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

«ЗАТВЕРДЖУЮ»
Проректор
з науково-педагогічної роботи
та міжнародної співпраці
Львівського національного університету
імені Івана Франка
проф. Різник С. В.

_____

«___» _____ 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КОМП'ЮТЕРНА КРИМІНАЛІСТИКА»

Галузь знань: **12 «Інформаційні технології»**
Спеціальність: **125 «Кібербезпека»**
вибіркова навчальна дисципліна

Юридичний факультет

Львів – 2023 рік

Робоча програма навчальної дисципліни «**Комп'ютерна криміналістика**» для студентів за галуззю знань *12 інформаційні технології*, спеціальністю *125 кібербезпека* у межах освітньо-професійної програми ОС бакалавр, 2023. 20 с.

Розробник:
Калужна Оксана Михайлівна, кандидат юридичних наук, доцент, доцент кафедри кримінального процесу і криміналістики

Робоча програма затверджена на засіданні кафедри кримінального процесу і криміналістики юридичного факультету Львівського національного університету імені Івана Франка (Протокол від «29» серпня 2023 року № 1)

Завідувач кафедри
кримінального процесу і криміналістики _____ Н. Р. Бобечко
«29» серпня 2023 року

Схвалено Вченою Радою юридичного факультету Львівського національного університету імені Івана Франка. Протокол від «30» серпня 2023 року № 1.

«30» серпня 2023 року Голова _____ проф. В. М. Бурдін

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>Денна форма навчання</th><th>Заочна форма навчання</th></tr>
<tr><td rowspan="3">Кількість кредитів – 4</td><td rowspan="3">Галузь знань 12 «Інформаційні технології»</td><td colspan="2">Вибіркова навчальна дисципліна</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="4">Спеціальність 125 «Кібербезпека»</td><td>4</td><td>–</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td>–</td></tr>
<tr><td colspan="2">Лекцій</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: аудиторних – 3 Самостійної роботи студента – 4,5</td><td rowspan="10">Освітньо-професійна програма ОС Бакалавр</td><td>16</td><td>–</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>72</td><td>–</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить для денної форми навчання – 2:3.

Мова навчання: українська

2. МЕТА І ЗАВДАННЯ ДИСЦИПЛІНИ

Предмет. Комп’ютерна (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. Розвиток технологій ускладнює ситуацію: соціальні мережі, мобільні пристрої та Інтернет використовуються для вчинення злочинів багатьма

досі невідомими способами. За цих умов комп’ютерна криміналістична експертиза дуже потрібна, а фахівців з сучасними знаннями не вистачає.

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, 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 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 цифрових злочинів та порушень безпеки, ознайомляться як збирати цифрові докази, досліджувати й аналізувати цифрову інформацію з метою відтворити хронологію вчинення кіберзлочину чи іншого кіберінциденту, як забезпечити управління та успішне функціонування підприємства, установи, організації.

Після успішного завершення курсу від студентів очікується розуміння інформаційної безпеки, 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, тому що результати цифрового полювання мають вистояти в суді як докази.

У результаті вивчення курсу випускник буде ***знати***:

- як виглядає (в чому полягає) робота цифрового криміналіста;
- характеристику злочинності, що вчиняється в мережі Інтернет та програми (методи, алгоритми) їх розслідування;
- криміналістичний аналіз транспортних 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 належно документально оформляти цифрові докази, в тому числі використання та володіння комп’ютерними програмами, іграми та мультимедійним контентом,

- як реагувати на інциденти (розпізнати кібератаку та сповістити правоохоронні органи);

вміти:

- використовувати технологічні інновації в процесі збору доказів;
- розпізнавати порушення безпеки та належним чином реагувати на інциденти;
- документувати та процесуально оформляти допустимості е-докази;
- забезпечити визнання отриманих доказів у суді;
- аналізувати вміст комп'ютерів та ІТ-систем з можливістю пошуку 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.

Необхідні попередні та супутні навчальні дисципліни: «Основи алгоритмізації та програмування», «Комп'ютерні мережі», «Комплексні системи захисту інформації».

