

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Юридичний факультет
Кафедра кримінального процесу і криміналістики

Затверджено

Проректор з науково-педагогічної
роботи та міжнародної співпраці
Львівського національного університету
імені Івана Франка
д.ю.н., проф. Різник С.В.

« ___ » _____ 2024 року

Силабус з навчальної дисципліни

“Електронні докази та цифрова форензика”

| | |
|------------------------------|------------------------|
| освітньо-професійна програма | «Право» |
| рівень вищої освіти | другий (магістерський) |
| код та назва галузі знань | 08 «Право» |
| код та назва спеціальності | 081 «Право» |
| вид дисципліни шифр | вибіркова ВК 9.6 |

| | |
|--|---|
| Назва дисципліни | «Електронні докази та цифрова форензика» |
| Адреса викладання дисципліни | м. Львів, вул. Січових Стрільців |
| Факультет та кафедра, за якою закріплена дисципліна | Юридичний факультет Кафедра кримінального процесу і криміналістики |
| Галузь знань, шифр та назва спеціальності | 081 – «Право» |
| Викладачі дисципліни | Калужна Оксана Михайлівна доцентка кафедри кримінального процесу і криміналістики; Піх Юрій Тарасович асистент кафедри кримінального процесу і криміналістики |
| Контактна інформація викладачів | oksana.kaluzhna@lnu.edu.ua https://law.lnu.edu.ua/employee/kaluzhna-oksana-myhajlivna yuriy.pikh@lnu.edu.ua https://law.lnu.edu.ua/employee/pikh-yuriy-tarasovych Місце знаходження: юридичний факультет, кафедра кримінального процесу і криміналістики, 79000, м. Львів, вул. Січових Стрільців, 14, ауд. Г-509, тел. (032) 239-47-40 |
| Консультації з питань навчання по дисципліні відбуваються | Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри). |
| Сторінка курсу | https://law.lnu.edu.ua/course/digitalforensics |
| Інформація про дисципліну | Дисципліна «Електронні докази та цифрова форензика» є вибірковою дисципліною з спеціальності 081 «Право» для освітньої програми «Право», яка викладається в 4-му семестрі в обсязі 4-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| Коротка анотація дисципліни | <p>Електронні докази та цифрова форензика (англ. <i>digital evidence, digital forensics</i> (форензика)) – це судова наука практичного спрямування, започаткована у 1970-80-х рр., займається збором, аналізом і використанням електронних доказів у цивільних і кримінальних справах (провадженнях), відновленням даних у цифрових пристроях. Історично сформувалася на виклик появи кіберзлочинності та інших зловживань у зв'язку з поширенням на ринку персональних комп'ютерів.</p> <p>Зростання кіберзлочинності, вимагало для її розслідування залучення спеціальних технічних знань. Без належно знайдених, зібраних та оформлених доказів неможливо висунути певній особі обвинувачення та притягнути її до відповідальності.</p> <p>Водночас електронні докази і цифрова форензика важливі не лише для розкриття кіберзлочинів. Їхнє значення є не меншим і в розслідуванні будь-яких, в тому числі традиційних злочинів - вбивств, шахрайств, промислового шпигунства, господарських, службових злочинів, злочинів проти правосуддя, незаконного обігу наркотиків, воєнних злочинів та злочинів проти національної безпеки. Наприклад, досліджуючи підозрюваного за його електронною поштою, можна встановити з ким він</p> |

| | |
|--|---|
| | <p>спілкувався, що шукав, яку інформацію збирав, що купував онлайн, його можливих спільників, місцеперебування на конкретний момент часу.</p> <p>Інструменти цифрової криміналістики дозволяють отримати багато файлів, доступ до яких утруднений, шукати та фільтрувати інформацію.</p> <p>Крім цього, закономірності пошуку та збирання цифрової інформації рівною мірою використовуються й у цивільних, господарських спорах між компаніями та/або фізичними особами (в рамках цивільного, господарського, адміністративного судочинства), коли цифрового спеціаліста залучають до відшукування інформації про особу чи компанію. Цей тип розслідувань йменується спеціальним терміном «eDiscovery».</p> <p>Окрім виявлення прямих доказів злочину, цифрова форензика може встановлювати приналежність (стосунок) доказів до конкретних підозрюваних, підтверджувати алібі, сприяти перевірці версій, визначати умисел, визначити джерело документа (наприклад, у справах про авторські права), автентифікувати документи.</p> |
| <p>Мета та цілі дисципліни</p> | <p>Мета спецкурсу: розвиток навичок у галузі цифрової форензики на основі поєднання теорії і практичних вмій. За допомогою курсу студенти ознайомляться як виявляти, досліджувати й аналізувати цифрову інформацію з метою відтворити хронологію вчинення кібер- чи іншого злочину, делікту (інциденту), освоють як збирати докази в електронній формі, засвідчувати на перевіряти їх достовірність.</p> <p>Після завершення курсу від студентів очікується розуміння використання в судочинстві електронних доказів. Особливістю курсу є поєднання знань ІТ та юридичної основи.</p> <p>Курс навчає критично ставити питання, «мислити як хакер», приймати технологічні рішення з дотриманням нормативно-правових актів.</p> |
| <p>Література для вивчення дисципліни</p> | <ol style="list-style-type: none"> 1. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р., ратифікована Законом № 2824-IV від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.05.2019). 2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651VI (зі змін. і доп.). URL: http://zakon2.rada.gov.ua/laws/show/4651-17 (дата звернення: 20.05.2019). 3. Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV (зі змін. і доп.). URL: http://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 20.05.2019). 4. Алексеева-Працюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. <i>Науковий вісник публічного та приватного права</i>. 2018. № 2. С. 247–253. 5. Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні. <i>Міжнародний науковий журнал «Інтернаука»</i>. 2020. № 10. С. 78–87. 14. 6. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. <i>Науковий вісник Ужгородського національного університету</i>. 2016. Вип. 36 (2). С. 123–125. 7. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. ... канд. юрид. наук. Київ, 2008. 18 с. 8. Васильєв С. В., Ніколенко Л. М. Доказування та докази у господарському процесі України : монографія. Харків : Еспада, 2004. 192 с. 9. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М. В. Гребенюк, В. Д. |

Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін. Київ, 2017. 76 с.

10. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. — Вид. 2-ге, доп. — Київ : Вид-во Нац. акад. внутр. справ, 2020. — 104 с.

[http://elar.naiu.kiev.ua/bitstream/123456789/17605/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D1%85%20\(%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85\)%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D1%96%D0%B2.pdf](http://elar.naiu.kiev.ua/bitstream/123456789/17605/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D1%85%20(%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85)%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D1%96%D0%B2.pdf)

11. Виходець Ю. О. До питання фіксування негласних слідчих (розшукових) дій, проведених з використанням комп'ютерних технологій. *Правова позиція*. 2022. № 2 (35). С. 108-111.

