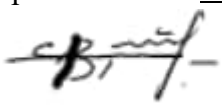
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(протокол № 15/23 від 29 серпня 2023 р.)



Завідувач кафедри Венгерський П.С.

Силабус з навчальної дисципліни "Комп'ютерна криміналістика", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Комп'ютерна криміналістика
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Калужна Оксана Михайлівна доцент кафедри кримінального процесу і криміналістики;
Контактна інформація викладачів	oksana.kaluzhna@lnu.edu.ua https://law.lnu.edu.ua/employee/kaluzhna-oksana-myhajlivna 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 "Комп'ютерна криміналістика" є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 5-му семестрі в обсязі 3-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Цифрова криміналістика (форензика) - це судова наука практичного спрямування, започаткована у 1970-80-х рр., вивчає відновлення та дослідження у цифрових пристроях даних, пов'язаних з кіберзлочинністю. Зростання кіберзлочинності вимагає для її розслідування залучення спеціальних технічних знань. Без належно знайдених, зібраних та оформлених доказів неможливо висунути певній особі обвинувачення та притягнути її до відповідальності. Цифрова криміналістика – традиційно охоплює не лише рекомендації, прийоми і засоби викриття та розслідування уже вчинених кіберзлочинів та інших цифрових зловживань, а й рекомендації щодо їх запобігання й випередження – тобто кібербезпеку. Крім цього, закономірності розслідування кіберзлочинів рівною мірою використовуються й у спорах між компаніями та/або фізичними особами (в рамках цивільного права), коли цифрового спеціаліста залучають до відшукання інформації про особу чи компанію, https://pl.alegsaonline.com/o/39908перевіривши їх комп'ютер. Для опису цього типу розслідувань використовується спеціальний термін «eDiscovery». Кібербезпека і кіберрозслідування тісно взаємопов'язані, проте суттєво відрізняються. Кіберрозслідування досліджує незаконну та/або шкідливу поведінку в Інтернеті, її рушійні сили, а кібербезпека - прогнозування, уникнення та реагування на ці дії.
Мета та цілі дисципліни	***Мета спецкурсу***: розвиток навичок у галузі інформаційної безпеки та цифрової криміналістики на основі поєднання теорії і практичних вмінь. За допомогою курсу студенти освоять ключові методи розслідування кіберзлочинів та порушень безпеки, ознайомляться як збирати цифрові

	докази, досліджувати й аналізувати цифрову інформацію з метою відтворити хронологію вчинення кіберзлочину чи іншого кібер-інциденту. Після завершення курсу від студентів очікується розуміння процедур та методів, що застосовуються при розслідуванні кіберзлочинів та інших комп'ютерних зловживань, використання в судочинстві цифрових (електронних доказів), а також уявлення про суміжні навчальні дисципліни. Курс цифрової криміналістики навчає критично ставити питання, «мислити як хакер», приймати технологічні рішення з дотриманням нормативно-правових актів. Особливістю курсу є поєднання знань ІТ та юридичної основи. ІТ-криміналістам потрібні знання права, адже результати цифрового полювання мають вистояти в суді як докази.
Література для вивчення дисципліни	1. 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. 2. 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 3. 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. 4. Кіберполіція попереджає про активізацію хакерів в період карантину. *Офіційний сайт кіберполіції України*. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-aktyvizacziyu-xakeriv-v-period-karantynu-617/ 5. Немного ресурсов по форензике (практика расследования кибер-преступлений). URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344671.php 6. Павлюк Н. В. Інтеграція інноваційний 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 7. 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 8. 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 9. Anderson, P., Sampson, D., & Gilroy, S. (2021). *Digital investigations: relevance and confidence in disclosure*. ERA Forum, 22 (4). 587-599. ISSN 1612-3093. 10. Android research and analysis tool Andr Ex R. *AOS company*. URL: https://www.fss.jp/android_andrex_r/ 11. AOS Image Analysis Forensics Professional. *AOS company*. URL: https://www.fss.jp/fss_movie01-2/ 12. Årnes, A. (2018). *Digital forensics*. Hoboken, NJ: John Wiley & Sons Inc. 13. Bodo Meseke. Digitale Forensik. Praxiswissen Cybercrime für Manager. Berlin. 2019. https://www.weltbild.de/artikel/ebook/digitale-forensik_34575890-1?ln=UHJvZHVrdHxNZWhyIELDvGNoZXIgZGVzIEF1dG9ycw==