3. КАР'ЄРНІ МОЖЛИВОСТІ

Кар'єрні перспективи. Випускники курсу можуть знайти себе як кваліфіковані кадри в галузі інформаційної безпеки в органах державної влади та місцевого самоврядування, на підприємствах, установах, організаціях незалежно від форми власності. Вони можуть також працевлаштуватися в органах досудового розслідування на посади детективів чи оперативно-технічних працівників, які безпосередньо розслідують кібер-злочини – у Національній поліції, а також у всіх інших органах досудового розслідування (ДБР, НАБУ, СБУ, БЕБ), яким доводиться збирати електронні докази під час розслідування будь-яких інших різновидів злочинів, що залишили сліди їх готування, вчинення чи приховування в Інтернеті та на інших носіях цифрової інформації. Деякі органи досудового розслідування (ОДР) щороку вилучають сотні комп'ютерів та іншої техніки, проте для їх огляду є лише кілька технічних спеціалістів. Випускники курсу можуть також стати співробітниками спеціалізованих державних та приватних охоронних фірм, судово-експертних установ, детективних агенцій, спеціалістами з ІТ в апараті суду, консультантами адвокатських бюро і компаній. Випускники можуть стати розробниками спеціалізованого програмного забезпечення для криміналістики, судових експертиз, ІТ-безпеки, біометрики. Цей курс також може використовуватися як доповнення (підвищення) кваліфікації для кар'єри у юридичних професіях у сфері кримінального судочинства. Його цільовою аудиторією можуть бути й журналісти-розслідувачі та ІТ-аналітики.

У світі не вистачає експертів у складному середовищі кіберзлочинності. Кількість інцидентів із безпекою щоразу досягає рекордних рівнів і продовжуватиме зростати із збільшенням оцифрування та створення мереж у всіх сферах життя. Це означає, що потреба у спеціалістах залишається високою, і перспективи кар'єрного зростання у випускників надзвичайно позитивні.

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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 та електронних доказів. Вимоги до оформлення цифрових доказів для набуття ними статусу судового доказу.

Види електронних (цифрових) доказів.

Тема 2: **Використання цифрових технологій та збір цифрових доказів під час досудового розслідування та судового розгляду**

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, відеозаписів 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 метаданими.

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.

Відеокриміналістика. 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 3: **Судова комп'ютерно-технічна експертиза**

Комп'ютерно-технічна експертиза під час розслідування кіберзлочинів, в т.ч. шахрайства в системах інтернет-банкінгу.

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 судово-комп'ютерної експертизи для виявлення і реагування на інциденти інформаційної безпеки, вилучення та дослідження інформації з цифрових пристроїв. Судово-експертні методики.

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 4. **Розслідування кіберзлочинів**

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

Виявлення ботоферм та злочини, що вчиняються за їх посередництва.

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, 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.

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.

5. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	ср		л	п	лаб	інд	ср
1	2	3	4	5	6	7	8	9	10	11	12	13
ТЕМА 1. Цифрові (електронні) сліди та докази	20	2		6		12						
ТЕМА 2. Використання цифрових технологій та збір цифрових доказів під час досудового розслідування та судового розгляду	30	4		8		18						
ТЕМА 3. Судова комп'ютерно-	20	2		6		12						

технічна експертиза												
ТЕМА 4. Розслідування кіберзлочинів	34	6		8		20						
ТЕМА 5. Кібербезпека	16	2		4		10						
Усього годин	120	16		32		72						

6. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	Цифрові (електронні) сліди та докази	6
2	Використання цифрових технологій та збір цифрових доказів під час досудового розслідування та судового розгляду	8
3	Судова комп'ютерно-технічна експертиза	6
4	Розслідування кіберзлочинів	8
5	Кібербезпека	4

7. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1	Цифрові (електронні) сліди та докази	12
2	Використання цифрових технологій та збір цифрових доказів під час досудового розслідування та судового розгляду	18
3	Судова комп'ютерно-технічна експертиза	12
4	Розслідування кіберзлочинів	20
5	Кібербезпека	10

8. МЕТОДИ НАВЧАННЯ

Серед методів навчання, зокрема, підлягають застосуванню такі: загальнонаукові і спеціальні методи пізнання правових явищ: логічний, проблемний, дослідницький, евристичний, ситуаційний, метод Сократа, групова дискусія, опрацювання аналітичних завдань, підготовка експертних висновків із проблемних питань, ділові/рольові ігри; кейс-стаді, дебати, виконання наукових робіт, практика з майбутньої професії, самостійна робота з літературою, Інтернет-ресурсами (самонавчання); методики з правової оцінки поведінки чи

діяльності індивідів і соціальних груп, ідентифікація (розпізнавання) проблеми та її вирішення.