12. Волков О. О. Основні джерела криміналістично-значимої інформації про злочини пов'язані з шкідливими програмними засобами. *Innovative solutions in modern science*, № 3 (22). 2018. 15 с.

13. Гавловський В. Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. 2019. № 1 (28). С. 108–117.

URL: https://mndcentr.com/vydania/pdf_publ/gv_28_19.pdf.

14. Гаркуша А.М. Питання визначення часових міток файлів у файлових системах «FAT» I «NTFS». *Криміналістичний вісник*. 2014. № 1(21). С. 177-181. URL:

<http://elar.naiu.kiev.ua/bitstream/123456789/1923/1/%D0%93%D0%B0%D1%80%D0%BA%D1%83%D1%88%D0%B0%20%D0%90.%20%D0%9C..pdf>

15. Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи* : матеріали круглого столу, м. Львів, 11 червня 2021 р. Львів : Львівський державний університет внутрішніх справ, 2021. С. 159–165.

URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/3865>

16. Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. – С. 72-76. URL:

https://www.researchgate.net/profile/Christian-Bachhiesl/publication/357434068_Christian_Bachhiesl_Forensic_Epistemology_According_to_Hans_Gross_in_Vdovicen_Vitalij_Anatolijovic_ua_Red_Naukovi_citanna_pam'ati_Gansa_Grossa_Zbirnik_tez_miznarodnoi_naukovo-practicnoi_konferencii_m_links/61cde7e1d4500608167ac8b2/Christian-Bachhiesl-Forensic-Epistemology-According-to-Hans-Gross-in-Vdovicen-Vitalij-Anatolijovic-ua-Red-Naukovi-citanna-pamati-Gansa-Grossa-Zbirnik-tez-miznarodnoi-naukovo-practicnoi-konferencii-m.pdf

17. Глинська, Н. В. Цифрові слідчі дії: актуальні аспекти забезпечення правомірності втручання в право особи на приватність. *Актуальні питання кримінального провадження у сучасних умовах*: матеріали міжнародної науково-практичної конференції 31 травня 2023 року. Одеса, 2023. С. 57-65. URL:

<https://dspace.oduvs.edu.ua/server/api/core/bitstreams/9f24586d-25fb-4fe7-8266-de0b510450e8/content#page=58>

18. Гонгало С.В. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку. Автореф. дис. ... к.ю.н. 12.00.09. Київ. 2013. С.13. (20с).

<https://eprints.oa.edu.ua/2301/1/Honhalo.pdf>

19. Гребенькова М. С. Належність і допустимість електронних відображень як джерел доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2021. № 12. С. 335–338.

20. Гребенькова, М. С. Актуальні проблеми електронних відображень у соціальних мережах як джерела доказів у кримінальному провадженні. *Право і суспільство*. №6 (2021): 251-257.

http://pravoisuspilstvo.org.ua/archive/2021/6_2021/36.pdf

21. Гребенькова, М. С. Стан наукових досліджень в сфері електронних відображень у кримінальному провадженні. *Науковий вісник Ужгородського Національного Університету. Серія: Право* 67 (2021): 267-272.

22. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1 (28). С. 118–128.

URL: http://ippi.org.ua/sites/default/files/15_9.pdf

23. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерел доказів у кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1. С. 37–49.

24. Давидюк П. П., Кубай І. Ю. Висунення і перевірка слідчих версій про цифрове алібі підозрюваного (обвинуваченого). *Молодий вчений*. 2017. № 5 (45). С. 29–32.

25. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник*. 2021. №6. С.273-278.

26. Доказування у кримінальному провадженні : кол. авт. Київ : Національна академія прокуратури України, 2017. 346 с.

27. Домашенко О. М. Проблемні питання використання цифрових доказів у криміналістиці. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матеріали міжнар. «круглого столу»* (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Харків : Право, 2019. С. 52–55.

28. Електронні докази. Обшук / [О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін.]. Харків : Фактор, 2020. Ч. 1. 80 с.

29. Зелена М. С. Дослідження комп'ютерної техніки та програмних продуктів у розслідуванні злочинів, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин або їх аналогів. *Теорія та практика судової експертизи і криміналістики*. 2020. Вип. 22. С. 373–381. doi: 10.32353/khrife.2.2020.30.

30. Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. 2021. № 8. С. 336-340. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

31. Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали V Міжнар. наук.-практ. конф., 2021.

<https://archer.chnu.edu.ua/jspui/bitstream/123456789/2242/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%28pdf.io%29.pdf>

32. Капліна О. В. Зняття показань технічних приладів та технічних засобів: правова сутність та процесуальний порядок. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 2. – С. 357-360.*
33. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с.
34. Книш М. Як розвалюють комп'ютерно-технічні експертизи? *Юридична газета online*. 2019. № 45–46. С. 699–700.
35. Кобець М. В. Дії слідчого під час виявлення на місці події мобільних терміналів (стільникових радіотелефонів). *Криміналістичний вісник*. 2023. № 1(39). С.52-63.
36. Коваленко А.В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2018. № 4. С. 237–245.
37. Коваленко І. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право*. 2020. Вип. 12. С. 262–266. doi: 10.32849/2663-5313/2020.12.45.
38. Когут Ю. І. Протидія кібертероризму як загрози інформаційній безпеці України : дис. ... канд. юрид. наук : 12.00.09. Київ, 2021. 258 с.
39. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.
40. Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації : збірник наукових праць*. Запоріжжя, 1998. № 2. С. 70–79. 15.
41. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с.
42. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–305.
43. Крицька І. О. Речові докази у кримінальному провадженні : дис. ... канд. юрид. наук : 12.00.09. Харків, 2017. 249 с.
44. Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3–2. С. 313–315.
45. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12–22.
46. Кравчук, О. «Обшук» мобільних телефонів і комп'ютерів та інші зміни до КПК. *Судебно-юридическая газета*. 25 (2022).
47. Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження.

Науковий вісник Ужгородського національного університету. 2020. № 60. С. 177–181.

48. Метелев О.П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238.

49. Михайлов П. С., Климчук М. П. Судова комп'ютерно-технічна експертиза як спосіб виявлення корупційного складника під час розслідування протиправного впливу на результати офіційних спортивних змагань. Вчені записки Таврійського національного університету імені В. І. Вернадського. 2020. Т. 31 (70). Ч. 3. № 2. С. 109–113. (Серія «Юридичні науки»). doi: 10.32838/2707-0581/2020.2-3/18.

50. Нізовцев Ю. Ю., Омельян О. С. Щодо підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов'язаних із кібератаками. *Криміналістичний вісник*. 2021. № 2 (36). С. 59–68. doi: 10.37025/1992-4437/2021-36-2-59.

51. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12–24.

