-демографічні ознаки та морально-психологічні якості).

45. Суб’єкти забезпечення кібербезпеки в Україні: види, повноваження.

46. Суб'єкти запобігання кіберзлочинності (їх система та функції).

47. Сучасна кібербезпека України: поняття, зміст, ознаки.

48. Типологія кіберзлочинності.

49. Феномен «кібертероризму» та історія його виникнення.

50. Характеристика кримінальних правопорушень передбачених у 16-му розділі особливої частини Кримінального кодексу України.

Керівник навчальної дисципліни
доктор філософії зі спеціальності «Право»,
асистент кафедри політики боротьби зі
злочинністю та кримінального права Яцина М. О.