МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Відділення інформаційних технологій
Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора
з навчальної роботи
29 серпня 2025 р.
Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Розслідування інцидентів кіберзлочинів	
галузь знань	*12 Інформаційні технології*
спеціальність	*125 Кібербезпека та захист інформації*
освітня програма	*Кібербезпека та захист інформації*

Рівне – 2025 рік

Програма навчальної дисципліни з *РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КІБЕРЗЛОЧИНІВ* розроблено на основі освітньо-професійної програми *Кібербезпека та захист інформації* для здобувачів освіти освітньо-професійного ступеня "Фаховий молодший бакалавр" галузі знань 12 Інформаційні технології, спеціальності *125 Кібербезпека та захист інформації, затвердженої Вченою радою НУБіП України протокол від 26.04.2023 №10*

Розробники: *Янок Назар Сергійович, викладач програмування та інформаційних дисциплін;*

Програму навчальної дисципліни розглянуто і схвалено на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від «29» серпня 2025 року № 1

Голова циклової комісії *програмування та інформаційних дисциплін*

«29» серпня 2025 року _____ *Павло СТРИК*

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від «29» *серпня* 2025 року № 1

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень	
Освітньо-професійний ступінь	*фаховий молодший бакалавр*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Характеристика навчальної дисципліни	
Вид	обов'язкова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	4
Мова викладання, навчання та оцінювання	українська
Форма контролю	екзамен
Показники навчальної дисципліни для денної та заочної форм навчання	
Форма навчання	денна
Рік підготовки	2025-2026
Семестр	6
Аудиторні години:	64
Лекційні	34
Практичні	30
Самостійна робота	26
Підготовка до екзамену	30
Кількість тижневих годин для денної форми навчання	4

МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни полягає в поглибленні теоретичної і практичної підготовки фахівця, спрямованої на вирішення типових та складних завдань цифрової криміналістики, що полягають у зборі цифрової криміналістичної інформації, збереженні, дослідженні і використанні цифрових доказів.

Завдання навчальної дисципліни:

- ознайомлення з основними поняттями кіберзлочинності та цифрової криміналістики;
- вивчення методів та інструментів цифрових розслідувань, що застосовуються у кіберзлочинах;
- розгляд класифікації кіберзлочинів та основних способів їхнього вчинення;
- освоєння методології збору, аналізу та збереження цифрових доказів;
- вивчення принципів роботи з цифровими доказами та їхньої правової значущості;
- навчання проведенню експертизи даних, відновленню видаленої інформації та аналізу цифрових слідів;
- дослідження способів приховування цифрових слідів та методів антикриміналістики;
- аналіз методів розслідування атак на комп'ютерні системи та мережі;
- ознайомлення з особливостями аналізу мобільних пристроїв у кіберрозслідуваннях;
- опрацювання методів виявлення та протидії стеганографії й шифруванню;
- вивчення методів атрибуції кіберзлочинців та аналізу цифрового місця злочину;
- засвоєння принципів експертної оцінки цифрових доказів та складання звітів;
- розгляд автоматизованих систем аналізу кіберзлочинів та їхніх можливостей.

вміти:

- визначати основні види кіберзлочинів та їхні характеристики;
- застосовувати методи збору, аналізу та збереження цифрових доказів;
- працювати з програмними та апаратними засобами цифрової криміналістики;
- аналізувати файлові системи, дискові структури та процеси завантаження операційних систем;
- відновлювати видалені дані та перевіряти їхню цілісність за допомогою хеш-функцій;
- проводити розслідування мережевих атак та аналізувати трафік;

- здійснювати криміналістичний аналіз мобільних пристроїв та хмарних сервісів;
- виявляти приховані та зашифровані дані, застосовувати методи стеганоаналізу;
- використовувати інструменти цифрової криміналістики для аналізу логів, реєстрів та метаданих;
- ідентифікувати способи уникнення цифрового сліду та протидіяти антикриміналістиці;
- проводити експертну оцінку цифрових доказів та складати висновки;
- використовувати моделі розслідування кіберзлочинів та планувати аналітичні розслідування.