52. Павлюк Н. В. Інтеграція інноваційних технологій у діяльність із розслідування злочинів – провідний напрям підвищення її ефективності. *Теорія і практика правознавства*. 2021. Вип.2 (20). URL: <http://tlaw.nlu.edu.ua/article/view/242807/248261>

53. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право*. 2020. № 6. С. 243–247. 11.

54. Прокопенко С. Практика та особливості проведення комп'ютерно-технічних експертиз. *Матеріали IV Всеукраїнської конференції з кримінального права та процесу*. Київ, 2017. URL: https://www.slideshare.net/cyberlab_ua/ss-81935770

55. Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні. Дис. ... на здобуття наук. Ступеня доктора філософії. Львів. 2021. 248 с. https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf

56. Ресурси з форензики (практика розслідування кіберзлочинів) URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344671.php

57. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса : 2020. 112 с. <http://dspace.onua.edu.ua/bitstream/handle/11300/12612/%D0%9D%D0%9C%D0%9F%20%D0%A1%D0%BF%D0%B5%D1%86%D0%BA%D1%83%D1%80%D1%81%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8.pdf?sequence=1&isAllowed=y>

58. Сіренко О.В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. № 14. С. 208–214.

59. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. ... д-ра філос. наук : 12.00.09. Харків, 2021. 369 с.

60. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / А. В. Скрипник ; Нац. юрид. ун-т ім. Ярослава Мудрого. – Харків : Право,

2022. – 408 с. https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=4651&download_id=1537

61. Столітній А. В., Каланча І.Г.. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. № 146. С. 179-191.

<http://plaw.nlu.edu.ua/article/view/171218/179266>

62. Тактика слідчого огляду комп'ютерних систем та їх елементів : наук.-практ. посіб. / В. О. Одерій, С. О. Корона, С. В. Самойлов. Донецьк, 2010. 87 с.

63. Татаренко Г.В., Болгарєва К.В., Татаренко Д.В. Електронні документи як засіб доказування: сутність та правове регулювання. *Актуальні проблеми права: теорія і практика*. 2019. № 1. С. 111–119.

64. Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 3 (120). С. 28–34. doi: 10.33270/01211203.28.

65. Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2 (18). С. 24–32 doi: 10.33270/04191802.24.

66. Хахановський В.Г., Гребенькова М.С. Identification, collection, and investigation of electronic imagery as sources of evidence. Виявлення, збирання та дослідження електронних відображень як джерел доказів. *Юридичний часопис Національної академії внутрішніх справ*. Том 12. № 4. 2022.

http://elar.naiu.kiev.ua/bitstream/123456789/23343/1/%d0%ae%d1%80%0%b8%d0%b4.%20%d1%87%d0%b0%d1%81%d0%be%d0%bf%d0%b8%d1%81%20%d0%a2.12%20%e2%84%964%202022_p28-39.pdf

67. Хахановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2019. № 1. С. 13–19.

68. Чванкін С. А. Комп'ютерно-технічна експертиза у цивільному судочинстві. *Право та державне управління*. 2021. № 1. С. 45–51. doi: <https://doi.org/10.32840/pdu.2021.1.7>.

69. Школьніков В.І. Правова основа отримання інформації з мережі інтернет у кримінальному провадженні. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. № 4. С. 172–176.

70. Щербаковський М. Г., Коршенко В. А. Комплексні телекомунікаційно-автотехнічні експертизи. *Вісник Харківського національного університету внутрішніх справ*. 2019. Вип. 4 (87). С. 179–186. doi: 10.32631/v.2019.4.18.

71. Що таке комп'ютерна криміналістика (форензика)? *GROSS digital forensics Lab*. 2017. URL: <https://g-ross.com.ua/novyny/kompyuterna-kryminalistyka-forenzika.html>

72. Що таке цифрова криміналістика? *GROSS digital forensics Lab*. 2018. URL: <https://g-ross.com.ua/novyny/cyfrova-kryminalistyka-2.html>

73. Alkaabi, A. (2020). A strategic Vision to Reduce Cyber-crime and Enhance Cyber security. *International Journal of Advanced Science and Technology*, 29(7), 14268-14274. Retrieved from <http://sersc.org/journals/index.php/IJAST/article/view/30648>

74. Ambika, T., & Senthilvel, K. (2021). Cyber Crimes against the State: A Study on Cyber Terrorism in India. *Webology*, 17(2). 65-72. [10.14704/WEB/V17I2/WEB17016](https://doi.org/10.14704/WEB/V17I2/WEB17016)
75. Anderson, P., Sampson, D., & Gilroy, S. (2021). *Digital investigations: relevance and confidence in disclosure*. ERA Forum, 22 (4). 587-599. ISSN 1612-3093.
76. Android research and analysis tool Andr Ex R. AOS company. URL: https://www.fss.jp/android_andrex_r/
77. AOS Image Analysis Forensics Professional. AOS company. URL: https://www.fss.jp/fss_movie01-2/
78. Årnes, A. (2018). *Digital forensics*. Hoboken, NJ: John Wiley & Sons Inc.
79. Bodo Meseke, Digitale Forensik. Praxiswissen Cybercrime für Manager. Berlin. 2019. https://www.weltbild.de/artikel/ebook/digitale-forensik_34575890-1?ln=UHIvZHVrdHxNZWhyIELDvGNoZXIgzZGVzIEF1dG9ycw==
80. Britz, M. (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson.
81. Caianiello, M. (2019). Criminal Process faced with the Challenges of Scientific and Technological Development, *European Journal of Crime, Criminal Law and Criminal Justice*, 27(4), 267-291. <https://doi.org/10.1163/15718174-02704001>
82. Carlton, A. (2020). Sextortion: the hybrid cyber-sex crime. *North Carolina Journal of Law & Technology*, 21(3), 177-216.
83. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Cham: Springer International Publishing.
84. Chen, L., Takabi, H., & Le-Khac, N.-A. (2019). *Security, privacy and digital forensics in the cloud*. Hoboken, NJ: John Wiley & Sons.
85. *Credit pages of MOOC on digital forensics*. CEMCA. (n.d.). Retrieved July 8, 2022, from <https://www.cemca.org/resources/credit-pages-mooc-digital-forensics#.YsiRr3ZBztU>
86. Dalrymple, B. E., & Smith, E. J. (2018). *Forensic Digital Image Processing: Optimization of Impression Evidence*. Boca Raton, FL: CRC Press.
87. DeceptionGrid – A Powerful Defense for Advanced Threats. *TrapX Security*. 2019. URL: <https://trapx.com/wp-content/uploads/2019/05/PB-DeceptionGridv6.3-1-1.pdf>
88. Digitale Forensik/IT Forensik – berufsbegleitender Online-Fernstudiengang. URL: <http://www.master-digitale-forensik.de/>
89. EC-Council Press. (2010). *Computer forensics*. Clifton Park, NY: Course Technology.
90. Freeman, L. (2018). Digital evidence and war crimes prosecutions: the impact of digital technologies on international criminal investigations and trials. *Fordham International Law Journal*, 41(2), 283-336.
91. Harkin, D., & Whelan, C. (2022). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, 24(1), 66–76. <https://doi.org/10.1177/14613557211036565>
92. Hassan, N. A. (2019). *Digital forensics basics: A practical guide using Windows OS*. New York: Apress.
93. Hayes, D. R., & Walczak, T. (2021). *Informatyka w kryminalistyce: Praktyczny przewodnik*. Gliwice: Helion.