До освітніх технологій належать: інформаційно-комунікативні технології, аудіовізуальні технології, інтерактивні та мережеві технології, контекстного навчання, ситуативного моделювання, проектні технології, навчання як дослідження, модульно-блокового навчання.

9. МЕТОДИ КОНТРОЛЮ

Знання та навички студентів, отримані при засвоєнні навчальної дисципліни «Цифрова криміналістика», оцінюються за рейтинговою системою.

Форми поточного контролю включають: усне опитування, експрес-опитування, розв'язання практичних завдань/задач, підготовка і захист наукових робіт за ініціативою студента, peer review, захист кейсу, захист портфоліо, самооцінка студента за питаннями для самоконтролю, колоквіум.

Студент може отримати максимально 50 балів за усні відповіді або виконання контрольних робіт на практичних заняттях.

Неготовність до заняття або незадовільна відповідь (розв'язання) задачі також підлягають відповідній оцінці і студенту виставляється «0» балів. Отримані у такому разі «0» балів потребують відпрацювання та оцінка, одержана під час відпрацювання враховуються при визначенні середнього балу поточної успішності.

Формою підсумкового контролю знань та навичок по дисципліні для студентів є залік, який виставляється з урахуванням поточної успішності.

9. РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

<table>
<tr><th colspan="4">Поточне тестування та самостійна робота</th><th>Поточна успішність</th><th>Модуль</th><th>Сума</th></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td><td rowspan="2">Т. 1-4</td><td rowspan="2">Т. 1-5</td><td rowspan="3">100</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td>50</td><td>50</td></tr>
</table>

Оцінювання знань студента здійснюється за 100 бальною шкалою

Шкала оцінювання: університету, національна та ECTS

Оцінка в балах	Оцінка ECTS	Визначення	Екзаменаційна оцінка
90-100	A	відмінно	відмінно
81-89	B	дуже добре	добре
71-80	C	добре	
61-70	D	задовільно	задовільно
51-60	E	достатньо	

до 51	FX	незадовільно з правом перездачі	незадовільно
до 51	F	незадовільно без права перездачі	

90-100 балів (відмінно) – виставляється студенту, який дав повну і правильну відповідь на всі питання, що базуються на знанні технічних аспектів питань, нормативно-правових актів, судової практики та спеціальної літератури. Прояви уміння застосування набуті знання до конкретних ситуацій дослідження цифрової інформації та здібності аналізу джерел вивчення даного курсу.

81-89 балів (дуже добре) – виставляється студенту, який дав не цілком повну але правильну відповідь на всі питання, що базується на знанні предмету.

71-80 балів (добре) – виставляється студенту, який дав повну і правильну відповідь, але не на всі питання, або відповідь не базується на всіх складових джерелах вивчення. Тобто знав технічні аспекти питання, нормативно-правовий акт та судову практику але не знав інформації, що міститься у спеціальній літературі, чи інформації, яка міститься у інших джерелах. Однак у підсумку його відповідь повинна базуватись не менше ніж на двох базових джерелах.

61-70 балів (задовільно) – виставляється студенту, який не дав вичерпної детальної відповіді на питання контрольних завдань і яка базується тільки на одному із рекомендованих джерел вивчення матеріалу.

51-60 балів (достатньо) – виставляється студенту, який не дав вичерпної (достатньої) відповіді на питання контрольних завдань та не може назвати джерела інформації навчальної дисципліни.

0-50 балів (незадовільно) – виставляється студентові, який виявив значні прогалини в знаннях основного навчального матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань, незнайомий з основною літературою з дисципліни.

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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: 01.09.2023).
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: 01.09.2023).
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: 01.09.2023).

