МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Кафедра кримінального процесу і криміналістики

Затверджено
на засіданні кафедри кримінального
процесу і криміналістики юридичного
факультету Львівського національного
університету імені Івана Франка
(протокол № 1 від 29 серпня 2024 року)

Завідувач кафедри  проф. Бобечко Н.Р.

Силабус з навчальної дисципліни

«ЦИФРОВА КРИМІНАЛІСТИКА ТА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ»,

що викладається в межах ОПП «Технології штучного інтелекту в кібербезпеці» другого (магістерського) рівня вищої освіти для здобувачів зі спеціальності 125 – Кібербезпека та захист інформації

Львів – 2024

Назва дисципліни	**Цифрова криміналістика та розслідування інцидентів**
Адреса викладання дисципліни	м. Львів, вул. Університетська, 1
Факультет та кафедра, за якою закріплена дисципліна	Юридичний факультет Кафедра кримінального процесу і криміналістики
Галузь знань, шифр та назва спеціальності	12 – Інформаційні технології 125 – Кібербезпека та захист інформації
Викладачі дисципліни	**Калужна Оксана Михайлівна,** кандидат юридичних наук, доцент, доцент кафедри кримінального процесу і криміналістики; **Піх Юрій Тарасович**, доктор філософії у галузі права, 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 Місцезнаходження: 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/лабораторних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://law.lnu.edu.ua/course/digital-forensics-and-incident-investigation
Інформація про дисципліну	Дисципліна «Цифрова криміналістика та розслідування інцидентів» є вибірковою дисципліною другого (магістерського) рівня вищої освіти зі спеціальності 125 – Кібербезпека та захист інформації для освітньо-професійної програми «Технології штучного інтелекту в кібербезпеці», яка викладається в 3-му навчальному семестрі в обсязі 3-х 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 кіберінцидентів, а й рекомендації щодо їх запобігання й випередження – тобто кібербезпеку. Крім цього, закономірності розслідування кіберінцидентів 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, перевіривши 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 інших кіберінцидентів, ознайомляться як збирати цифрові докази, досліджувати й аналізувати цифрову інформацію з метою відтворити хронологію вчинення відповідного кіберзлочину чи іншого кіберінциденту. Після завершення курсу від студентів очікується розуміння процедур та методів, що застосовуються при розслідуванні кіберзлочинів та інших кіберінцидентів, використання в судочинстві цифрових (електронних доказів), а також уявлення про суміжні навчальні дисципліни. Курс цифрової криміналістики та розслідування інцидентів навчає критично ставити питання, «мислити як хакер», приймати технологічні рішення з дотриманням нормативно-правових актів. Особливістю курсу є поєднання знань IT та юридичної основи. IT-криміналістам потрібні знання права, адже результати цифрового полювання мають вистояти в суді як докази.
Література для вивчення дисципліни	1. Конвенція Ради Європи про кіберзлочинність від 23.11.2001, ратифікована Законом № 2824-IV від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 29.08.2024). 2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI (зі змін. і доп.). URL: http://zakon2.rada.gov.ua/laws/show/4651-17 (дата звернення: 29.08.2024). 3. Цивільний процесуальний кодекс України від 18.03.2004 № 1618-IV (зі змін. і доп.). URL: http://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 29.08.2024). 4. Використання електронних (цифрових) доказів у кримінальних провадженнях: 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. 5. Електронні докази. Обшук / [О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін.]. Харків: Фактор, 2020. Ч. 1. 80 с. 6. Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України: дис. … канд. юрид. наук: 12.00.09. Київ, 2021. 258 с. 7. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … на здобуття наук. ступеня доктора філософії. Львів, 2021. 248 с. 8. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. Одеса, 2020. 112 с. 9. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дис. … д-ра філос. наук: 12.00.09. Харків, 2021. 369 с.

	10. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с. **Допоміжна:** 1. Bernard, G. (2023). *Digital Forensics and OSINT: The Perfect Match for Investigating Cybercrime*. ISBN 979-8393170554. 2. Johnson, E. (2023). *Digital Forensic 101: Investigating Cyber Incidents – A Digital Forensic Guide*. ISBN 979-8389326828. 3. Johansen, G. (2023). *Digital Forensics and incident response: Incident response tools and techniques for effective cyber threat response*. Packt Publishing. 4. Harisha, A., Mishra, A., & Singh, C. (Eds.). (2023). *Advancements in Cybercrime Investigation and Digital Forensics* (1st ed.). Apple Academic Press. https://doi.org/10.1201/9781003369479 5. Hayes, D. R., & Walczak, T. (2021). *Informatyka w kryminalistyce: Praktyczny przewodnik*. Gliwice: Helion. **Ресурси:** www.master-digitale-forensik.de Верховний Суд – https://supreme.court.gov.ua/ Офіс Генерального прокурора – 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: 32 год., з них 16 год. лекцій та 16 год. лабораторних занять. Самостійної роботи: 58 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.