94. Ho, A. T. S., & Li, S. (2015). *Handbook of digital forensics of multimedia data and devices*. Chichester: Wiley.
95. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. London: Routledge, Taylor & Francis Group.
96. Horan C., & Saiedian. H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*, 1 (4). 580-596. <https://doi.org/10.3390/jcp1040029>
97. Kasprzak, W. A. (2015). *Ślady cyfrowe: Studium prawnokryminalistyczne*. Warszawa: Difin.
98. Kävrestad, J. (2017). *Guide to Digital Forensics: A Concise and Practical Introduction*. Cham: Springer International Publishing.
99. Kävrestad, J. (2018). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. Cham: Springer International Publishing.
100. Kleiman, D. (2007). *The official CHFI study guide (Exam 312-49): For computer hacking forensic investigator*. Syngress.
101. Kotsiuba, I., Skarga-Bandurova, I., Giannakoulis A., & Bulda O. (2019). Basic Forensic Procedures for Cyber Crime Investigation in Smart Grid Networks. *2019 IEEE International Conference on Big Data (Big Data)*, 4255-4264. [10.1109/BigData47090.2019.9006215](https://doi.org/10.1109/BigData47090.2019.9006215)
102. Labudde, D., & Spranger, M. (2017). *Forensik in der digitalen Welt*. Berlin, Heidelberg: Springer Berlin Heidelberg.
103. Latysh, K. K. (2021). Criminalistics Analysis of Cyber Tools for Committing Crimes. *Problems of Legality*, 153, 165-172.
104. Lavorgna, A. Cyber-organised crime. A case of moral panic?. *Trends Organ Crim* 22, 357–374 (2019). <https://doi.org/10.1007/s12117-018-9342-y>
105. Leroux, O. (2004). Legal admissibility of electronic evidence, *International Review of Law, Computers & Technology*, 18:2, 193-220. [10.1080/1360086042000223508](https://doi.org/10.1080/1360086042000223508)
106. Lewulis, P. (2021). *Dowody cyfrowe: Teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.
107. Lin, X. (2018). *Introductory Computer Forensics: A Hands-on Practical Approach*. Cham: Springer International Publishing.
108. Luttgens, J., Mandia, K., & Pepe, M. (2014). *Incident Response & Computer Forensics, Third Edition*. McGraw-Hill.
109. Maras, M.-H. (2015). *Computer forensics: Cybercriminals, laws, and evidence*. Burlington, MA: Jones & Bartlett Learning.
110. Maskun, M., Achmad, A., Naswar, N., Assidiq, H., Syafira, A., Napang, M. & Hendrapati, M. (2020). Qualifying Cyber Crime as a Crime of Aggression in International Law. *Cybercrime under International Law*, 13 (2).
111. Pandelica, I. (2020). The phenomenon of cyber crime. *International Journal of Information Security and Cybercrime*, 9(1), 29-36.
112. Patil, R. Y., & Devane, S. R. (2022). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. *Journal of King Saud University – Computer and Information Sciences*, 34, 5. 2031-2044. ISSN 1319-1578. <https://doi.org/10.1016/j.jksuci.2019.11.016>.
113. Paweł Olbe. Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur

- obliczeniowych. Wydawnictwo: Wyższa Szkoła Policji w Szczytnie. 2021. 412 S.
114. Philipp, A., Cowen, D., Davis, C. M., & Scharringhausen, L. S. (2010). *Hacking exposed computer forensics*. New York: McGraw-Hill.
 115. Phillips, A., Nelson, B., & Steuart, C. (2019). *Guide to computer forensics and investigations: Processing digital evidence*. Boston: Cengage Learning.
 116. Piotr Lewulis, Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym Wydawnictwa Uniwersytetu Warszawskiego. 2021. 298 S.
URL: <https://www.taniaksiazka.pl/dowody-cyfrowe-teoria-i-praktyka-kryminalistyczna-w-polskim-postepowaniu-karnym-piotr-lewulis-p-1515673.html>
 117. Popular Computer Forensics Top 21 Tools [Updated for 2019]. *Infosec*. 2019. URL: <https://resources.infosecinstitute.com/computer-forensics-tools/#gref>
 118. Prasad, Ajay & Pandey, Jeetendra. (2016). *Digital Forensics*. Utrakhand Open University.
 119. Quan, W. (2019). Cyber economic crimes: challenges and countermeasures of the Chinese police. *China Legal Science*, 7(3), 67-94.
 120. Reddy, E. (2020). Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill. *Statute Law Review*, 41, 2. 226-239. <https://doi.org/10.1093/slr/hmz001>
 121. Rizqa, Z. F. (2019, November 14). *Computer Hacking Forensic Investigator (CHFI)*. Academia.edu. Retrieved July 8, 2022, from https://www.academia.edu/40932694/Computer_Hacking_Forensic_Investigator_CHFI
 122. Sachowski, J. (2016). *Implementing Digital Forensic Readiness : From Reactive to Proactive Process*. Elsevier Science.
 123. Sachowski, J. (2018). *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*. London: Taylor and Francis.
 124. Sammons, J. (2012). *The basics of digital forensics: The primer for getting started in digital forensics*. Syngress.
 125. Sammons, J. (2016). *Digital forensics: Threatscape and best practices*. Amsterdam: Syngress.
 126. Shavers, B. (2013). *Placing the suspect behind the keyboard: Using digital forensics and investigative techniques to identify cybercrime suspects*. Waltham, MA: Syngress.
 127. Sunde, N. (2022). *Unpacking the evidence elasticity of digital traces*, *Cogent. Social Sciences*, 8:1, 2103946, DOI: 10.1080/23311886.2022.2103946
 128. TrapX Security DeceptionGrid 6.3. *SC Media magazine*. 14 August 2019. URL: <https://www.scmagazine.com/review/trapx-security-deceptiongrid-6-3/>
 129. Van Dine, A. (2020). When is cyber defense crime: evaluating active cyber defense measures under the Budapest convention. *Chicago Journal of International Law*, 20(2), 530-564.
 130. Volonino, L., & Anzaldua, R. (2008). *Computer forensics for dummies*. Hoboken, NJ: Wiley.
 131. Widup, S. (2014). *Computer forensics and digital investigation with Encase Forensic v7*. New York : McGraw-Hill Education.