4. Алєксєєва-Працюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права.* 2018. № 2. С. 247–253.
5. Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні. *Міжнародний науковий журнал «Інтернаука».* 2020. № 10. С. 78–87.
6. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету.* 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: 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.naiau.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» І «NTFS». *Криміналістичний вісник*. 2014. № 1(21). С. 177–181. URL: http://elar.naiau.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-prakticnoi_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-prakticnoi-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. 20 с. URL: 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). С. 251–257. URL: 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. Дєгтярьова 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. URL: 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. Книш М. Як розвалюють комп'ютерно-технічні експертизи? *Юридична газета online*. 2019. № 45–46. С. 699–700.
34. Кобець М. В. Дії слідчого під час виявлення на місці події мобільних терміналів (стільникових радіотелефонів). *Криміналістичний вісник.* 2023. № 1(39). С.52–63.
35. 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.
36. 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.
37. Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України: дис. … канд. юрид. наук: 12.00.09. Київ, 2021. 258 с.
38. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 8. С. 418–421.
39. 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.
40. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–305.
41. Крицька І. О. Речові докази у кримінальному провадженні: дис. ... канд. юрид. наук: 12.00.09. Харків, 2017. 249 с.
42. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльно-аналітичне право. 2013. № 3–2. С. 313–315.
43. 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.
44. Кравчук, О. «Обшук» мобільних телефонів і комп'ютерів та інші зміни до КПК. *Судебно-юридическая газета*. 25 (2022).
45. 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.
46. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства.* 2019. № 3. С. 224–238.
47. 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.
48. Нізовцев Ю. Ю., Омельян О. С. Щодо підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов'язаних із кібератакими. *Криміналістичний вісник*. 2021. № 2 (36). С. 59–68. DOI: 10.37025/1992-4437/2021-36-2-59.
49. 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.
50. 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
51. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право.* 2020. № 6. С. 243–247.

52. 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
53. 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
54. Ресурси з форензики (практика розслідування кіберзлочинів) URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344671.php
55. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. 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
56. Сіренко О.В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. № 14. С. 208–214.
57. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дис. … д-ра філос. наук: 12.00.09. Харків, 2021. 369 с.
58. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с. https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=4651&download_id=1537
59. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. № 146. С. 179-191. https://www.ceeol.com/search/article-detail?id=796280
60. 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.
61. 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.
62. 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.

63. 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.
64. 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.naiau.kiev.ua/bitstream/123456789/23343/1/%d0%ae%d1%80%d0%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
65. Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2019. № 1. С. 13–19.
66. 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.
67. Школьніков В. І. Правова основа отримання інформації з мережі інтернет у кримінальному провадженні. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. № 4. С. 172–176.
68. 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.
69. Що таке комп’ютерна криміналістика (форензіка)? *GROSS digital forensics Lab.* 2017. URL: https://g-ross.com.ua/novyny/kompyuterna-kryminalistyka-forenzika.html
70. Що таке цифрова криміналістика*? GROSS digital forensics Lab.* 2018. URL: https://g-ross.com.ua/novyny/cyfrova-kryminalistyka-2.html
71. 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
72. 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
73. Anderson, P., Sampson, D., & Gilroy, S. (2021). *Digital investigations: relevance and confidence in disclosure*. ERA Forum, 22 (4). 587-599. ISSN 1612-3093.
74. Android research and analysis tool Andr Ex R. *AOS company*. URL: https://www.fss.jp/android_andrex_r/
75. AOS Image Analysis Forensics Professional. *AOS company*. URL: https://www.fss.jp/fss_movie01-2/
76. Årnes, A. (2018). *Digital forensics*. Hoboken, NJ: John Wiley & Sons Inc.
77. Bodo Meseke. Digitale Forensik. Praxiswissen Cybercrime für Manager. Berlin. 2019. https://www.weltbild.de/artikel/ebook/digitale-forensik_34575890-1?ln=UHJvZHVrdHxNZWhyIELDvGNoZXIgZGVzIEF1dG9ycw==

78. Britz, M. (2013). Computer Forensics and Cyber Crime: An Introduction. Pearson.
79. 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
80. Carlton, A. (2020). Sextortion: the hybrid cyber-sex crime. *North Carolina Journal of Law & Technology*, 21(3), 177-216.
81. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Cham: Springer International Publishing.
82. Chen, L., Takabi, H., & Le-Khac, N.-A. (2019). *Security, privacy and digital forensics in the cloud*. Hoboken, NJ: John Wiley & Sons.
83. *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
84. Dalrymple, B. E., & Smith, E. J. (2018). *Forensic Digital Image Processing: Optimization of Impression Evidence*. Boca Raton, FL: CRC Press.
85. 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
86. Digitale Forensik/IT Forensik – berufsbegleitender Online-Fernstudiengang. URL: http://www.master-digitale-forensik.de/
87. EC-Council Press. (2010). *Computer forensics*. Clifton Park, NY: Course Technology.
88. 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.
89. 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
90. Hassan, N. A. (2019). *Digital forensics basics: A practical guide using Windows OS*. New York: Apress.
91. Hayes, D. R., & Walczak, T. (2021). *Informatyka w kryminalistyce: Praktyczny przewodnik*. Gliwice: Helion.
92. Ho, A. T. S., & Li, S. (2015). *Handbook of digital forensics of multimedia data and devices*. Chichester: Wiley.
93. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. London: Routledge, Taylor & Francis Group.
94. 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
95. Kasprzak, W. A. (2015). *Ślady cyfrowe: Studium prawno-kryminalistyczne*. Warszawa: Difin.
96. Kävrestad, J. (2017). *Guide to Digital Forensics: A Concise and Practical Introduction*. Cham: Springer International Publishing.

