Л. Майданевич, О. Войтович, Г. Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Міністерство освіти і науки України
Вінницький національний технічний університет

Л. Майданевич, О. Войтович, Г. Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Електронний навчальний посібник

Вінниця
ВНТУ
2025

УДК [343.982.4: 004.946.5.056] (075.8)
М14

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 8 від 30.01.2025 р.)

Рецензенти:
О. О. Можаєв, доктор технічних наук, професор
О. О. Кирбят'єв, доктор юридичних наук, професор
В. В. Карпінець, кандидат технічних наук, доцент

Майданевич, Л. О.

М14 Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник [Електронний ресурс] / Майданевич Л. О., Войтович О. П., Шелепало Г. В. – Вінниця : ВНТУ, 2025. – (PDF, 109 с.)
ISBN 978-617-8163-60-0 (PDF)

Навчальний посібник відповідає програмі дисципліни «Техніко-криміналістичне забезпечення розслідування кіберзлочинів» для здобувачів, що навчаються на магістерській програмі за спеціальністю 125 «Кібербезпека та захист інформації» освітньої програми «Безпека інформаційних і комунікаційних систем».

Посібник стане в нагоді здобувачам вищої освіти при вивчені дисципліни, підготовці до іспиту та в практичній діяльності за фахом.

Рекомендується для здобувачів вищої освіти, викладачів, науковців та спеціалістів в сфері кібербезпеки.

УДК [343.982.4: 004.946.5.056] (075.8)

ISBN 978-617-8163-60-0 (PDF)

ЗМІСТ

ЗМІСТ 3
ВСТУП 4
РОЗДІЛ 1 КІБЕРПРОСТІР ТА ЗЛОЧИНИ ЯК ОБ'ЄКТ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ 6
1.1 Кіберзлочинність та її місце в загальній структурі злочинності 6
1.2 Основи правового регулювання боротьби з кіберзлочинністю 16
1.3 Використання новітніх технологій у розслідуванні злочинів 29
РОЗДІЛ 2 ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ 43
2.1 Поняття та види техніко-криміналістичних засобів, що застосовуються у ході розслідування кіберзлочинів 43
2.2 Теоретико-множинні моделі категорій кіберінцидентів та найпоширеніших кіберзлочинів 54
2.3 Моделі розслідування кіберзлочинів 68
РОЗДІЛ 3 ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У ПРОЦЕСІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ 84
3.1 Види та можливості судових експертиз у ході розслідування кіберзлочинів 84
3.2 Оцінювання та використання результатів судових експертиз у ході розслідування кіберзлочинів 88
3.3 Експериментальне дослідження кіберзлочинів як основа розробки методики 92
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 103

ВСТУП

Шостий технологічний уклад характеризується стрімким розвитком новітніх технологій, які суттєво впливають на всі аспекти життя, зокрема кібербезпеку та методи розслідування кіберзлочинів. Серед ключових тенденцій слід виділити цифровізацію, роботизацію, прогрес у сфері нано- і біотехнологій, а також впровадження штучного інтелекту. Особливо важливим є розвиток нано- та біотехнологій, які відкривають унікальні можливості, недоступні на попередніх технологічних етапах. Ці досягнення сприяють удосконаленню інформаційно-комунікаційної інфраструктури та суттєво впливають на методи та інструменти криміналістики, що використовуються для розслідування кіберзлочинів.

Зростання складності кіберзлочинів зумовлює потребу вдосконалення криміналістичних методів. Основними напрямами є: цифрова криміналістика, яка забезпечує збирання, аналіз та зберігання цифрових доказів з гарантією їх автентичності; використання машинного навчання для прогнозування кіберзагроз і аналізу поведінкових моделей у кіберпросторі; блокчейн-аналітика, спрямована на дослідження транзакцій у розподілених мережах для виявлення підозрілих операцій; а також розробка нових підходів до захисту даних через шифрування і квантову криптографію, що враховують потенційні ризики використання квантових комп'ютерів для зламу класичних алгоритмів.

Різноманіття апаратних і програмних засобів для обробки інформації в комп'ютерних мережах, їх швидке оновлення та зростання функціональних можливостей, а також використання злочинцями сучасних технологій створюють значні труднощі для працівників правоохоронних органів. Ситуація ускладнюється також недоліками правового, організаційного, тактичного та методичного забезпечення у застосуванні цих технологій у розшуковій та слідчій роботі. Ці тенденції вимагають нових підходів до організації взаємодії кіберполіції та інших поліцейських підрозділів з органами досудового розслідування, особливо під час виконання слідчих доручень. Це також ставить завдання з підготовки фахівців таких підрозділів. Потребує вдосконалення організація та розробка нових методик і тактик для роботи й взаємодії слідчих та оперативних підрозділів, оскільки ефективність їх діяльності значною мірою залежить від оновлення та адаптації методів, які вони використовують.