| | |
|--------------------------------------|--|
| | <p>132. Zarpala, L., & Casino, F. (2021). A blockchain-based forensic model for financial crime investigation: the embezzlement scenario. <i>Digit Finance</i> 3, 301–332. https://doi.org/10.1007/s42521-021-00035-5</p> <p>Ресурси: www.master-digitale-forensik.de codeby.net https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344671.php Верховний Суд https://supreme.court.gov.ua/supreme/gromadyanam/kontakts/ Офіс Генерального прокурора України - https://www.gp.gov.ua/ СБУ - https://ssu.gov.ua/ НАБУ - https://nabu.gov.ua/ ДБР - https://dbr.gov.ua/ БЕБ - https://esbu.gov.ua/ Кіберполіція НП - https://cyberpolice.gov.ua/ Кіберцентр UA30 - https://cert.gov.ua/</p> |
| Обсяг курсу | Загальний обсяг: 120 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 72 год. |
| Очікувані результати навчання | <p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p>знати:</p> <ul style="list-style-type: none"> • в чому полягає робота з джерелами цифрової інформації; • характеристику злочинності, що вчиняється в мережі Інтернет та програми (методи, алгоритми) їх розслідування; • аналіз телекомунікаційних засобів та мобільних додатків; аналіз і документування вмісту носіїв даних; перевірку та документування інформації, що міститься в мобільних телефонах, інших пристроях доступу до Інтернет та SIM-картках; • як встановлювати та правильно документально оформляти електронні докази, в тому числі - факт використання та володіння комп'ютерними програмами, іграми, мультимедійним контентом, <p>вміти:</p> <ul style="list-style-type: none"> • виявляти, та процесуально документувати електронні докази; • підтверджувати (доводити) достовірність, належність та допустимість електронних доказів у суді; • аналізувати вміст комп'ютерів, ІТ-систем з метою пошуку і виявлення конкретних даних та інформації, що міститься в них, здійснювати пошук інформації у файлах, видалених з диска, або після його повного форматування, обмін файлами, захищеними паролем. <p>Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 4, КЗ 5, КФ 1, КФ 3, КФ 4, КФ 6, КФ 7, КФ 8, КФ 9, КФ 10; та програмних результатів навчання: ПРН 3, ПРН 4, ПРН 5, ПРН 9, ПРН 10, ПРН 12, ПРН 14, ПРН 32, ПРН 34, ПРН 50, ПРН 54.</p> |
| Ключові слова | Цифрові докази, електронні докази, електронні документи, компютерні дані, допустимість електронних доказів, достовірність електронних доказів, кіберзлочин, кібеззлочинність, компютерна криміналістика, цифрова криміналістика, ІТ-детектив, збирання електронних доказів, судова компютерно-технічна експертиза, судова телекомунікаційна експертиза, «eDiscovery», OSINT. |
| Формат курсу | Очний Проведення лекцій, лабораторних робіт і консультацій. |

| Теми | Тема 1: Поняття, предмет, система завдання цифрової форензики Поняття та значення цифрової форензики. Система цифрової форензики. Історія цифрової форензики. Перші дослідницькі центри, слідчі органи, міжнародні слідчі органи із застосуванням цифрової форензики в США, Європі, Україні. Навички, підготовка та освіта, необхідна для роботи з цифровою доказовою інформацією. | Год |
|------|--|-----|
| | <p>Тема 2. Цифрові сліди та електронні докази Поняття цифрової інформації та слідів її створення, зміни, транспортування, зміни, відновлення. Поняття електронних доказів, їх властивості, види, класифікація. Вимоги до оформлення цифрових джерел інформації для набуття ними статусу судового електронного доказу.</p> <p>Тема 3: Способи збирання електронних доказів. Гласні слідчі (розишуківі) дії. Огляд, обшук Залучення ІТ-спеціалістів до проведення оглядів, обшуків, НСРД для їх технічного супроводу. Пошук необхідних цифрових даних, в тому числі прихованих і видалених, та оформлення їх за правилами судових доказів. Форензика мобільних пристроїв. Дослідження мобільних пристроїв з метою встановлення даних про дзвінки та повідомлення (SMS, Email), відновлення видалених даних, а також з метою встановлення інформації про місцезнаходження. Огляд, вилучення і аналіз усіх даних (переписки, медіа, документів та ін.) із сучасних мобільних пристроїв. Відновлення видалених даних; вилучення інформації з хмарних сховищ і онлайн сервісів. Тимчасовий доступ до речей і документів та їх витребування. Негласні слідчі (розишуківі) дії. Мережева форензика. Аналіз і відстеження мережевого трафіку, локального і глобального Інтернету, збір доказів і виявлення вторгнень у систему. Програмне забезпечення для аналізу великих обсягів даних (перехопленого трафіку, сегмента мережі Інтернет). Встановлення (ідентифікація) кінцевих користувачів мережевого обладнання. Відео-криміналістика. Відеофіксація гласних і негласних слідчих дій. Поліпшення якості відео, збільшення окремих ділянок зображення; визначення розмірів і швидкості руху об'єктів. Швидкий автоматизований аналіз великих обсягів відео з різних джерел з виділенням подій. Дослідження (демонстрація) відео- та інших цифрових доказів у суді. OSINT. Аналіз відкритих банків даних, реєстрів, реєстрів з обмеженим доступом для моніторингу (діагностування) та виявлення можливого вчинення злочинів та збирання доказової інформації (Youcontrol, ProZorro, Реєстри Міністерства юстиції, МВС, НАЗК, та інших, відозаписів з автошляхів та публічно-доступних місць).</p> | |

Цифрові методи оперативної (попередньої) та експертної ідентифікації осіб: програмні додатки до смартфонів для швидкої автоматичної попередньої дактилоскопічної перевірки поліцією відбитків пальців на місці події (Великобританія), технології розпізнавання обличчя, технології розпізнавання та встановлення місцевості, будівель, споруд, техніки (в тому числі військової) за метаданим.

Тема 4: Судова комп'ютерно-технічна та телекомунікаційна експертиза

Комп'ютерно-технічна експертиза у кримінальних провадженнях та під час вирішення **господарських і цивільних спорів**.

Предмет (коло вирішуваних питань) та об'єкти комп'ютерно-технічної експертизи. Встановлення схеми і хронології втручання, вилучення даних про способи атак,

Правила підготовки об'єктів та інших необхідних матеріалів, а також постановки запитань на комп'ютерно-технічні експертизи.

Можливості різновидів судово-комп'ютерної експертизи

Аналіз і оцінка експертних висновків на прийнятність використовуваних при дослідженні методик і процедур та достовірність отриманих результатів, відповідність сучасним науковим підходам і вимогам законодавства.