14. Britz, M. (2013). Computer Forensics and Cyber Crime: An Introduction. Pearson.
15. 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
16. Carlton, A. (2020). Sextortion: the hybrid cyber-sex crime. *North Carolina Journal of Law & Technology*, 21(3), 177-216.
17. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Cham: Springer International Publishing.
18. Chen, L., Takabi, H., & Le-Khac, N.-A. (2019). *Security, privacy and digital forensics in the cloud*. Hoboken, NJ: John Wiley & Sons.
19. *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
20. Dalrymple, B. E., & Smith, E. J. (2018). *Forensic Digital Image Processing: Optimization of Impression Evidence*. Boca Raton, FL: CRC Press.
21. 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
22. Digitale Forensik/IT Forensik – berufsbegleitender Online-Fernstudiengang. URL: http://www.master-digitale-forensik.de/
23. EC-Council Press. (2010). *Computer forensics*. Clifton Park, NY: Course Technology.
24. Freeman, L. (2018). Digital evidence and war crimes prosecutions: the impact of digital technologies on international criminal investigations and trials. *FordhamInternational Law Journal*, 41(2), 283-336.
25. 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
26. Hassan, N. A. (2019). *Digital forensics basics: A practical guide using Windows OS*. New York: Apress.
27. Hayes, D. R., & Walczak, T. (2021). *Informatyka w kryminalistyce: Praktyczny przewodnik*. Gliwice: Helion.
28. Ho, A. T. S., & Li, S. (2015). *Handbook of digital forensics of multimedia data and devices*. Chichester: Wiley.
29. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. London: Routledge, Taylor & Francis Group.
30. 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
31. Kasprzak, W. A. (2015). *Ślady cyfrowe: Studium prawno-kryminalistyczne*. Warszawa: Difin.
32. Kävrestad, J. (2017). *Guide to Digital Forensics: A Concise and Practical Introduction*. Cham: Springer International Publishing.
33. Kävrestad, J. (2018). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. Cham: Springer International Publishing.
34. Kleiman, D. (2007). *The official CHFI study guide (Exam 312-49): For computer hacking forensic investigator*. Syngress.

35. Kotsiuba, I., Skarga-Bandurova, I., Giannakoulias 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
36. Labudde, D., & Spranger, M. (2017). *Forensik in der digitalen Welt*. Berlin, Heidelberg: Springer Berlin Heidelberg.
37. Latysh, K. K. (2021). Criminalistics Analysis of Cyber Tools for Committing Crimes. *Problems of Legality*, 153, 165-172.
38. 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
39. Leroux, O. (2004). Legal admissibility of electronic evidence, International Review of Law, Computers & Technology, 18:2, 193-220. 10.1080/1360086042000223508
40. Lewulis, P. (2021). *Dowody cyfrowe: Teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.
41. Lin, X. (2018). *Introductory Computer Forensics: A Hands-on Practical Approach*. Cham: Springer International Publishing.
42. Luttgens, J., Mandia, K., & Pepe, M. (2014). *Incident Response & Computer Forensics, Third Edition*. McGraw-Hill.
43. Maras, M.-H. (2015). *Computer forensics: Cybercriminals, laws, and evidence*. Burlington, MA: Jones & Bartlett Learning.
44. 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).
45. Pandelica, I. (2020). The phenomenon of cyber crime. International Journal of Information Security and Cybercrime, 9(1), 29-36.
46. 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.
47. Paweł Olbe. Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych. Wydawnictwo: Wyższa Szkoła Policji w Szczytnie. 2021. 412 S.
48. Philipp, A., Cowen, D., Davis, C. M., & Scharringhausen, L. S. (2010). *Hacking exposed computer forensics*. New York: McGraw-Hill.
49. Phillips, A., Nelson, B., & Steuart, C. (2019). *Guide to computer forensics and investigations: Processing digital evidence*. Boston: Cengage Learning.
50. 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
51. Popular Computer Forensics Top 21 Tools [Updated for 2019]. *Infosec*. 2019. URL: https://resources.infosecinstitute.com/computer-forensics-tools/#gref
52. Prasad, Ajay & Pandey, Jeetendra. (2016). *Digital Forensics*. Uttrakhand Open University.
53. Quan, W. (2019). Cyber economic crimes: challenges and countermeasures of the Chinese police. *China Legal Science*, 7(3), 67-94.