В посібнику: досліджено апаратні та програмні засоби, що застосовуються для аналізу комп'ютерної техніки та програмного забезпечення; проаналізовано теоретико-множинні моделі кіберінцидентів та ознак кіберзлочинів, передбачених статтями 190, 200, 361–363[1] Кримінального кодексу України; проведено експериментальний аналіз найпоширеніших кіберзлочинів із використанням міждисциплінарного та трансдисциплінарного

підходів, спрямованих на покращення взаємодії між суб'єктами розслідування кіберзлочинів та експертами в галузі інформаційних технологій. Незважаючи на широкі можливості цих інструментів, їх ефективність має обмеження, наприклад: які пов'язані з проблемами визначення формату, методів чи способів створення шкідливого програмного забезпечення та інших факторів.

Цей навчальний посібник спрямований на систематизацію знань і практичних навичок, потрібних для забезпечення ефективного розслідування кіберзлочинів. У ньому розглядаються ключові технікокриміналістичні засоби та методи, що застосовуються для аналізу кіберзагроз, дослідження цифрових слідів, а також організації взаємодії між суб'єктами протидії кіберзлочинності.

Матеріали посібника будуть корисними для здобувачів вищої освіти, викладачів, практикуючих фахівців, а також усіх, хто цікавиться питаннями криміналістики та кібербезпеки. Він покликаний допомогти розвинути навички аналізу цифрових доказів, оцінювання ризиків у кіберпросторі та впровадження інноваційних підходів у протидії злочинності у сфері інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дзьобань О. П. Цифрова людина. *Енциклопедія соціогуманітарної інформології* / коорд. проєкту та заг. ред. проф. К. І. Беляков. Одеса, 2021. Т. 2. С. 177–181.

2. Дудатьєв А. Аксіоматика теорії комплексної безпеки соціотехнічних систем. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 1. С. 22–25.

3. Кримінальний процесуальний кодекс України : *Закон України*, 13.04.2012. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

4. Кримінальний кодекс України : *Закон України*, 05.04.2001. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

5. Конституція України : *Закон України* від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254% D0%BA/96-%D0%B2%D1%80#Text

6. Криміналістична тактика : навч. посіб. / за ред. д-ра юрид. наук, проф. М. А. Погорецького. Київ : Алерта, 2016. 244 с.

7. Ващук О. Структура окремих методик розслідування кримінальних правопорушень. *Юридичний вісник*. 2024. № 3. С. 30–36.

8. Білоус Р., Василинчук В., Таран О. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 1 (118). С. 131–137.

9. Шевчук В. Інноваційні криміналістичні продукти у правозастосовній діяльності: поняття, ознаки та проблеми впровадження у практику. *Наукові праці НУ «Одеська юридична академія»*. 2020. С. 139–155. URL: https://doi.org/10.32837/npnuola.v26i0.671.

10. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів: ЛьвДУВС, 2020. 256 с.

11. Волков О. О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів : дис. ... канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 198 с.

12. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2008. 230 с.

13. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. на здобуття наук. степеня канд. юрид. наук : 12.00.09 / Київ, 2005. 20 с.

14. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого наук.-практ. семінару* (м. Харків, 23 трав. 2019 р.) / редкол.: С. О. Гриненко (голов. ред.) та ін. Харків : Право, 2019. Вип. 10. С. 177–181.

15. C.A.IN.E. (Computer Aided Investigative Environment). URL : https://www.caine-live.net/ (дата звернення: 27.11.2024)

16. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2021. 268 с.