Ключові слова	Кіберзлочин, кіберзлочинність, інцидент, комп'ютерна криміналістика, цифрова криміналістика, кібер-детектив, розслідування, цифрові докази, електронні докази, електронні документи, допустимість цифрових доказів, процесуальні умови і загальна тактика зняття інформації з каналів зв'язку, звід відомостей про державну таємницю, судова комп'ютерно-технічна експертиза, судова телекомунікаційна експертиза, «eDiscovery».
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	**Тема 1: 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. Значення електронних (цифрових) доказів для розслідування кіберзлочинів та інших інцидентів. **Тема 2: Способи збирання цифрових доказів під час розслідування кіберзлочинів та інших інцидентів.** ***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). Встановлення (ідентифікація) кінцевих користувачів мережевого обладнання. Пошук необхідних для розслідування інциденту цифрових даних, в тому числі прихованих і віддалених, та оформлення їх за правилами судових доказів. Проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій. Залучення спеціалістів–IT-фахівців до проведення оглядів, обшуків, НСРД для їх технічного супроводу. ***Судова комп'ютерно-технічна експертиза.*** Комп'ютерно-технічна експертиза під час розслідування кіберзлочинів та інших кіберінцидентів, зокрема господарських та цивільних спорів. Можливості (коло вирішуваних питань) комп'ютерно-технічної експертизи. 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. Цифрові технології під час проведення інших судових експертиз: криміналістичних, технічних, економічних, медичних, психологічних тощо. Програмні судово-експертні методики на службі різних видів судових експертиз. **Тема 3: E-Discovery та використання цифрових технологій під час розслідування кіберзлочинів та інших інцидентів.** ***E-Discovery (electronic discovery)*** та сфера його використання. Основні аспекти e-Discovery. Джерела даних для e-Discovery. ***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 метаданими. ***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. ***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). ***Криміналістика мобільних пристроїв.*** Дослідження мобільних пристроїв з метою встановлення даних про дзвінки та повідомлення (SMS, E-mail), 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. **Тема 4. Особливості розслідування окремих категорій кіберзлочинів.** Поняття та кримінологічна, кримінально-правова та криміналістична характеристика кіберзлочинності. Види кіберзлочинів. Виявлення ботоферм та злочини, що вчиняються за їх посередництва. ***Кібертероризм***. Розслідування злочинів проти основ національної безпеки, проти громадської безпеки, виборчих злочинів, що вчиняються в мережі. ***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. ***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, COVID-сертифікатів, посвідчення водія тощо у додатку «Дія»). Кіберзлочини проти особистості: кіберсталкінг, кібербулінг, фішинг, крадіжки ідентичності. Кіберзлочини проти приватності. Незаконне втручання в приватне спілкування. Кіберзлочини проти неповнолітніх. Розслідування розповсюдження в мережі Інтернет порнографії. Розслідування кібернасильства та злочинів сексуального характеру. Dark-web.

	Тема 5. Розслідування інших видів кіберінцидентів та їх запобігання. 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.
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, лабораторне заняття, індивідуальні завдання, дослідні проекти, модульний контроль Під час лабораторних 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 лабораторних 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 єдиноправильної 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	Магістранти використовують технічні засоби та програмне забезпечення під час підготовки до лабораторних 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: • лабораторні заняття, 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 системи Moodle – **https://e-learning.lnu.edu.ua.**

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 лабораторних 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 лабораторне 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 лабораторне 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 лабораторних 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 на модуль	1. Поняття цифрової криміналістики та її соціальна мета і значення. 2. Система цифрової криміналістики 3. Знання, навички та підготовка, кібер-криміналіста. 4. Сфера працевлаштування. 5. Історія цифрової криміналістики за кордоном та в Україні (США, Європа, міжнародні