Тема 5. Розслідування кіберзлочинів та інших кримінальних правопорушень, вчинюваних з використанням цифрових технологій

Поняття та кримінологічна, кримінально-правова та криміналістична характеристика кіберзлочинності. Види кіберзлочинів.

Дата-злочини (злочини з банками даних). Розслідування втручання у бази даних та у системи ЕОМ. Аналіз банківських троянських програм і виявлення керуючих серверів. Виявлення і фіксація дій інсайдерів. Розслідування підробки електронних документів (податкових декларацій, декларацій НАЗК, Державного земельного кадастру, реєстрів Міністерства юстиції та МВС, ковід-сертифікатів, прав водія тощо у додатку «Дія»). Виявлення ботоферм та злочини, що вчинюються за їх посередництва.

Фінансові злочини. Розслідування крадіжок через системи дистанційного банківського обслуговування (клієнт-банк, інтернет-банк). Визначення способу крадіжки. Інтернет-шахрайства. Використання додатків, які незаконно стягують кошти. Криптоджекінг (незаконний майнінг).

Кардшейрінг та інші види інтернет-піратства. Розслідування інших порушень у сфері інтелектуальної власності.

Розслідування злочинів проти основ національної безпеки, проти громадської безпеки, виборчих злочинів, що вчиняються в мережі.

Незаконне втручання в приватне спілкування.

| | | |
|--|--|--|
| | <p>Розслідування розповсюдження в мережі інтернет порнографії.</p> <p>Розслідування кібернасильства та злочинів сексуального характеру.</p> <p>Розслідування незаконного обігу наркотиків, зброї (Dark-web).</p> <p>Розслідування службових злочинів та злочинів проти правосуддя.</p> <p>Розслідування воєнних злочинів та злочинів проти миру і людяності.</p> | |
| <p>Підсумковий контроль, форма</p> | <p>Залік у кінці семестру</p> | |
| <p>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</p> | <p>Серед методів навчання, зокрема, застосовуються: розповідь, пояснення, бесіда, лекція, демонстрація (презентація), спостереження, практичне заняття, індивідуальні завдання, дослідні проекти, модульний контроль</p> <p>Під час практичних занять забезпечується постановка питань на тлі змодельованих кейсів, пов'язаних з використанням спеціальних знань, їх обговорення з метою пошуку оптимальних шляхів вирішення практичної ситуації. На практичних заняттях викладач виконує роль модератора дискусії, визначає її напрями, забезпечує необхідну динаміку та загострює увагу на проблемних аспектах. Після завершення обговорення проблеми викладач підсумовує найважливіші моменти, аналізує сильні та слабкі сторони висловлених аргументів.</p> <p>Індивідуальні завдання студенти вирішують письмово, надсилаючи їх викладачеві на електронну пошту. Індивідуальні завдання мають пошуково-аналітичний характер – полягають у науковому, законодавчому обґрунтуванні неоднозначних ситуацій у судовій практиці щодо цифрових доказів, проведення судової комп'ютерно-технічної експертизи. Вирішення індивідуальних запитань потребує не механістичного пошуку у літературі, компіляції з різних джерел, а завжди власного аналізу й вміння обґрунтувати свою позицію. Іноді на поставлені індивідуальні завдання немає строго єдино правильної відповіді, а відповідь буде варіативною залежно від додаткових деталей складових (змінних) кейсу (ситуації). Оцінюється ж глибина і всебічність мислення, аналізу, горизонт і масштаб бачення студентом проблеми.</p> | |
| <p>Необхідне обладнання</p> | <p>Бакалаври використовують технічні засоби та програмне забезпечення під час підготовки до практичних занять з метою пошуку необхідної спеціальної літератури, нормативно-правових актів, судової практики, а також під час виконання індивідуальних завдань</p> | |
| <p>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</p> | <p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> • практичні заняття, індивідуальні завдання: 50% семестрової оцінки; • модуль: 50% семестрової оцінки. Максимальна кількість балів – 50 балів. <p>Підсумкова максимальна кількість балів – 100 балів.</p> <p>Оцінювання поточної успішності: <i>Поточна успішність</i> (оцінюється за 50-бальною шкалою): Відмінно (50) Добре (40; 45)</p> | |

Задовільно (26; 31)

Незадовільно (0)

Критерії оцінювання при проведенні іспиту:

90-100 балів (відмінно)

81-89 балів (добре)

71-80 балів (добре)

61-70 балів (достатньо)

51-60 балів (задовільно)

0-51 балів (незадовільно)

50 балів - виставляється студенту, який дав повну і правильну відповідь на всі питання, що базуються на знанні нормативно-правових актів, судової, слідчої практики та спеціальної літератури; проявив уміння застосувати набуті знання до конкретних ситуацій та здібності аналізу джерел.

45 балів - достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи у цьому нормативну та обов'язкову літературу. Але під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускає окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість завдань. Студент здатен виокремлювати суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно - наслідкові зв'язки, у яких можуть бути окремі несуттєві помилки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями.

40 балів - за повну і правильну відповідь, але не на всі питання, або відповідь не базується на всіх складових джерелах вивчення. Тобто знав основне як для відповідної ситуації літературу, нормативно-правовий акт та слідчу, судову практику але не знав інформації, що міститься у спеціальній літературі, чи інформації, яка міститься у інших деталізованих джерелах. Однак у підсумку його відповідь повинна базуватись не менше ніж на двох базових джерелах.

31 бал - виставляється студенту, який не дав вичерпної детальної відповіді на питання контрольних завдань і яка базується тільки на одному із рекомендованих джерел вивчення матеріалу.

26 балів – в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних виступів та письмових вирішень, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи у цьому розрізі окремі суттєві неточності та помилки. Правильно вирішив половину письмових (в тому числі /тестових) завдань. Студент має труднощі з виокремлення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв'язків і формулювання висновків.

0 балів - не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та вирішення домашніх завдань, недостатньо розкриває зміст теоретичних питань та практичних моделювань, допускаючи тут суттєві неточності. Безсистемне розмежування випадкових ознак вивченого; невміння робити найпростіші операції аналізу і синтезу; робити узагальнення, висновки.