17. Cellebrite UFED Touch 2. EPOS-ForensicTools. URL : https://forensictools.com.ua/viluchennya-danikh-z-mobilnikh-telefoniv/ufed-touch-2.html (дата звернення: 27.11.2024)

18. MSAB XR / MSAB XRY Field. Mobile Forensics and Data Recovery Software. URL : https://www.msab.com/product/xry-extract/ (дата звернення: 27.11.2024)

19. RUSOLUT. Monolithic Adapters. URL : https://rusolut.com/tag/monolithic-adapters/ (дата звернення: 27.11.2024)

20. Magnet AXIOM. Introduction to Magnet AXIOM. URL : https://www.magnetforensics.com/resources/introduction-magnet-axiom/ (дата звернення: 27.11.2024)

21. Magnet Forensics. Belkasoft Evidence Center. URL : https://belkasoft.com/x (дата звернення: 27.11.2024)

22. Tableau T35U. Opentext Tableau Forensic T35u/T35u-RW SATA/IDE BridgeUser Guide. URL : https://manuals.plus/opentext/tableau-forensic-t35ut35u-rw-sataide-bridge-manual.pdf (дата звернення: 27.11.2024)

23. Wiebitech Forensic UltraDock v5. EPOS-ForensicTools. URL : https://forensictools.com.ua/blokatori-zapisu/wiebetech-forensic-ultradock-v55.html (дата звернення: 27.11.2024)

24. Encase Forensics. EPOS-ForensicTools. URL : https://forensictools.com.ua/search?controller=search&orderby=position&orderway=desc&search_query=Encase+Forensics (дата звернення: 27.11.2024)

25. Access Data FTK. URL : https://www.pluralsight.com/paths/accessdata-forensic-toolkit-ftk (дата звернення: 27.11.2024)

26. X-Ways Forensics: Integrated Computer Forensics Software. URL : https://www.x-ways.net/forensics/ (дата звернення: 27.11.2024)

27. ACELab. URL : https://www.acelab.eu.com/ (дата звернення: 27.11.2024)

28. Autopsy. URL : https://www.autopsy.com/download/ (дата звернення: 27.11.2024)

29. Photorec. Digital Picture and File Recovery. URL : https://www.cgsecurity.org/wiki/photoRec (дата звернення: 27.11.2024)

30. Eric Zimmerman Tools. URL : https://www.sans.org/tools/ez-tools/ (дата звернення: 27.11.2024)

31. Про затвердження Положення про організаційно-технічну модель кіберзахисту : *Постанова Кабінету Міністрів України*; Положення від 29.12.2021 року № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF

32. Про основні засади забезпечення кібербезпеки України : *Закон України* від 05.10.2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

33. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту (затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426) / Щиголь Ю., Потій О., Семенченко А., Дубов Д., Бакалинський О. та Мялковський Д. URL: https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426

34. Субач І. Ю, Кубрак В. О. Модель ідентифікації кіберінцидентів SIEM-системою захисту інформаційно-комунікаційних систем. *Кібербезпека: освіта, наука, техніка*. 2023. № 4 (20). С. 81–91.

35. SIEM (Security information and event management). URL: https://uk.wikipedia.org/wiki/SIEM

36. Кулешов М. В. Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України. *Інформація і право*. 2019. № 2 (29). С. 115–122.

37. Перелік категорій кіберінцидентів : схвалений Національним координаційним центром кібербезпеки при РНБО України (протокол № 18 від 28.10.2021 №16/320/21 дск). URL: https://cert.gov.ua/recommendation/16904

37. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем. *Сучасний захист інформації*. 2018. № 2 (34). С. 53–58.

38. Конвенція про кіберзлочинність : від 23.11.2001 р. *Верховна Рада України. Офіційний вісник України* від 10.09.2007. № 65, С. 107. URL: https://zakon.rada.gov.ua/laws/show/994_575/

39. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України. Київ : Істина, 2004. 504 с.

40. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту :. навчальний посібник. Львів : «Новий Світ – 2000», 2024. 678 с.

41. Про Положення про технічний захист інформації в Україні : *Указ Президента України* від 27.09.1999 № 1229/99 (в редакції від 04.05.2008). URL: https://zakon.rada.gov.ua/go/1229/99

42. Про захист інформації в інформаційно-комунікаційних системах : *Закон України* від 05.07.1994 № 80/94-ВР (в редакції від 28.06.2024). URL : https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

43. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : *Указ Президента України* від 22.05.1998 № 505/98 (в редакції від 12.09.2009). URL : https://zakon.rada.gov.ua/go/505/98

44. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / Укладачі: Микитишин А. Г., Митник М. М., Стухляк П. Д. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

45. Кант Іммануїл. Критика чистого розуму / пер. з нім. та приміт. І. Бурковського. Київ : Юніверс, 2000. 504 с

46. ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» // Кіберзлочинність та електронні докази : навч. посібник. Львів : ЛНУ ім. Івана Франка, 2022. С. 212–278.