54. 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
55. 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
56. Sachowski, J. (2016). *Implementing Digital Forensic Readiness : From Reactive to Proactive Process*. Elsevier Science.
57. Sachowski, J. (2018). *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*. London: Taylor and Francis.
58. Sammons, J. (2012). *The basics of digital forensics: The primer for getting started in digital forensics*. Syngress.
59. Sammons, J. (2016). *Digital forensics: Threatscape and best practices*. Amsterdam: Syngress.
60. Shavers, B. (2013). *Placing the suspect behind the keyboard: Using digital forensics and investigative techniques to identify cybercrime suspects*. Waltham, MA: Syngress.
61. Sunde, N. (2022). *Unpacking the evidence elasticity of digital traces*, Cogent. Social Sciences, 8:1, 2103946, DOI: 10.1080/23311886.2022.2103946
62. TrapX Security DeceptionGrid 6.3. *SC Media magazine*. 14 August 2019. URL: https://www.scmagazine.com/review/trapx-security-deceptiongrid-6-3/
63. 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.
64. Volonino, L., & Anzaldua, R. (2008). *Computer forensics for dummies*. Hoboken, NJ: Wiley.
65. Widup, S. (2014). *Computer forensics and digital investigation with Encase Forensic v7*. New York : McGraw-Hill Education.
66. Zarpala, L., & Casino, F. (2021). A blockchain-based forensic model for financial crime investigation: the embezzlement scenario. *Digit Finance* 3, 301–332. https://doi.org/10.1007/s42521-021-00035-5
67. 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
68. Що таке комп'ютерна криміналістика (форензіка)? *GROSS digital forensics Lab.* 2017. URL: https://g-ross.com.ua/novyny/kompyuterna-kryminalistyka-forenzika.html
69. Що таке цифрова криміналістика*? GROSS digital forensics Lab.* 2018. URL: https://g-ross.com.ua/novyny/cyfrova-kryminalistyka-2.html

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/
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 42 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: ***знати:*** • в чому полягає робота цифрового криміналіста; • характеристику злочинності, що вчиняється в мережі Інтернет та програми (методи, алгоритми) їх розслідування; • криміналістичний 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 цифрові докази, в тому числі - факт використання та володіння комп'ютерними програмами, іграми, мультимедійним контентом, • як реагувати на інциденти (розпізнати кібератаку та сповістити правоохоронні органи); ***вміти:*** • виявляти, та процесуально документувати цифрові докази; • підтверджувати (доводити) достовірність, належність та допустимість цифрових 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. **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.**
Ключові слова	Кіберзлочин, кібеззлочинність, компютерна криміналістика, цифрова криміналістика, кібер-детектив, цифрові докази, електронні докази, електронні документи, допустимість цифрових доказів, процесуальні умови і загальна тактика зняття інформації з каналів звязку, звід відомостей про державну таємницю, судова компютерно-технічна експертиза, судова телекомунікаційна експертиза, «eDiscovery».
Формат курсу	Очний
Теми	Теми подано в схемі курсу
Підсумковий контроль, форма	Залік у кінці семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Серед методів навчання, зокрема, застосовуються: розповідь, пояснення, бесіда, лекція, демонстрація (презентація), спостереження, практичне заняття, індивідуальні завдання, дослідні проекти, модульний контроль 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.