Очікувані результати навчання.

Після вивчення дисципліни «Розслідування інцидентів кіберзлочинів» у здобувачів освіти формуються такі **компетентності:**

Загальні (ЗК):

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК02. Знання та розуміння предметної області та професії.

ЗК04. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК05. Здатність здійснювати пошук, оброблення та аналіз інформації.

Спеціальні (ФК):

ФК08. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК12. Здатність виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційного простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки

Програмні результати навчання (ПР):

ПР01. Знати законодавчу та нормативно-правову базу України та вимоги відповіднихстандартів, у тому числі міжнародних в галузі інформаційної безпеки та\або кібербезпеки.

ПР02. Знати національні та міжнародні стандарти, регулюючі акти виявлення, ідентифікації, аналізу та реагування на інциденти в сфері інформаційної безпеки та/ або кібербезпеки.

ПР10. Знати теорію та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПР11. Вміти впроваджувати заходи щодо попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем згідно зі встановленою політикою інформаційної безпеки та\або кібербезпеки.

ПР12. Вміти впроваджувати заходи щодо попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем згідно зі встановленою політикою інформаційної безпеки та/ або кібербезпеки.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1: Основи кіберрозслідувань

Тема 1. Вступ до розслідування кіберзлочинів

Визначення та основи кіберзлочинності. Роль цифрової криміналістики у розслідуванні кіберзлочинів. Наука про розслідування кіберзлочинів. Основні методи та підходи до кіберрозслідувань. Спільноти та організації у сфері кіберрозслідувань. Медіавплив та міфи щодо кіберзлочинності.

Тема 2. Основні поняття та методи кіберрозслідувань

Цифрові докази: визначення, властивості, юридична значущість. Волатильність даних: RAM, процеси, мережевий трафік. Порядок збору доказів за принципом Order of Volatility. Основні заходи розслідування кіберзлочинів: ідентифікація інциденту, збір доказів, аналіз, звітність. Кіберзлочини в різних контекстах: державний сектор, бізнес, приватне життя. Доказова база: типи цифрових доказів, стандарти доказування. Chain of custody (ланцюжок зберігання доказів): документування, захист від фальсифікації. Роль наукового підходу: повторюваність, верифікація, експертна оцінка. Класифікація кіберзлочинів за об'єктом атаки, мотивацією, технічною складністю.

Тема 3. Правові аспекти та процедури кіберрозслідувань

Законодавство України у сфері кіберзлочинів: Кримінальний кодекс (статті 361-363-1), Закон "Про основні засади забезпечення кібербезпеки України". Міжнародні правові акти: Будапештська конвенція, директиви ЄС. Повноваження правоохоронних органів у кіберпросторі. Процедури отримання санкцій на проведення обшуків та вилучення. Правила роботи з цифровими доказами. Chain of custody: юридичні вимоги, документування кожного етапу. Судова експертиза: призначення, проведення, експертний висновок. Права підозрюваних та свідків у кіберрозслідуваннях. Міжнародне співробітництво: запити на правову допомогу (MLA), екстрадиція. Конфіденційність та захист персональних даних під час розслідування.

Змістовий модуль 2: Комп'ютерна криміналістика

Тема 4. Основи комп'ютерної криміналістики

Типи накопичувачів даних: HDD (жорсткі диски), SSD (твердотільні накопичувачі), USB flash, SD-карти, оптичні диски. Принципи роботи HDD: магнітний запис, головки читання/запису, сектори, треки, циліндри. Принципи роботи SSD: NAND flash memory, контролери, wear leveling, TRIM. Різниця між HDD та SSD у контексті цифрової криміналістики: відновлення даних, видалення. Логічна структура жорстких дисків: сектори (sectors), кластери (clusters), блоки. Фізична структура: поверхні, доріжки, циліндри. Методи адресації: CHS

(Cylinder-Head-Sector), LBA (Logical Block Addressing). Розбиття дисків: MBR (Master Boot Record), GPT (GUID Partition Table). Файлові системи: FAT32, NTFS, exFAT, ext3/ext4, HFS+, APFS. Структура файлових систем: boot sector, FAT, MFT (Master File Table), журналювання. Slack space та unallocated space: приховані дані.