47. Про судову експертизу : *Закон України* від 25.02.1994 року № 4038-XII (в редакції від 01.01.2024). URL: ttps://zakon.rada.gov.ua/laws/card/4038-12

48. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : *Наказ Мін'юст України* від 08.10.1998. № 53/5. (в редакції від 30.10.2024). URL : https://zakon.rada.gov.ua/laws/show/z0705-98#Text

49. Про затвердження Інструкції про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах : *Наказ Мін'юст України* від 12.12.2011. № 3505/5 (в редакції від 30.10.2024). URL: https://zakon.rada.gov.ua/laws/show/z1431-11#Text

50. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : *Наказ Міністерства внутрішніх справ України* від 03.11.2015 №1343. (в редакції від 25.01.2022). URL:: https://zakon.rada.gov.ua/laws/show/z1390-15#Text

51. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.09. Харків, 2007. 19 с.

52. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. / Климчук М. П. та ін. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.

53. Clark, David. Characterizing cyberspace: past, present and future // MIT,CSAIL. Version1.2. of March12 2010. URL: https://ecir.mit.edu/sites /default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf

54. Про судову експертизу в кримінальних та цивільних справах: *Постанова Пленуму Верховного Суду України* № 8 від 30.05.1997 р. (із змінами) URL: https://zakon.rada.gov.ua/laws/show/v0008700-97#Text

Електронне навчальне видання

Леонід Олександрович Майданевич
Олеся Петрівна Войтович
Галина Василівна Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Навчальний посібник

Рукопис оформив *Л. Майданевич*

Редактор *В. Дружиніна*

Оригінал-макет виготовила *Т. Старічек*

Підписано до видання 19.09.2025 р.
Гарнітура Times New Roman.
Зам. № Р2025-132.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
Email: rvv.vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

МАЙДАНЕВИЧ Леонід Олександрович
кандидат філософських наук, старший викладач кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: філософія інформаційного права, організаційно-правові основи забезпечення кібербезпеки, механізми публічного управління, методологія та організація наукових досліджень

Наукові здобутки: кандидат філософських наук (2015), захистив дисертацію з проблеми проведення релігієзнавчої експертизи. Закінчив магістерські програми: в Інституті міжнародних відносин Київського національного університету імені Тараса Шевченка; в Національній академії державного управління при Президентові України; на філософському факультеті Київського національного університету імені Тараса Шевченка; на факультеті інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету. Є автором більше 40 публікацій в наукових та інших виданнях

Практична діяльність: адвокат (Рада адвокатів Вінницької області)

Перелік дисциплін: Техніко-криміналістичне забезпечення розслідування кіберзлочинів; Захист інтелектуальної власності в кіберпросторі; Нормативно-правове забезпечення інформаційної безпеки; Законодавство з кібербезпеки критичних систем

ВОЙТОВИЧ Олеся Петрівна
кандидат технічних наук, доцент, доцент кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: захист інформації в інформаційно-комунікаційних системах

Наукові здобутки: кандидат технічних наук (2006), захистила дисертацію з питань інформаційно-вимірювальних систем для діагностування на основі нейронечітких алгоритмів. Результатом наукової діяльності є більше 90 наукових праць, серед них: десять у виданнях, що входять до наукометричних баз Scopus і Web of Science, більше 20 статей у фахових виданнях, п'ять монографій, сім навчальних посібників, два патенти на корисну модель, п'ять авторських свідоцтв на комп'ютерну програму

Практична діяльність: доцент кафедри захисту інформації

Перелік дисциплін: Безпека інформаційно-комунікаційних систем; Кібербезпека; Моніторинг та аудит кібербезпеки

ШЕЛЕПАЛО Галина Василівна
кандидат фізико-математичних наук, доцент кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: безпека даних (кодування та шифрування) в інформаційно- комунікаційних системах, математичні механізми захисту інформації, методологія та організація наукових досліджень в кібербезпеці

Наукові здобутки: кандидат фізико-математичних наук (2019), захистила дисертацію з питань класифікації квазігрупових функційних рівнянь і тотожностей мінімальної довжини, які застосовуються у криптографії. Є автором 85 наукових праць, з них п'ять у виданнях, що входять до наукометричних баз Scopus і Web of Science, більше 12 статей у фахових виданнях, два навчальні посібники

Практична діяльність: провідний інспектор відділу інформаційних технологій та програмування в центральному регіоні (м. Вінниця) управління інформаційних технологій та програмування Департаменту кіберполіції Національної поліції України

Перелік дисциплін: Криптографія на основі груп; Криптографія на основі квазігруп; Основи наукових досліджень, аналізу та синтезу інформації; Сучасні інформаційні технології в кібербезпеці