Питання до іспиту

з навчальної дисципліни «Цифрові технології в правоохоронній діяльності»

1. Поняття інновацій та інноваційних методів у правоохоронній діяльності.
2. Криміналістична інновація: сутність та приклади.
3. Роль цифрових технологій у підвищенні ефективності правоохоронної діяльності.
4. Основні напрями впровадження інновацій у діяльність правоохоронних органів.
5. Переваги використання цифрових технологій у досудовому розслідуванні.
6. Основні ризики та етичні проблеми цифровізації правоохоронної діяльності.
7. Поняття інформаційно-аналітичного забезпечення діяльності Національної поліції України.
8. Єдина інформаційна система МВС України: призначення та структура.
9. Інформаційний портал Національної поліції України: мета створення та функції.
10. Підсистема «Єдиний облік»: значення для реєстрації кримінальних правопорушень.
11. Підсистема «Гарпун»: призначення та практичне застосування.
12. Значення цифровізації досудового розслідування для діяльності слідчого.
13. Поняття електронних (цифрових) доказів у кримінальному провадженні.
14. Види цифрових доказів та їх загальна характеристика.
15. Джерела отримання електронних доказів.
16. Вимоги належності та допустимості цифрових доказів.
17. Особливості електронного документа як доказу.

18. Контрольні (хеш-) суми та їх значення для збереження цілісності даних.
19. Процесуальні дії щодо виявлення та вилучення цифрових доказів.
20. Основні принципи роботи з цифровими доказами.
21. Поняття OSINT та його місце в правоохоронній діяльності.
22. Основні джерела інформації в OSINT-дослідженнях.
23. Основні напрями використання OSINT у кримінальних розслідуваннях.
24. Переваги та обмеження OSINT як інструменту збирання інформації.
25. Етичні та правові вимоги при використанні OSINT.
26. Поняття біометрії та біометричних даних.
27. Основні види біометричної ідентифікації особи.
28. Використання біометричних технологій у діяльності правоохоронних органів.
29. Біометричні реєстри та інформаційні системи МВС України.
30. Переваги та ризики застосування біометричних технологій.
31. Поняття спеціальних знань у кримінальному провадженні.
32. Форми використання спеціальних знань у сфері цифрових технологій.
33. Поняття та процесуальний статус спеціаліста у кримінальному провадженні.
34. Роль ІТ-спеціаліста під час роботи з цифровими доказами.
35. Взаємодія слідчого та спеціаліста під час проведення слідчих дій.
36. Поняття цифрової ідентифікації особи.
37. Електронний підпис: сутність та правове значення.
38. Поняття криптографії та її призначення.
39. Хеш-функції та їх роль у забезпеченні цілісності інформації.
40. Використання криптографічних засобів у правоохоронній діяльності.
41. Поняття економічної безпеки держави.
42. Роль цифрових технологій у забезпеченні економічної безпеки.
43. Використання державних реєстрів у боротьбі з корупцією.

44. Система електронного декларування як антикорупційний інструмент.
45. Значення цифрових закупівель (Prozorro) для протидії корупції.
46. Поняття безвісти зниклої особи в умовах збройного конфлікту.
47. Єдиний реєстр осіб, зниклих безвісти: призначення та значення.
48. ДНК-ідентифікація у встановленні осіб, зниклих безвісти.
49. Використання OSINT у розшуку зниклих осіб.
50. Проблеми та виклики ідентифікації осіб в умовах війни.
51. Поняття воєнних злочинів у міжнародному праві.
52. Роль цифрових технологій у документуванні воєнних злочинів.
53. Використання відкритих джерел у розслідуванні воєнних злочинів.
54. Міжнародні платформи та бази даних для фіксації воєнних злочинів.
55. Значення цифрових доказів у міжнародних кримінальних провадженнях.
56. Поняття організованої та транснаціональної злочинності.
57. Роль Інтерполу в протидії транснаціональній злочинності.
58. Інформаційні системи та банки даних Інтерполу.
59. Європол та його інформаційно-аналітичні системи.
60. Значення міжнародного інформаційного співробітництва у боротьбі зі злочинністю.