ТЕМИ
КУРСОВИХ РОБІТ
з навчальної дисципліни
«Актуальні питання кримінально-правової та кримінологічної характеристики кіберзлочинності в Україні»

1. Проблеми кримінально-правової охорони власності в сучасних умовах інформатизації суспільства.
2. Проблеми кримінально-правової охорони інтересів правосуддя за допомогою мережі Інтернет.
3. Кримінологічна характеристика кіберзлочинності.
4. Кіберзлочинність: її детермінація та запобігання.
5. Феномен кіберзлочинності в сучасній кримінологічній теорії.
6. Кримінально-правова характеристика кіберзлочинності в Україні.
7. Загальнотеоретичні засади правового регулювання боротьби з кіберзлочинністю.
8. Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні.
9. Теоретико-правові основи боротьби з кіберзлочинністю.
10. Кіберзлочинність в Україні: причини, наслідки та шляхи протидії.
11. Протидія кіберзлочинності як складова національної безпеки держави.
12. Стан та особливості кіберзлочинності в Україні.
13. Фішинг як найпоширеніший вид шахрайства в Інтернеті: види та сутність.
14. Проблеми нормативно-правового регулювання у сфері застосування новітніх інформаційних технологій.
15. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами.
16. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов’язані з фінансовоекономічною сферою відносин у кіберпросторі.
17. Розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, пов’язаних з державнополітичною сферою відносин суб’єктів у кіберпросторі.
18. Розслідування злочинів, вчинених з соціальноекономічних мотивів, що пов’язаних з соціальною сферою відносин суб’єктів у кіберпросторі.
19. Поняття кіберзлочинів та їх класифікація в Європейській конвенції по боротьбі з кіберзлочинністю.
20. Джерела інформації про кіберзлочин, виявлення кіберзлочинів як напрямок правоохоронної діяльності.
21. Конвенція Ради Європи про кіберзлочинність як основа кримінально-правової охорони суспільних відносин у кіберпросторі в України.
22. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
23. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

24. Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату.
25. Сутність понять “комп’ютерний злочин”, “кіберзлочин”, “злочини у сфері ІТ-технологій” та “злочини у сфері комп’ютерної інформації”: теоретичні та нормативні позиції вказаних термінів в Україні та за кордоном.
26. Діяльність кіберполіції в Україні щодо запобігання кіберзагрозам національній безпеці.
27. Основні галузі права для регулювання відносин у кіберпростір в Україні: проблема міжгалузевих питань та шляхи їх вирішення.
28. Основи правового регулювання відносин у кіберпросторі в сфері незаконного наркообігу та торгівлі іншими товарами, що мають особливий порядок обігу в Україні та світі.
29. Зміст суспільних відносин, що виступають об’єктом злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв'язку.
30. Загальна характеристика ознак суб’єктивної сторони складів злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.
31. Загальна характеристика ознак суб’єктів складів злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.
32. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку».
33. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут».
34. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації».
35. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї».
36. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється».
37. Об’єктивна сторона та кваліфікуючі ознаки складу злочину «Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку».

38. Фактори зростання кількості злочинів і правопорушень в сфері високих технологій.
39. Визначальні фактори при прийнятті рішень потерпілими від злочинів у сфері високих технологій. Норми, що рекомендовані до включення в національне законодавство Рекомендацією RNo 89 «Про комп'ютерну злочинність».
40. Які правопорушення відповідно до Конвенції «Про кіберзлочинність» відносяться до комп'ютерних злочинів.
41. Класифікація комп'ютерних правопорушень за міжнародним кодифікатором Інтерполу.
42. Форми співпраці країн СНД у сфері боротьби з комп'ютерними злочинами.
43. Загальна характеристика злочинів у сфері високих технологій відповідно до законодавства Англії.
44. Загальна характеристика злочинів у сфері високих технологій відповідно до законодавства Іспанії.
45. Загальна характеристика злочинів у сфері високих технологій відповідно до законодавства Швейцарії.
46. Загальна характеристика злочинів у сфері високих технологій відповідно до законодавства США.
47. Два основних напрямки формування системи правоохоронних органів здійснюють боротьбу зі злочинами у сфері високих технологій.
48. Загальна характеристика системи правоохоронних США здійснюють боротьбу з комп'ютерними злочинами.
49. Загальна характеристика системи правоохоронних органів України, що здійснюють боротьбу зі злочинами у сфері високих технологій.
50. Типові моделі різних категорій злочинців, які скоюють злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
51. Статистична характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
52. Основні напрямки профілактика і припинення злочинів у сфері високих технологія.
53. Основні напрямки вдосконалення українського національного законодавства про відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
54. Кіберзлочинність як складова кібернебезпеки.
55. Основні види кіберзлочинності.
56. Глобальні тенденції в галузі використання технологій та підключення до Інтернету.
57. Офіційні механізми міжнародного співробітництва у сфері боротьби з кіберзлочинністю.
58. Неофіційні механізми міжнародного співробітництва у сфері боротьби з кіберзлочинністю.
59. Стратегії кібербезпеки: основні особливості.
60. Національні стратегії кібербезпеки: життєві цикли, передова практика та репозиторії.

61. Заходи забезпечення кібербезпеки та зручність використання комп’ютерами та інформаційними мережами.
62. Ситуаційне попередження кіберзлочинів.
63. Криміналістичні та кримінологічні особливості кіберзлочинності.
64. Організаційно-правові засади боротьби із кіберзлочинністю: Україна та світ.
65. Механізми міжнародного співробітництва у сфері боротьби з кіберзлочинністю: проблеми та шляхи їх вирішення.