МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

ПРОГРАМА

навчальної дисципліни «*Поліцейська діяльність у кіберсфері*»
***вибіркових* компонент**
освітньої програми *першого* рівня вищої освіти

125 Кібербезпека (протидія кіберзлочинності)

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки
(*протокол від 15.09.2020 № 16*)

Розробник:
Доцент кафедри інформаційних технологій та кібербезпеки, к.ю.н., доцент
Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент;

Янович Ю.П., декан факультету права та підприємництва Харківського університету, к.ю.н., доцент.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма *вибіркової* навчальної дисципліни складена відповідно до освітньої програми *першого* рівня вищої освіти *спеціальності «Кібербезпека» спеціалізації «Протидія кіберзлочинності».*

Предметом вивчення навчальної дисципліни є особливості використання комп'ютерних технологій працівниками поліції з метою виявлення, попередження та розслідування злочинів.

Міждисциплінарні зв'язки: «Кібербезпека», «Оперативно-розшукова діяльність», «Цифрова криміналістика».

Програма навчальної дисципліни складається з таких тем:

1. Засадничі принципи протидії кіберзлочинності.
2. Оперативне маскування у кіберсфері.
3. Кримінальна розвідка.
4. Особливості використання технологій під час попередження та розслідування кіберзлочинів.
5. Оперативно-технічні засоби.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «Поліцейська діяльність у кіберсфері» є засвоєння курсантами особливостей використання комп'ютерних технологій працівниками поліції під час виявлення, попередження та розслідування злочинів.

1.2. Завданнями вивчення дисципліни «Поліцейська діяльність у кіберсфері» є дослідження принципів та методів протидії кіберзлочинам (визначення, класифікація, організаційні основи, нормативно-правова база застосування, типові схеми), ознайомлення з міжнародним досвідом протидії кіберзлочинності (особливості протидії кіберзлочинності у країнах з англо-саксонською та романо-германською системами права), засвоєння моделей поліцейської розвідки, методів і способів оперативного маскування у кіберсфері, набуття знань і навичок використання технологій під час попередження та розслідування кіберзлочинів.

1.3. Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- визначення, ознаки та класифікацію кіберзлочинів;
- нормативно-правову базу протидії кіберзллочинності;
- організаційну структуру протидії кіберзлочинності правоохоронним органами в Україні та за її межами;
- особливості організації і тактики оперативного маскування під час роботи в інформаційно-телекомунікаційних системах;
- моделі поліцейської розвідки;
- технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події;
- методи встановлення IP-адреси;

- визначення, ознаки та класифікацію оперативно-технічних засобів;
- характеристики та способи використання оперативно-технічних засобів;
- нормативно-правову базу використання оперативно-технічних засобів;
- основні принципи застосування оперативно-технічних засобів;

вміти:

- застосовувати норми законодавства у протидії кіберзлочинності;
- визначати методи протидії конкретним кіберзлочинам;
- використовувати зарубіжний досвід у протидії кіберзлочинності;
- застосовувати прийоми оперативного маскування у кіберсфері;
- здійснювати віддалений збір інформації про вузли комп'ютерної мережі;
- шукати інформацію про об'єкти в мережі;
- аналізувати профілі соціальних мереж та поштові повідомлення;
- встановлювати інформацію про фінансові інструменти;
- застосовувати різні види оперативно-технічних засобів;
- створювати макети окремих оперативно-технічних засобів;
- використовувати оперативно-технічні засоби в конкретній оперативно-розшуковій ситуації;
- моделювати окремі етапи застосування оперативно-технічних засобів;

бути ознайомленими

- з особливостями функціонування комп'ютерних мереж, веб-технологій, засобів комунікації, мережних засобів зберігання інформації, фінансових комп'ютерних технологій;
- зі сферою застосування оперативно-технічних засобів.

1.4. Форма підсумкового контролю залік, екзамен

На вивчення навчальної дисципліни відводиться 270 годин / 9 кредитів ECTS.