	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.
Необхідне обладнання	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
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • індивідуальні завдання: 50% семестрової оцінки; • модуль: 50% семестрової оцінки. Максимальна кількість балів – 50 балів. Підсумкова максимальна кількість балів – 100 балів. **Оцінювання поточної успішності:** *Поточна успішність* (оцінюється за 50-бальною шкалою): Відмінно (50) Добре (40; 45) Задовільно (26; 31) Незадовільно (0) **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. **Модуль:** Модуль здійснюється в тестовій формі з використанням програми Мудл - **https://e-learning.lnu.edu.ua/course/view.php?id=5187.** Модульне завдання для кожного студента включає 20 тестових запитань, з яких 10 першого рівня складності по 2 бали за правильну відповідь, і 10 – другого рівня по 3 (до 3-х) балів за правильну відповідь. У тестах першого рівня складності 4-5 варіантів відповідей, серед яких лише одна правильна. У тестах 2-го рівня складності є від 2 до 4 правильних відповіді серед понад 6 варіантів відповідей. Студенту потрібно обрали лише правильні відповіді. Вказування неправильної відповіді знімає бал, пропорційний до ціни (%) варіанта правильної відповіді. Студент має право перездати модуль за правилами перездач. На модуль виносяться лише питання, які розглядались на лекціях та лабораторних заняттях, відображені в презентації, текстах лекцій, наданих студентам викладачами. **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 одинакові роботи студентів не перевіряються з 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. **Відвідування занять** є добровільним для лекційної форми і обов'язковим для лабораторних. Викладач фіксує неявку студента на практичне заняття, що вважається академічною заборгованістю, яку студент повинен відпрацювати до дня виставлення заліку. Відпрацювання полягає у перевірці підготовки студентом тих самих завдань, які виносилися на практичне заняття, на якому студент був відсутній. **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.

	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 теоретико - правову позицію; 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. **Жодні форми порушення академічної доброчесності не толеруються.**
Питання до контролю	1. Поняття комп'ютерної криміналістики та її соціальна мета і значення. 2. Система комп'ютерної криміналістики 3. Знання, навички та підготовка, кібер-криміналіста. 4. Сфера працевлаштування. 5. Історія комп'ютерної криміналістики за кордоном та в Україні (США, ВБ, міжнародні слідчі органи із застосуванням комп'ютерної криміналістики). 6. Які вам відомі закономірності (способи) становлення самостійних наук на сьогоднішньому цивілізаційному етапі? Приведіть приклади появи самостійних наук у спосіб виділення та у спосіб синтезу. 7. Як і коли відбувалося становлення «комп'ютерної криміналістики»? 8. Чи є термін «комп'ютерна криміналістика» коректним з точки зору сьогоднішнього технологічного рівня розвитку людства? Чому (з яких мотивів) він досі використовується? Якими іншими термінами-синонімами позначається ця наука та практична сфера діяльності? 9. Якими альтернативними термінами-синонімами йменується фах кібер-криміналіста? 10. Що (які об'єкти та процеси) є предметом вивчення (дослідження) «комп'ютерної криміналістики»? 11. Яким є місце «комп'ютерної криміналістики» в системі наук? Це ІТ-наука чи юридична наука? 12. Як співвідносяться комп'ютерна криміналістика та кібербезпека? 13. Які пристрої можуть входити до системи «розумний дім»? Як вона організована? Які функції може виконувати? 14. Які загрози можуть походити від Інтернет-речей (Internet of Things)? 15. Чому криптовалюти є зручними для платежів між злочинцями? 16. Яка специфіка темних веб-магазинів (dark web)? 17. Якою є система комп'ютерної криміналістики? Охарактеризуйте її підгалузі. 18. Чим займається напрям «комп'ютерної криміналістики» «eDiscovery»? 19. Для яких потреб (напрямків) цивільного життя найчастіше залучається інструментарій (можливості) комп'ютерної криміналістики? 20. Яка роль і можливості комп'ютерної криміналістики при розслідуванні злочинів, які не є кібернетичними? 21. Як називається пристрій банкоматів для зчитування інформації, записаної на магнітній смузі кредитних або дебетових карток? 22. Як називається короткочасна енергонезалежна пам'ять, вміст якої зникає при вимкненні комп'ютера? У яких ситуаціях її слід враховувати? 23. Які можливості комп'ютерної криміналістики для дослідження фото- і відео-зображень з відкритих джерел (з мережі Інтернет) для доказування воєнних злочинів рф в Україні? 24. Якою є історія походження терміну «комп'ютерні докази» та його трансформація? 25. Сучасне поняття та властивості цифрових доказів? 26. Оформлення (у процесуальних документах) цифрових доказів та можливості їх дослідження. 1 27. Що вам відомо про доказовий ланцюжок роботи з цифровим доказом? 28. Чи мають комп'ютерні докази ефект новинки? В чому суть доктрини «доказу-новинки» (novel evidence)? Звідки вона походить? 29. Яке співвідношення між поняттями «комп'ютерні докази»,