	слідчі органи із застосуванням цифрової 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 «цифрової криміналістики»? 8. Чи є термін «цифрова 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 кіберкриміналіста? 10. Що (які об'єкти та процеси) є предметом вивчення (дослідження) «цифрової криміналістики»? 11. Яким є місце «цифрової криміналістики» в системі наук? Це ІТ-наука чи юридична наука? 12. Як співвідносяться цифрова 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 цифрової криміналістики? Охарактеризуйте її підгалузі. 18. Чим займається напрям «цифрової криміналістики» «eDiscovery»? 19. Для яких потреб (напрямків) цивільного життя найчастіше залучається інструментарій (можливості) цифрової криміналістики? 20. Яка роль і можливості цифрової 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 цифрової 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. 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 «цифрової криміналістики»? 53. Якими термінами НЕ позначається «комп'ютерна криміналістика» як наука та практична сфера діяльності? 54. Що є предметом вивчення (дослідження) «цифрової криміналістики»? 55. Виберіть правильні твердження щодо співвідношення цифрової 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 цифрової криміналістики. 59. Виберіть правильні твердження щодо «eDiscovery» як напряму цифрової криміналістики. 60. Для яких потреб (напрямків) цивільного життя може залучатися інструментарій (можливості) цифрової 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 цифрову 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 об’єктом дослідження для цифрової 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. Кіберінцидент – це? 82. Кіберпростір відповідно до українського законодавства – це? 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/кіберінцидентами. 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/кіберінцидентів. 110. Виберіть твердження, які правильно характеризують знаряддя вчинення кіберзлочинів. 111. Виберіть твердження, які правильно характеризують предмет посягання кіберзлочинів/кіберінцидентів. 112. Виберіть твердження, які правильно характеризують місце вчинення кіберзлочинів/кіберінцидентів. 113. Виберіть твердження, які правильно характеризують особу кіберзлочинця. 114. Виберіть твердження, які правильно характеризують особу потерпілого від кіберзлочину/кіберінциденту. 115. Виберіть твердження, які правильно характеризують типову слідову картину кіберзлочинів/кіберінцидентів. 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/кіберінцидентів? 119. Який алгоритм дій слідчого під час огляду місця події кіберзлочину/кіберінциденту, якщо під час такого огляду комп'ютера, який має з'єднання із мережею, виникли підозри у використанні хмарних сервісів? 120. Який алгоритм дій слідчого після завершення вилучення енергозалежних і тимчасових даних в ході огляду місця події кіберзлочину/кіберінциденту? 121. Які відомості підлягають фіксації у протоколі огляду місця події кіберзлочину/кіберінциденту? 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 підпадають під ознаки домашнього насильства в кіберпросторі? 139. За яких умов видавання однієї особи за іншу в кіберпросторі 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 після завершення курсу.

Схема курсу

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література**	**Завдання, год.**	**Термін виконання**
1	**Тема 1:** Цифрові (електронні) сліди та докази.	лекція, самостійна робота	[1-10]	2 10	1 тиждень
	Тема 1: Цифрові (електронні) сліди та докази.	лабораторне заняття	[1-10]	2	
2-3	**Тема 2:** Способи збирання цифрових доказів під час розслідування кіберзлочинів та інших інцидентів.	лекція, самостійна робота	[1-10]	4 12	2 тижні
	Тема 2: Способи збирання цифрових доказів під час розслідування кіберзлочинів та інших інцидентів.	лабораторне заняття	[1-10]	4	
4	**Тема 3:** E-Discovery та використання цифрових технологій під час	лекція, самостійна	[1-10]	2 11	1 тиждень

	розслідування кіберзлочинів та інших інцидентів.	робота			
	Тема 3: E-Discovery та використання цифрових технологій під час розслідування кіберзлочинів та інших інцидентів.	лабораторне заняття	[1-10]	2	
5-6	**Тема 4.** Особливості розслідування окремих категорій кіберзлочинів.	лекція, самостійна робота	[1-10]	6 18	2 тижні
	Тема 4. Особливості розслідування окремих категорій кіберзлочинів.	лабораторне заняття	[1-10]	4	
7	**Тема 5.** Розслідування інших видів кіберінцидентів та їх запобігання.	лекція, самостійна робота	[1-10]	2 7	1 тиждень
	Тема 5. Розслідування інших видів кіберінцидентів та їх запобігання.	лабораторне заняття	[1-10]	2	
8	**Модуль**.	лабораторне заняття	[1-10]	2	1 тиждень
	Всього			**90**	