1.5. Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень	
Загальні компетентності (ЗК)	ЗК.3	Знання та розуміння предметної області та розуміння професії
	ЗК.5	Навички використання інформаційних і комунікаційних технологій
	ЗК.6	Здатність до пошуку, обробки та аналізу інформації з різних джерел
Спеціальні (фахові, предметні) компетентності (ФК)	ФК.7	Здатність здійснювати пошук і фіксацію фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена кримінальним законодавством, а також отримувати інформацію в інтересах безпеки громадян, суспільства і держави
	ФК.10	Здатність здійснювати документування під час

		проведення оперативно-розшукових та оперативно-технічних заходів у кіберсфері, використовувати оперативну інформацію при їх проведенні
	ФК.11	Здатність застосовувати тактику розкриття та виявлення злочинів у кіберсфері
	ФК.12	Здатність до збирання, оцінки, систематизації та аналізу інформації для вирішення завдань кримінальних розслідувань

2. Короткий опис змісту навчальної дисципліни

Тема № 1. Засадничі принципи протидії кіберзлочинності.

Об’єкти та суб’єкти протидії кіберзлочинності. Організаційно-правові засади протидії кіберзлочинності. Міжнародний досвід протидії кіберзлочинності.

Тема № 2. Оперативне маскування у кіберсфері.

Поняття, суб’єкти та підстави застосування оперативного маскування. Забезпечення анонімності під час роботи в інформаційно-телекомунікаційних системах. Термінологічні особливості спілкування у кіберпросторі. Легендування профілів користувача для використання у кіберсфері.

Тема № 3. Кримінальна розвідка.

Аналітична робота у протидії кіберзлочинності. Розвідка з відкритих джерел (OSINT).

Тема № 4. Особливості використання технологій під час попередження та розслідування кіберзлочинів.

Мережні технології. Мережні засоби зберігання інформації. Фінансові комп’ютерні технології. Технічні особливості огляду засобів комп’ютерної техніки, виявлених на місці події. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери.

Тема № 5. Оперативно-технічні засоби.

Основні положення щодо оперативно-технічних засобів. Технічні канали витоку інформації. Сигналізація та методи її нейтралізації. Класифікація та методи подолання запірних пристроїв.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.

2. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.

3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.

4. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.

5. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.

6. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.

7. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.

8. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

9. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.

10. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.08.2020).

11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.

12. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.

13. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.

Допоміжна

14. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.

15. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.

16. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.

17. Mccoy M. Collection and Preservation of Digital Evidence / Mark Mccoy, Rachael Elliott // The Detective's Handbook / edited by John A. Eterno, Cliff Roberson. London, New-York : CRC Press, 2015. 358 с.

18. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.

19. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.

20. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. Vol. 13, Iss. 1. pp. 5–11 (DOI: 10.1093/police/pax057).

21. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.

22. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.

23. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.

24. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.

25. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.

26. Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ ; Незалеж. асоц. банків України, Харк. банк. союз. регіон. представник НАБУ. Х. : ХНУВС, 2013. С. 20-23.

27. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практ. конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського нац. ун-ту внутр. справ. 2008. С. 151-153.

28. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.

29. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

30. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.

31. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.

32. Панасюк І.В. Робота з великими текстовими масивами у правоохоронних органах // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 192–193.

33. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.

34. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.

35. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.

36. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.

37. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.

38. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265. *Українська інвестиційна газета*. 2007. № 44, 11.

39. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 10.08.2020).

40. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.08.2020).

41. Манжай О. В, Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

42. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen. *Journal of Criminal Justice*. 2014. № 42. pp. 433-442.

43. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с.

URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.08.2020).

44. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.

45. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.

Інформаційні ресурси в Інтернеті

46. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2017).

47. cyberpolice.gov.ua.

48. Comissioner’s Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html(дата звернення: 31.07.2020).

49. Contents - EasyPatterns 2.5. URL: https://www.datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm (дата звернення: 09.09.2019).

50. FBI: Woman Posted Craigslist and Seeking Killer for Lover’s Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 03.08.2020).

51. hackthebox.eu.

52. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.08.2020).

53. Mission & Priorities. URL: https://www.fbi.gov/about/mission (дата звернення: 03.08.2020).

54. Monette H. Herrera NBI creates crime unit to capture cybercrime violators URL: http://www.pia.gov.ph/news/index.php?article=1901353660025 (дата звернення: 10.12.2018).

55. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.12.2018).

56. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. URL: https://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication (дата звернення: 03.08.2020).

57. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers. 25 p. URL: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf (дата звернення: 10.08.2020).

58. Robertson N. Documents reveal al Qaeda’s plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister. URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.12.2018).

59. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2020).

60. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1 (дата звернення: 10.12.2018).

61. Skype URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 10.07.2020).

62. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.07.2020).

63. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.08.2020).

64. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.07.2020).

65. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.07.2020).

66. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 10.07.2020).

67. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.07.2020).

68. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.07.2020).

69. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.08.2020).

70. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.08.2020).

71. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html (дата звернення: 10.08.2020).

72. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.08.2020).

73. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 12.06.2017).

74. 互联网信息服务管理办法（国务院令第292号）. URL: http://www.gov.cn/gongbao/content/2000/content_60531.htm (дата звернення: 03.08.2020).

4. Засоби оцінювання здобувачів вищої освіти

1. Використання комп’ютерних технологій під час вчинення кримінальних правопорушень.
2. Поняття та способи вчинення кіберзлочинів.
3. Нормативно-правова база боротьби з кіберзлочинністю.
4. Суб’єкти боротьби з кіберзлочинністю.
5. Завдання підрозділів боротьби з кіберзлочинністю.
6. Функції підрозділів боротьби з кіберзлочинністю.
7. Типові схеми здійснення кіберзлочинів.
8. Визначення поняття «кіберпростір», його ознаки.
9. Вчинення злочинів через кіберпростір.
10. Питання визначення компетенції правоохоронних органів у кіберпросторі.
11. Шляхи конвергенції організованої злочинності та кіберпростору.
12. Цілодобова мережа для здійснення контактів з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.
13. Український досвід регулювання питання здійснення оперативно-розшукових заходів шляхом використання кіберпростору.
14. Органи боротьби з кіберзлочинністю в різних країнах.
15. Боротьба зі злочинністю з використанням комп’ютерних технологій у російському законодавстві та в теорії оперативно-розшукової діяльності.
16. Інструменти здійснення оперативно-розшукових заходів через кіберпростір у США.
17. Зміст онлайнової секретної операції в США.
18. Правила онлайнових розслідувань США.
19. Боротьба з кіберзлочинністю у ФРН та загальний порядок здійснення проникнення за допомогою технічних засобів у інформаційно-технічні системи, що використовуються підозрюваним.
20. Використання комп’ютерних технологій в негласній роботі правоохоронних органів Великої Британії та КНР.
21. Поняття, суб’єкти та підстави застосування оперативного маскування.
22. Забезпечення анонімності під час роботи в інформаційно-телекомунікаційних системах.
23. Термінологічні особливості спілкування у кіберпросторі.
24. Легендування профілів користувача для використання у кіберсфері.
25. Загальний порядок пошуку інформації правоохоронними органами про об’єкти в мережі.
26. Поняття, структура та класифікація комп’ютерних мереж.
27. Адресація в комп’ютерних мережах.
28. Загальний порядок пошуку інформації правоохоронними органами

про об’єкти в мережі.