	«цифрові докази», «електронні докази»? 30. Розкрите основні властивості комп'ютерних доказів. Чи автентичним є використання в доказуванні копій (дублікатів) комп'ютерних доказів і оригіналів? Чому? 31. Яким є співвідношення між поняттями «електронні докази» та «електронні документи»? Що становлять собою електронні документи (зовнішня і внутрішня структура, вимоги, спосіб оформлення та засвідчення)? 32. Якими є можливості комп'ютерних доказів для вирішення кримінальних справ? 33. Розкрийте суть такого напрямку використання комп'ютерних доказів як для доказування наміру (мотиву). 34. Розкрийте суть такого напрямку використання комп'ютерних доказів як для доказування алібі (digital alibi). 35. Охарактеризуйте основні способи дослідження комп'ютерних доказів у суді. 36. До якого класу судової експертизи належать комп'ютерно-технічна та телекомунікаційна судові експертизи? 37. Якими нормативними актами визначені назви та шифри (цифрові позначення) експертних спеціальностей зазначених для даних родів судової експертизи? 38. Назвіть види комп'ютерно-технічної експертизи. 39. Які питання може вирішувати програмно-комп'ютерна експертиза? У яких категоріях справ типово виникає потреба у її проведенні? 40. Які питання може вирішувати інформаційно-комп'ютерна експертиза? У яких категоріях справ типово виникає потреба у її проведенні? 41. Що є об'єктами апаратно-комп'ютерної експертизи? 42. Які завдання може вирішувати апаратно-комп'ютерна експертиза та у яких справах (ситуаціях) виникає потреба у її проведенні? 43. Які завдання вирішує телекомунікаційна експертиза та що є її об'єктами? У яких справах (ситуаціях) виникає необхідність її проведення? 44. Чим є телематичні модулі? Які функції виконують та яку інформацію можуть містити? У яких категоріях проваджень вони можуть бути важливим джерелом доказової інформації? 45. Вкажіть приклади комплексних комп'ютерно-технічних та телекомунікаційних судових експертиз у колаборації з іншими судовими експертизами. 46. Де знайти судового експерта в разі необхідності проведення комп'ютерно-технічної чи телекомунікаційної судової експертизи? 47. Чи належить комп'ютерно-технічна та/чи телекомунікаційна судова експертизи до державної судово-експертної монополії? 48. Чи можна доручити виконання телекомунікаційної судової експертизи інженеру ПрАТ Київстар? 49. Чи можна доручити виконання комп'ютерно-технічної експертизи професору факультету прикладної математики? Якщо так, то за яких умов? 50. На підставі яких процесуальних документів проводиться судова експертиза. Назвіть їх залежно від суб'єкта провадження, який залучає судового експерта. Які обовязкові відомості повинні у них міститися? Чим відрізняються зазначені документи? 2 51. Як потрібно упакувати та які правила схоронності дотримати щодо об'єктів, які надаються на судово-експертне дослідження? 52. Коли відбулося становлення «комп'ютерної криміналістики»? 53. Якими термінами НЕ позначається «комп'ютерна криміналістика» як наука та практична сфера діяльності? 54. Що є предметом вивчення (дослідження) «комп'ютерної криміналістики»? 55. Виберіть правильні твердження щодо співвідношення комп'ютерної криміналістики та кібербезпеки? 56. Які особливості криптовалюти як засобу для платежів між злочинцями? 57. Виберіть правильні твердження щодо специфіки веб-магазинів (dark web)? 58. Виберіть підгалузі комп'ютерної криміналістики. 59. Виберіть правильні твердження щодо «eDiscovery» як напряму комп'ютерної криміналістики. 60. Для яких потреб (напрямків) цивільного життя може залучатися інструментарій (можливості) комп'ютерної криміналістики? 61. Як називається пристрій банкоматів для зчитування інформації, записаної на магнітній смузі кредитних або дебетових карток? 62. Як називається короткочасна енергонезалежна пам'ять, вміст якої зникає при вимкненні