Тема 5. Процеси завантаження та низькорівневий аналіз

Процес завантаження ОС Windows. Процес завантаження Linux. Процес завантаження macOS. Legacy BIOS vs UEFI: порівняння, переваги UEFI. Secure Boot: верифікація підписів завантажувачів. Аналіз маніпуляцій із завантажувачем: bootkit-атаки, підміна завантажувачів. Приховані розділи диска: system reserved, EFI System Partition, recovery partitions. Маніпуляції з розділами: приховування даних, створення прихованих розділів. DCO (Device Configuration Overlay): приховування областей диска від ОС. HPA (Host Protected Area): зарезервовані області диска. Використання DCO/HPA у кіберзлочинах: приховування malware, даних. Методи виявлення прихованих областей: низькорівневі утиліти, hex-аналіз.

Тема 6. Цифрові докази: типи, збір та аналіз

Класифікація цифрових доказів: докази на локальних пристроях, мережеві докази, хмарні докази, докази з IoT. Місця зберігання доказів: комп'ютери, сервери, мобільні пристрої, зовнішні накопичувачі, хмарні сховища (cloud storage), соціальні мережі, месенджери. Аналіз логів: системні логи (Windows Event Logs, syslog), логи додатків, логи безпеки (firewall, IDS/IPS). Аналіз історії браузера: історія відвідувань, cookies, кеш, автозаповнення форм, збережені паролі. Докази у соціальних мережах: пости, повідомлення, друзі/підписники, лайки, чек-іни. Докази у месенджерах: чати, файли, історія дзвінків (WhatsApp, Telegram, Viber, Signal). EXIF-метадані: дата створення, модель камери, GPS-координати, налаштування зйомки. Використання EXIF у розслідуваннях: встановлення місця та часу. Геолокація: GPS-дані, Wi-Fi позиціонування, cell tower triangulation. Відстеження переміщень: timeline analysis, correlation з іншими доказами.

Змістовий модуль 3: Технічні методи розслідування

Тема 7. Методологія збору доказів на місці події

Принцип обміну Локарда (Locard's Exchange Principle) у цифровому середовищі. Основи роботи на місці кіберзлочину: first responder, crime scene investigation. Фіксація цифрових доказів: фотографування, відеозйомка, документування конфігурації. Документування місця події: схеми, описи, протоколи. Захист цифрових доказів від фальсифікації: контроль доступу, опечатування. Набори для кіберрозслідувань (forensic kits): апаратні та програмні компоненти. Вилучення доказів: живі системи vs вимкнені системи. Live forensics: збір volatile даних (RAM, процеси, мережеві з'єднання). Dead forensics: аналіз вимкнених систем. Порядок дій при вилученні: RAM dump → мережеві з'єднання

→ системна інформація → вимикання/вилучення. Аналіз комп'ютерів: системні файли, реєстр, логи, user profiles. Аналіз мобільних пристроїв: контакти, SMS, історія дзвінків, додатки. Аналіз хмарних сервісів: Google Drive, Dropbox, OneDrive, iCloud. Legal holds та збереження хмарних даних. Аналіз мережевого середовища: мережевий трафік, логи маршрутизаторів/комутаторів, DHCP logs. Моніторинг активності: packet capture, flow analysis.