29. Документування інформації з вебсайтів та дощок оголошень.
30. Документування інформації з комп’ютерних соціальних мереж.
31. Встановлення відправника електронних поштових повідомлень.
32. Емейл-трекінг.
33. Види мультимедійних засобів спілкування.
34. Ідентифікація володільців облікових записів мультимедійних засобів спілкування.
35. Тимчасове збереження даних.
36. Загальна інформація про бази даних.
37. Банки даних Національної поліції України.
38. Хмарні сховища.
39. Peer-to-peer.
40. FTP та відеохостинги.
41. Електронні гроші та Інтернет орієнтовані платіжні системи.
42. Головні способи легалізації коштів.
43. Огляд стандартних засобів комп’ютерної техніки.
44. Огляд мобільних засобів комп’ютерної техніки із функцією телефону.
45. Огляд автомобільних засобів комп’ютерної техніки.
46. Особливості використання комп’ютерних технологій в негласній роботі Національної поліції України.
47. Сенс кримінальної розвідки.
48. Стратегії кримінальної розвідки.
49. Види кримінальної розвідки.
50. Стратегічна кримінальна розвідка.
51. Інструменти і методи стратегічної кримінальної розвідки.
52. Тактична кримінальна розвідка.
53. Інструменти і методи тактичної кримінальної розвідки.
54. Оперативна кримінальна розвідка.
55. Інструменти і методи оперативної кримінальної розвідки.
56. Засоби кримінальної розвідки.
57. Застосування методології Anacapa у кримінальній розвідці.
58. Етапи кримінальної розвідки.
59. Постановка завдань як етап здійснення кримінальної розвідки.
60. Збирання даних як етап здійснення кримінальної розвідки.
61. Оцінка даних як етап здійснення кримінальної розвідки.
62. Системи оцінки 4x4, 5x5, 6x6.
63. Обробка даних як етап здійснення кримінальної розвідки.
64. Аналіз даних як етап здійснення кримінальної розвідки.
65. Дерево зв’язків (link charting).
66. Дерево подій (event charting).
67. Дерево цінностей (commodity flow charting).
68. Дерево дій (activity charting).
69. Фінансове профілювання (financial profiling).

70. Частотний графік (frequency charting).
71. Кореляція даних (data correlation)
72. Мережний аналіз даних.
73. Особливості побудови діаграм за даними про телефонні з’єднання.
74. Розробка аналітичних висновків як етап здійснення кримінальної розвідки.
75. Види аналітичних висновків.
76. Зміст аналітичних висновків. Система запитань 5W+H.
77. Етапи проведення аналізу конкуруючих гіпотез.
78. Поширення інформації як етап здійснення кримінальної розвідки.
79. Повторний аналіз інформації.
80. Джерела відкритої інформації.
81. Пошук інформації про об’єкти в мережі.
82. Збирання інформації про мережі даних.
83. Аналіз профілів соціальних мереж.
84. Методи встановлення IP-адреси.
85. Аналіз заголовків електронних документів.
86. Аналіз метаданих.
87. Систематизація одержаної інформації.
88. Загальні інструменти для аналізу даних.
89. Сенс та завдання картографування злочинних проявів.
90. Інструменти картографічного профілювання.
91. Ключові відстані, які вимірюються під час побудови географічного профілю.
92. Використання MS Excel для вирішення завдань кримінальної розвідки.
93. Використання IBM i2 для вирішення завдань кримінальної розвідки.
94. Використання Palantir для вирішення завдань кримінальної розвідки.
95. Використання Maltego для вирішення завдань кримінальної розвідки.
96. Використання Splunk для вирішення завдань кримінальної розвідки.
97. Використання Datasploit для вирішення завдань кримінальної розвідки.
98. Здійснення картографування з використанням засобів Rigel компанії ECRI.
99. Здійснення картографування з використанням засобів CrimeStat.
100. Здійснення картографування з використанням засобів RICAS.
101. Вітчизняний досвід проведення аналітичної роботи.
102. Поняття оперативної техніки, оперативно-технічних засобів та спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших засобів негласного отримання інформації.
103. Класифікація та ознаки спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших засобів негласного отримання інформації.
104. Нормативно-правова база використання оперативно-технічних засобів.
105. Поняття та принципи застосування оперативної техніки.

106. Класифікація та ознаки запірних пристроїв.
107. Однорядні штифтові циліндричні механізми.
108. Дворядні штифтові циліндричні механізми.
109. Хрестоподібний циліндровий механізм.
110. Циліндровий механізм із конічними фрезеруваннями на ключі.
111. Циліндровий механізм із поворотними штифтами.
112. Ознаки сувальдних запірних пристроїв.
113. Основні частини сувальдного запірного пристрою.
114. Підкласи сувальдних запірних пристроїв.
115. Дискові запірні пристрої.
116. Реєчні запірні пристрої.
117. Електронні запірні пристрої.
118. Кодові запірні пристрої.
119. Напрямлені мікрофони**.**
120. Основні елементи радіозакладки.
121. Електронні стетоскопи.
122. Електромережні закладки.
123. Види сигналізації.
124. Методи нейтралізації сигналізації.
125. Вразливості програмного забезпечення.