	комп'ютера? 63. Виберіть правильні твердження щодо доктрини «доказу-новинки» (novel evidence)? 64. Виберіть правильні твердження щодо співвідношення між поняттями «комп'ютерні докази», «цифрові докази», «електронні докази»? 65. Виберіть властивості комп'ютерних доказів. 66. Виберіть правильні твердження щодо співвідношення між поняттями «електронні докази» та «електронні документи»? 67. Що таке електронний документ? 68. Виберіть правильні твердження щодо сутності та властивостей електронних документів. 69. В чому полягає суть такого напрямку використання комп'ютерних доказів як для доказування наміру (мотиву)? 70. В чому полягає суть такого напрямку використання комп'ютерних доказів як для доказування алібі (digital alibi)? 71. Виберіть основні способи дослідження комп'ютерних доказів у суді. 72. Яке з наступних тверджень найкраще визначає комп'ютерну криміналістику? 73. Що таке доказовий ланцюжок роботи з цифровим доказом? 74. Що це таке «слідча інформатика»? 75. Які з наведених нижче речей можуть мати доказове значення і бути обєктом дослідження для комп'ютерної криміналістики? 76. Що з наведеного нижче описує переваги доказів електронною поштою? 77. Який із наведених термінів найкраще описує приховування, модифікацію або приховування цифрових доказів? 78. Чи передбачено у національному законодавстві поняття "кіберзлочин"? 79. Як співвідносяться поняття "кіберзлочин" та "комп'ютерний злочин"? 80. Кіберзлочин - це? 81. Комп'ютерний злочин - це? 82. Кіберпростір відповідно до українського законодавства - це? 3 83. 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? 84. Чи визначено у Конвенції про кіберзлочинність зміст поняття "кіберзлочинність"? 85. Які види злочинних діянь віднесені до кіберзлочинів відповідно до Конвенції про кіберзлочинність? 86. Які діяння є правопорушеннями проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відповідно до Конвенції про кіберзлочинність? 87. Які діяння є правопорушеннями, пов'язаними з комп'ютерами, відповідно до Конвенції про кіберзлочинність? 88. Чи передбачена в Україні кримінальна відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж? 89. 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? 90. Що слід розуміти під "кіберлочинністю" у широкому розумінні? 91. Що слід розуміти під "кіберлочинністю" у вузькому розумінні? 92. Які класифікації кіберзлочинів Вам відомі? 93. Виберіть діяння, які не є кіберзлочинами. 94. Виберіть твердження, які правильно характеризують кіберзлочини. 95. Виберіть способи вчинення кіберзлочинів, пов'язаних з несанкціонованим доступом і перехопленням. 96. Виберіть способи вчинення кіберзлочинів, пов'язаних зі зміною комп'ютерних даних. 97. Виберіть способи вчинення комп'ютерних шахрайств. 98. Виберіть способи вчинення кіберзлочинів, пов'язаних з незаконним копіюванням. 99. Виберіть способи вчинення комп'ютерного саботажу. 100. Що таке комп'ютерний абордаж? 101. Що таке крадіжка часу? 102. Що таке логічна бомба? 103. Що таке троянський кінь? 104. Що таке комп'ютерний вірус? 105. Що таке комп'ютерний черв'як? 106. Що таке комп'ютерна підробка? 107. Що таке телефонне шахрайство? 108. Виберіть способи вчинення? 109. Виберіть твердження, які правильно характеризують типові способи приховування кіберзлочинів. 110. Виберіть