Академічна доброчесність: Очікується, що кожен студент повинен самостійно готуватися до практичних занять та вирішувати індивідуальні завдання, обдумувати та викладати власну аргументацію своєї правової позиції. Дві чи більше однакові роботи студентів не перевіряються з

| | |
|---------------------------|---|
| | <p>виставлення кожному зі студентів 0 балів. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману; у разі незарахування роботи студент в узгоджені з викладачем строки повинен повторно виконати письмову роботу та подати її викладачу для оцінювання.</p> <p>Відвідування занять є добровільним для лекційної форми і обов'язковим для лабораторних.</p> <p>Викладач фіксує неявку студента на практичне заняття, що вважається академічною заборгованістю, яку студент повинен відпрацювати до дня виставлення заліку(іспиту). Відпрацювання полягає у перевірці підготовки студентом тих самих завдань, які виносилися на практичне заняття, на якому студент був відсутній.</p> <p>Література. Уся література у вільному доступі в мережі Інтернет із наданням студентам лінків, на її розміщення. Лекції та презентації надаються студентам викладачем виключно в освітніх межах без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p>Політика виставлення балів. Враховуються бали набрані на практичних заняттях та за виконання індивідуальних завдань, бали одержані за модуль. Враховуються активність студента під час лабораторного заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття з метою не пов'язаною з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Критеріями оцінювання роботи студента на лабораторних заняттях є аргументованість наукової, правової позиції та її відповідність чинному законодавству; уміння лаконічно, переконливо та логічно висловити свою думку; здатність до аргументованого аналізу наукових і правових позицій у літературі, думок, висловлених іншими студентами; уміння підсумувати усі висловлені щодо певної проблеми аргументи і віднайти їхні сильні та слабкі сторони.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p> |
| <p>Питання на модуль.</p> | <ul style="list-style-type: none"> ✓ Поняття цифрової форензики, її соціальна мета і значення. ✓ Які вам відомі закономірності (способи) становлення самостійних наук на сьогодишньому цивілізаційному етапі? Приведіть приклади появи самостійних наук у спосіб виділення та у спосіб синтезу. ✓ Як і коли відбувалося становлення цифрової форензики. ✓ Якими іншими термінами-синонімами позначається ця наука та практична сфера діяльності? Якими альтернативними термінами-синонімами йменується фах ІТ-криміналіста? ✓ Що (які об'єкти та процеси) є предметом вивчення (дослідження) цифрової форензики? ✓ Яким є місце цифрової форензики в системі наук? ✓ Які пристрої можуть входити до системи «розумний дім»? Як вона організована? Які функції може виконувати? ✓ Які загрози можуть походити від Інтернет-речей (Internet of Things)? ✓ Чому криптовалюти є зручними для платежів між злочинцями? ✓ Яка специфіка темних веб-магазинів (dark web)? |

- ✓ Якою є система цифрової форензики? Охарактеризуйте її підгалузі.
- ✓ Чим займається напрям цифрової форензики «eDiscovery»?
- ✓ Для яких потреб (справ) цивільного життя найчастіше залучається інструментарій (можливості) цифрової форензики?
- ✓ Яка роль і можливості цифрової форензики при розслідуванні злочинів, які не є кібернетичними?
- ✓ Як називається пристрій банкоматів для зчитування інформації, записаної на магнітній смузі кредитних або дебетових карток?
- ✓ Як називається короткочасна енергонезалежна пам'ять, вміст якої зникає при вимкненні комп'ютера? У яких ситуаціях її слід враховувати?
- ✓ Які можливості цифрової форензики для дослідження фото- і відеозображень з відкритих джерел (з мережі Інтернет) для доказування воєнних злочинів рф в Україні?
- ✓ Якою є історія походження терміну «комп'ютерні докази» та його трансформація?
- ✓ Сучасне поняття та властивості електронних доказів?
- ✓ Оформлення (у процесуальних документах) електронних доказів та можливості їх дослідження.
- ✓ Що таке «доказовий ланцюжок» роботи з електронним доказом?
- ✓ Чи мають комп'ютерні докази ефект новинки? В чому суть доктрини «доказу-новинки» (novel evidence)? Звідки вона походить?
- ✓ Яке співвідношення між поняттями «комп'ютерні докази», «цифрові докази», «електронні докази», «комп'ютерні дані»?
- ✓ Розкрийте основні властивості електронних доказів. Чи автентичним є використання в доказуванні копій (дублікатів) комп'ютерних доказів і оригіналів? Чому?
- ✓ Яким є співвідношення між поняттями «електронні докази» та «електронні документи»? Що становлять собою електронні документи (зовнішня і внутрішня структура, вимоги, спосіб оформлення та засвідчення)?
- ✓ Якими є можливості е-доказів для вирішення кримінальних справ?
- ✓ Розкрийте суть такого напрямку використання е-доказів як для доказування наміру (мотиву).
- ✓ Розкрийте суть такого напрямку використання е-доказів як для доказування алібі (digital alibi).
- ✓ Охарактеризуйте основні способи дослідження е-доказів у суді.
- ✓ До якого класу судової експертизи належать комп'ютерно-технічна та телекомунікаційна судові експертизи? Якими нормативними актами визначені назви та шифри (цифрові позначення) експертних спеціальностей даних родів судової експертизи?
- ✓ Назвіть види комп'ютерно-технічної експертизи.
- ✓ Які питання може вирішувати програмно-комп'ютерна експертиза? У яких категоріях справ типово виникає потреба у її проведенні?
- ✓ Які питання може вирішувати інформаційно-комп'ютерна експертиза? У яких категоріях справ типово виникає потреба у її проведенні?
- ✓ Що є об'єктами апаратно-комп'ютерної експертизи? Які завдання може вирішувати апаратно-комп'ютерна експертиза та у яких справах (ситуаціях) виникає потреба у її проведенні?
- ✓ Які завдання вирішує телекомунікаційна експертиза та що є її об'єктами? У яких справах (ситуаціях) виникає необхідність її проведення?
- ✓ Чим є телематичні модулі? Які функції виконують та яку інформацію можуть містити? У яких категоріях проваджень вони можуть бути важливим джерелом доказової інформації?

