

Питання на іспит

з навчальної дисципліни «Розслідування комп'ютерних злочинів»

1. Поняття комп'ютерних злочинів та їх кримінально-правова характеристика.
2. Криміналістична класифікація комп'ютерних злочинів.
3. Склад, структура та особливості криміналістичної характеристики комп'ютерних злочинів.
4. Поняття й сутність комп'ютерних об'єктів в криміналістичній характеристиці злочинів.
5. Способи використання комп'ютерних технологій у злочинній діяльності.
6. Особа комп'ютерного злочинця.
7. Загальна модель (схема) виявлення та розслідування несанкціонованого доступу до інформації в автоматизованих системах.
8. Встановлення факту несанкціонованого доступу до інформації в автоматизованих системах.
9. Встановлення місця несанкціонованого доступу до інформації в автоматизованих системах.
10. Встановлення часу несанкціонованого доступу до інформації в автоматизованих системах.
11. Встановлення способу несанкціонованого доступу до інформації в автоматизованих системах.
12. Встановлення осіб, що вчинили несанкціонований доступ до інформації в автоматизованих системах.
13. Встановлення ступеня провини та мотивів щодо осіб, які вчинили несанкціонований доступ до інформації в автоматизованих системах.
14. Встановлення шкідливих наслідків несанкціонованого доступу до інформації в автоматизованих системах.
15. Виявлення обставин, які сприяли несанкціонованому доступу до інформації в автоматизованій системі.
16. Поняття слідів комп'ютерних злочинів та їх криміналістична класифікація
17. Особливості механізму слідоутворення при вчиненні комп'ютерних злочинів.
18. Типові слідоутворюючі ознаки злочинної діяльності в телекомунікаційних системах.
19. Віртуальний слід в генезі наукових уявлень про механізм слідоутворення.
20. Криміналістичні особливості формування віртуальних слідів.
21. Основні слідчі версії, що висувуються при розслідуванні комп'ютерних злочинів.
22. Основні ситуації початкового етапу розслідування комп'ютерних злочинів.
23. Огляд місця події та комп'ютерних об'єктів.
24. Обшук та виїмка комп'ютерних об'єктів.
25. Допит. Тактика допиту при перевірці «цифрового алібі».
26. Відтворення обстановки та обставин події при розслідуванні комп'ютерних злочинів та слідчий експеримент.
27. Предмет посягання створення та використання шкідливих програм для ЕОМ.
28. Обстановка вчинення злочину створення та використання шкідливих програм для ЕОМ.
29. Особа злочинця створення та використання шкідливих програм для ЕОМ.
30. Особа потерпілого створення та використання шкідливих програм для ЕОМ.
31. Особливості мотивів та мети створення та використання шкідливих програм для ЕОМ.
32. Спосіб вчинення створення та використання шкідливих програм для ЕОМ.

33. Особливості проведення огляду при розслідуванні створення та використання шкідливих програм для ЕОМ.
34. Особливості проведення обшуку та виїмки при розслідуванні створення та використання шкідливих програм для ЕОМ.
35. Особливості проведення допиту при розслідуванні створення та використання шкідливих програм для ЕОМ.
36. Предмет, об'єкт та класифікація СКТЕ.
37. Систематизація експертних завдань, що вирішуються СКТЕ.
38. Основні можливості СКТЕ.
39. Сучасний стан СКТЕ.
40. Правові основи призначення експертизи.
41. Особливості призначення та проведення СКТЕ.
42. Оцінка висновків експерта при проведенні СКТЕ.
43. Процесуальні проблеми проведення СКТЕ.
44. Поняття спеціальних знань. Спеціальні знання, які використовуються при розслідуванні комп'ютерних злочинів.
45. Форми використання спеціальних знань при розслідуванні комп'ютерних злочинів.
46. Особливості участі спеціаліста в окремих слідчих діях при розслідуванні комп'ютерних злочинів.
47. Комп'ютерні технології збирання і дослідження слідів комп'ютерних злочинів.
48. Сутність, засоби та способи діагностування комп'ютерних засобів і систем.
49. Класифікація типових об'єктів СКТЕ.
50. Судово-експертні дослідження текстових файлів.
51. Види та способи представлення програмних засобів на СКТЕ
52. Основні засоби та методи дослідження програмних об'єктів СКТЕ.
53. Експертні завдання, що вирішуються при дослідженні інформації, пов'язаної з роботою в мережі Інтернет.
54. Опис та характеристика деяких об'єктів дослідження інформації, пов'язаної з роботою в мережі Інтернет.
55. Послідовність дій експерта СКТЕ при дослідженні інформації, пов'язаної з роботою в мережі Інтернет.
56. Основні відомості про криптографічний захист комп'ютерних даних.
57. Актуальні аспекти експертного дослідження захищеної інформації в архівах і офісних програмах.
58. Проблеми проведення судово-експертного дослідження комп'ютерної інформації, яка захищена стеганографічними засобами.
59. Правові та організаційно-технічні заходи попередження комп'ютерних злочинів.
60. Міжнародне співробітництво у боротьбі з комп'ютерними злочинами.