	твердження, які правильно характеризують знаряддя вчинення кіберзлочинів. 111. Виберіть твердження, які правильно характеризують предмет посягання кіберзлочинів. 112. Виберіть твердження, які правильно характеризують місце вчинення кіберзлочинів. 4 113. Виберіть твердження, які правильно характеризують особу кіберзлочинця. 114. Виберіть твердження, які правильно характеризують особу потерпілого від кіберзлочину. 115. Виберіть твердження, які правильно характеризують типову слідову картину кіберзлочинів. 116. Які ознаки можуть вказувати на факт несанкціонованого доступу до інформаційної системи або мережі? 117. Як можна виявити факт несанкціонованого доступу до інформаційної системи або мережі? 118. Які особливості огляду місця події при розслідуванні кіберзлочинів? 119. Який алгоритм дій слідчого під час огляду місця події кіберзлочину, якщо під час такого огляду комп'ютера, який має з'єднання із мережою, виникли підозри у використанні хмарних сервісів? 120. Який алгоритм дій слідчого після завершення вилучення енергозалежних і тимчасових даних в ході огляду місця події кіберзлочину? 121. Які відомості підлягають фіксації у протоколі огляду місця події кіберзлочину? 122. Що таке "латентність кіберзлочинів"? 123. Причини, які впливають на латентність кіберзлочинів? 124. Чи міститься термін "кібернасильство" у національному законодавстві України? 125. Чи передбачена кримінальна відповідальність за вчинення кібернасильства в Україні? 126. Що таке сталкінг? 127. Чи може сталкінг вчинятися у кіберпросторі? 128. Яка відповідальність передбачена за вчинення кіберсталкінгу в Україні? 129. Що слід розуміти під поняттям "секстинг"? Чи є таке діяння кримінально караним? 130. Що розуміти під поняттям "кріпшоти"? Чи передбачена відповідальність за їх поширення? 131. Що розуміти під поняттям "доксинг"? Чи передбачена відповідальність за вчинення такого діяння в Україні? 132. Положення яких міжнародних документів державам варто брати до уваги при здійсненні розвитку законодавства в сфері встановлення відповідальності за вчинення різних видів кібернасильства? 133. Як співвідноситься поняття "кібернасильство" та "насильство проти жінок"? 134. Які діяння можуть розглядатися як сексуальні домагання в Інтернеті? 135. Як співвідносяться поняття "кібернасильство" та "кібербулінг"? 136. Чи передбачена в Україні відповідальність за вчинення "кібербулінгу"? 137. Чи може вчинятися домашнє насильство в кіберпросторі? 138. Які діяння підпалають під ознаки домашнього насильства в кіберпросторі? 139. За яких умов видавання однієї особи за іншу в кібепросторі може підпадати під ознаки кібернасильства? 140. Чи може здійснюватися економічне насильство за допомогою цифрових технологій?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання

1-2	**Цифрові (електронні) сліди та докази** Цифрова криміналістика – наука про цифрові сліди. Поняття цифрової інформації та слідів її створення, зміни, транспортування, зміни, відновлення. Поняття цифрових (електронних) доказів. Вимоги до оформлення цифрових доказів для набуття ними статусу судового доказу. Види електронних (цифрових) доказів.	лекція, Самостійна робота лаб		2 6 4	2 тижні
3-4	**Використання цифрових технологій та збір цифрових доказів під час досудового розслідування та судового розгляду** ***SINT.*** 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). Встановлення (ідентифікація) кінцевих користувачів мережевого обладнання. 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.. Пошук необхідних для розслідування інциденту цифрових даних, в тому числі прихованих і віддалених, та оформлення їх за правилами судових доказів. Залучення спеціалістів–ІТ-фахівців до проведення оглядів, обшуків, НСРД для їх технічного супроводу.	лекція, Самостійна робота лаб		2 4 4	2 тижні
5	***Відео-криміналістика***. Відеофіксація гласних і негласних слідчих дій. Поліпшення якості відео, збільшення окремих ділянок	лекція, Самостійна робота		2 2	1 тиждень

	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.	лаб		2	
6	***Мережева криміналістика.*** Аналіз і відстеження мережевого трафіку, локального і глобального Інтернету, збір доказів і виявленням вторгнень у систему. Програмне забезпечення для аналізу великих обсягів даних (перехопленого трафіку, сегмента мережі Інтернет).	Самостійна робота лаб		2 2	1 тиждень
7	***Криміналістика 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.) з сучасних мобільних пристроїв. Відновлення видалених даних; вилучення інформації з хмарних сховищ і онлайн сервісів.	лекція, Самостійна робота лаб		2 6 2	1 тиждень
8-10	Тема 3: **Судова комп'ютерно-технічна експертиза** Комп'ютерно-технічна експертиза під час розслідування кіберзлочинів, господарських та цивільних спорів. Можливості (коло вирішуваних питань) 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.	лекція, Самостійна робота лаб		2 8 6	3 тижні

	Цифрові технології під час проведення інших судових експертиз: криміналістичних, технічних, економічних, медичних, психологічних тощо. Програмні судово-експертні методики на службі різних видів судових експертиз.				
11	Тема 4. **Розслідування кіберзлочинів** Поняття та кримінологічна, кримінально-правова та криміналістична характеристика кіберзлочинності. Види кіберзлочинів. Виявлення ботоферм та злочини, що вчинються за їх посередництва. Розслідування злочинів проти основ національної безпеки, проти громадської безпеки, виборчих злочинів, що вчиняються в мережі.	лекція, Самостійна робота лаб		2 2 2	1 тиждень
12	***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.	лекція Самостійна робота лаб		2 2 2	1 тиждень
13	***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»). Незаконне втручання в приватне спілкування. Розслідування розповсюдження в мережі інтернет порнографії. Розслідування кібернасильства та злочинів сексуального характеру. Dark-web.	лекція, Самостійна робота лаб		2 4 2	1 тиждень

14-16	Тема 5. **Кібербезпека** Кваліфікована фіксація слідів і збір доказів у випадку підозри на кібератаку. Усунення наслідків інциденту, діагностування проблем і надання рекомендації, які дозволять запобігти повторенню інцидентів в майбутньому. Технічні канали витоку інформації. Методи і засоби блокування витоку інформації. Спеціальне програмне забезпечення для діагностування проникнення. Організація кібербезпеки робочого місця. Правила безпечного зберігання інформації.	лекція, Самостійна робота лаб		2 6 6	3 тижні