| | |
|--|--|
| | <ul style="list-style-type: none"> ✓ Вкажіть приклади комплексних комп'ютерно-технічних та телекомунікаційних судових експертиз у колаборації з іншими судовими експертизами. ✓ Де знайти судового експерта в разі необхідності проведення комп'ютерно-технічної чи телекомунікаційної судової експертизи? ✓ Чи належить комп'ютерно-технічна та/чи телекомунікаційна судова експертиза до державної судово-експертної монополії? ✓ Чи можна доручити виконання телекомунікаційної судової експертизи інженеру ПрАТ Київстар? ✓ Чи можна доручити виконання комп'ютерно-технічної експертизи професору факультету прикладної математики? Якщо так, то за яких умов? ✓ На підставі яких процесуальних документів проводиться судова експертиза. Назвіть їх залежно від суб'єкта провадження, який залучає судового експерта. Які обов'язкові відомості повинні у них міститися? Чим відрізняються зазначені документи? ✓ Як потрібно упакувати та які правила схоронності дотримати щодо об'єктів, які надаються на судово-експертне дослідження? ✓ Які особливості криптовалюти як засобу платежів між злочинцями? ✓ Виберіть правильні твердження щодо «eDiscovery». ✓ Які з наведених нижче речей можуть мати доказове значення і бути об'єктом дослідження для комп'ютерної криміналістики? ✓ Що з наведеного нижче описує переваги доказів електронною поштою? ✓ Який із наведених термінів найкраще описує приховування, модифікацію або приховування цифрових доказів? ✓ Чи передбачено у національному законодавстві поняття «кіберзлочин»? ✓ Як співвідносяться поняття «кіберзлочин» та «комп'ютерний злочин»? Кіберзлочин - це? Комп'ютерний злочин - це? ✓ Кіберпростір відповідно до українського законодавства - це? ✓ У нормах якого закону передбачено відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку? ✓ Які види злочинних діянь віднесені до кіберзлочинів відповідно до Конвенції про кіберзлочинність? ✓ Які діяння є правопорушеннями проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відповідно до Конвенції про кіберзлочинність? ✓ Які діяння є правопорушеннями, пов'язаними з комп'ютерами, відповідно до Конвенції про кіберзлочинність? ✓ Чи передбачена в Україні кримінальна відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж? ✓ Який вид відповідальності відповідно до національного законодавства України передбачено за несанкціонований 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? ✓ Що слід розуміти під «кіберзлочинністю» у широкому розумінні? ✓ Що слід розуміти під «кіберзлочинністю» у вузькому розумінні? ✓ Які класифікації кіберзлочинів вам відомі? ✓ Виберіть діяння, які не є кіберзлочинами. |
|--|--|

- ✓ Виберіть твердження, які правильно характеризують кіберзлочини. Виберіть способи вчинення кіберзлочинів, пов'язаних з несанкціонованим доступом і перехопленням.
- ✓ Виберіть способи вчинення кіберзлочинів, пов'язаних зі зміною комп'ютерних даних.
- ✓ Виберіть способи вчинення комп'ютерних шахрайств.
- ✓ Виберіть способи вчинення кіберзлочинів, пов'язаних з незаконним копіюванням.
- ✓ Виберіть способи вчинення комп'ютерного саботажу.
- ✓ Що таке комп'ютерний абордаж, крадіжка часу, логічна бомба, троянський кінь, комп'ютерний вірус, комп'ютерний черв'як?
- ✓ Що таке комп'ютерна підробка?
- ✓ Що таке телефонне шахрайство?
- ✓ Виберіть твердження, які правильно характеризують типові способи приховування кіберзлочинів.
- ✓ Виберіть твердження, які правильно характеризують знаряддя вчинення кіберзлочинів.
- ✓ Виберіть твердження, які правильно характеризують предмет посягання кіберзлочинів.
- ✓ Виберіть твердження, які правильно характеризують місце вчинення кіберзлочинів.
- ✓ Виберіть твердження, які правильно характеризують особу кіберзлочинця.
- ✓ Виберіть твердження, які правильно характеризують особу потерпілого від кіберзлочину.
- ✓ Виберіть твердження, які правильно характеризують типову слідову картину кіберзлочинів.
- ✓ Які ознаки можуть вказувати на факт несанкціонованого доступу до інформаційної системи або мережі?
- ✓ Як можна виявити факт несанкціонованого доступу до інформаційної системи або мережі?
- ✓ Які особливості огляду місця події при розслідуванні кіберзлочинів?
- ✓ Який алгоритм дій слідчого під час огляду місця події кіберзлочину, якщо під час такого огляду комп'ютера, який має з'єднання із мережею, виникли підозри у використанні хмарних сервісів?
- ✓ Який алгоритм дій слідчого після завершення вилучення енергозалежних і тимчасових даних в ході огляду місця події кіберзлочину?
- ✓ Які відомості підлягають фіксації у протоколі огляду місця події кіберзлочину?
- ✓ Що таке "латентність кіберзлочинів"? Причини, які впливають на латентність кіберзлочинів?
- ✓ Чи міститься термін "кібернасильство" у національному законодавстві України? Чи передбачена кримінальна відповідальність за вчинення кібернасильства в Україні?
- ✓ Що таке сталкінг? Чи може сталкінг вчинятися у кіберпросторі? Яка відповідальність передбачена за вчинення кіберсталкінгу в Україні?
- ✓ Що слід розуміти під поняттям "секстинг"? Чи є таке діяння кримінально караним?
- ✓ Що розуміти під поняттям "доксинг"? Чи передбачена відповідальність за вчинення такого діяння в Україні?
- ✓ Положення яких міжнародних документів державам варто брати до уваги при здійсненні розвитку законодавства в сфері встановлення відповідальності за вчинення різних видів кібернасильства?

| | |
|-------------------|--|
| | <ul style="list-style-type: none"> ✓ Які діяння можуть розглядатися як сексуальні домагання в Інтернеті? ✓ Як співвідносяться поняття “кібернасильство” та “кібербулінг”? Чи передбачена в Україні відповідальність за вчинення “кібербулінгу”? ✓ Чи може вчинятися домашнє насильство в кіберпросторі? Які діяння підпадають під ознаки домашнього насильства в кіберпросторі? ✓ За яких умов видавання однієї особи за іншу в кіберпросторі може підпадати під ознаки кібернасильства? ✓ Чи може здійснюватися економічне насильство за допомогою цифрових технологій? ✓ Оберіть, за поширення чого (якої інформації) в мережі Інтернет КК України передбачає відповідальність. ✓ У чому може виражатися поширення в мережі Інтернет публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ст. 109 КК України)? ✓ В чому суть публічних закликів до зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (ст. 110 КК України)? ✓ Який злочин становитиме поширення в мережі Інтернет інформації про необхідність проведення місцевих референдумів з метою проголошення певної адміністративно-територіальної одиниці України суверенною державою? ✓ Що у міжнародному та національному праві розуміють під розпалюванням національної чи релігійної ворожнечі у міжнародному праві розуміють заклики до дискримінації, насильства чи знищення майна на основі релігії чи національності? ✓ Який злочин становить заклики у соціальних медіа прогнати певну соціальну групу (за релігійною, етнічною, статевою ознакою) з певної території? ✓ Чи може у спосіб поширення певної інформації в Інтернеті вчинятися державна зрада? ✓ Оберіть форми вчинення в мережі Інтернет колабораційної діяльності (ст.111-1 КК України)? ✓ Які Інтернет ресурси є найпоширенішим місцем вчинення колабораційної діяльності (ч. 1 ст. 111-1 КК)? ✓ Оберіть ознаки типового колаборанта в мережі Інтернет (за узагальненням на основі вироків 2022-23 років). ✓ У чому може виражатися виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України, глорифікація її учасників (ст. 436-2 КК України)? ✓ Чи може особу бути притягнути до кримінальної відповідальності за «лайк» в соціальних медіа? Якщо так, то чому? ✓ Поширення в мережі Інтернет символіки яких політичних режимів є кримінально-караним? |
| Опитування | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу. |