97. Kävrestad, J. (2018). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. Cham: Springer International Publishing.
98. Kleiman, D. (2007). *The official CHFI study guide (Exam 312-49): For computer hacking forensic investigator*. Syngress.
99. 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
100. Labudde, D., & Spranger, M. (2017). *Forensik in der digitalen Welt*. Berlin, Heidelberg: Springer Berlin Heidelberg.
101. Latysh, K. K. (2021). Criminalistics Analysis of Cyber Tools for Committing Crimes. *Problems of Legality*, 153, 165-172.
102. 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
103. Leroux, O. (2004). Legal admissibility of electronic evidence, International Review of Law, Computers & Technology, 18:2, 193-220. 10.1080/1360086042000223508
104. Lewulis, P. (2021). *Dowody cyfrowe: Teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.
105. Lin, X. (2018). *Introductory Computer Forensics: A Hands-on Practical Approach*. Cham: Springer International Publishing.
106. Luttgens, J., Mandia, K., & Pepe, M. (2014). *Incident Response & Computer Forensics, Third Edition*. McGraw-Hill.
107. Maras, M.-H. (2015). *Computer forensics: Cybercriminals, laws, and evidence*. Burlington, MA: Jones & Bartlett Learning.
108. 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).
109. Pandelica, I. (2020). The phenomenon of cyber crime. International Journal of Information Security and Cybercrime, 9(1), 29-36.
110. 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.
111. Paweł Olbe. Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych. Wydawnictwo: Wyższa Szkoła Policji w Szczytnie. 2021. 412 S.
112. Philipp, A., Cowen, D., Davis, C. M., & Scharringhausen, L. S. (2010). *Hacking exposed computer forensics*. New York: McGraw-Hill.
113. Phillips, A., Nelson, B., & Steuart, C. (2019). *Guide to computer forensics and investigations: Processing digital evidence*. Boston: Cengage Learning.
114. 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
115. Popular Computer Forensics Top 21 Tools [Updated for 2019]. *Infosec*. 2019. URL: https://resources.infosecinstitute.com/computer-forensics-tools/#gref
116. Prasad, Ajay & Pandey, Jeetendra. (2016). *Digital Forensics*. Uttrakhand Open University.
117. Quan, W. (2019). Cyber economic crimes: challenges and countermeasures of the Chinese police. *China Legal Science*, 7(3), 67-94.
118. 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
119. 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
120. Sachowski, J. (2016). *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*. Elsevier Science.
121. Sachowski, J. (2018). *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*. London: Taylor and Francis.
122. Sammons, J. (2012). *The basics of digital forensics: The primer for getting started in digital forensics*. Syngress.
123. Sammons, J. (2016). *Digital forensics: Threatscape and best practices*. Amsterdam: Syngress.
124. Shavers, B. (2013). *Placing the suspect behind the keyboard: Using digital forensics and investigative techniques to identify cybercrime suspects*. Waltham, MA: Syngress.
125. Sunde, N. (2022). *Unpacking the evidence elasticity of digital traces,* Cogent. Social Sciences, 8:1, 2103946, DOI: 10.1080/23311886.2022.2103946
126. TrapX Security DeceptionGrid 6.3. *SC Media magazine*. 14 August 2019. URL: https://www.scmagazine.com/review/trapx-security-deceptiongrid-6-3/
127. 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.
128. Volonino, L., & Anzaldua, R. (2008). *Computer forensics for dummies*. Hoboken, NJ: Wiley.
129. Widup, S. (2014). *Computer forensics and digital investigation with Encase Forensic v7*. New York: McGraw-Hill Education.
130. 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