Тема 8. Технічні засоби цифрової криміналістики

Програмні засоби цифрової криміналістики: EnCase, FTK (Forensic Toolkit), Autopsy, X-Ways Forensics, Sleuth Kit. Апаратні засоби: forensic workstations, write blockers, forensic duplicators. Блокувальники запису (write blockers): апаратні (Tableau, WiebeTech) та програмні (FTK Imager в режимі read-only). Призначення: запобігання зміні оригінальних доказів. Побітові копії (bit-by-bit copies, forensic images): dd, dcfldd, FTK Imager. Формати образів: raw (dd), E01 (EnCase), AFF (Advanced Forensic Format). Резервне копіювання vs forensic imaging. Хеш-функції для перевірки цілісності: MD5, SHA-1, SHA-256. Chain of custody для образів дисків. Аналіз образів дисків: монтування, пошук файлів, відновлення видалених даних. Відновлення видалених даних: file carving, аналіз unallocated space. Інструменти: Recuva, PhotoRec, Scalpel. Аналіз реєстру Windows: структура реєстру (HKEY_LOCAL_MACHINE, HKEY_USERS), важливі ключі (Run, RunOnce, UserAssist). Інструменти: Registry Explorer, RegRipper. Аналіз журналів подій Windows: Security, System, Application logs. Важливі події: logon/logoff (4624/4634), account creation, privilege escalation.

Тема 9. Мережеві кіберзлочини та їх розслідування

Основи мережевого аналізу: моделі OSI та TCP/IP. Протоколи: TCP, UDP, HTTP/HTTPS, DNS, SMTP, FTP. Методи збору мережевих доказів: packet capture (PCAP), NetFlow, logs. Розташування точок збору: network taps, SPAN ports, inline sensors. Аналіз мережевих атак: DDoS (Distributed Denial of Service), MITM (Man-in-the-Middle), SQLi (SQL Injection), XSS (Cross-Site Scripting), RCE (Remote Code Execution). Ознаки атак у мережевому трафіку. Локалізація зловмисників: аналіз IP-адрес, geolocation, whois, reverse DNS. Проблеми з NAT, проксі, VPN. Аналіз VPN-логів: connection logs, traffic logs. Обмеження: no-log VPN services. Використання TOR: onion routing, exit nodes, hidden services. Деанонімізація TOR-користувачів: correlation attacks, timing attacks. Спеціалізовані інструменти мережевого аналізу: Wireshark (packet analyzer), Zeek/Bro (network security monitor), Suricata (IDS/IPS), tcpdump, NetworkMiner. Аналіз PCAP-файлів: фільтрація, пошук артефактів, extraction файлів.

Тема 10. Розслідування кіберзлочинів на мобільних пристроях

Особливості мобільних пристроїв: Android, iOS, Windows Phone. Архітектура ОС: Android (Linux kernel, Dalvik/ART), iOS (Darwin, Cocoa Touch). Методи видобутку даних: logical extraction, file system extraction, physical extraction, chip-off, JTAG.

Logical extraction: через API ОС, резервні копії. File system extraction: повний доступ до файлової системи. Physical extraction: побітова копія пам'яті. Chip-off та JTAG: апаратні методи для пошкоджених пристроїв. Виявлення прихованих даних: deleted SMS, app data, encrypted containers. Аналіз шифрування на мобільних: Android FDE/FBE, iOS Data Protection. Обхід шифрування: brute force, exploits, vendor backdoors. Аналіз історії дзвінків: call logs, duration, timestamps. Аналіз SMS/MMS: тексти, вкладення, метадані. Аналіз GPS-координат: location history, EXIF у фото, check-ins. Геофенсинг у розслідуваннях. Аналіз додатків: WhatsApp, Telegram, Viber, Signal, social media apps. Databases: SQLite, XML, plist files. Дослідження маніпуляцій із ОС: jailbreak (iOS), root (Android). Виявлення ознак: Cydia, SuperSU, Magisk. Інструменти мобільної криміналістики: Cellebrite UFED, Oxygen Forensics, XRY, MOBILedit Forensic.

Змістовий модуль 4: Просунуті техніки та аналітика

Тема 11. Антикриміналістика та приховування слідів

Визначення антикриміналістики (anti-forensics): методи протидії цифровому розслідуванню. Категорії: data hiding, data destruction, trail obfuscation, attacks against forensic tools. Методи уникнення цифрового сліду: анонімні мережі (TOR, I2P), VPN (Virtual Private Networks), проксі-сервери. No-log VPN та проблеми атрибуції. Файлові структури та маніпуляції: стеганографія (приховування даних у зображеннях, аудіо, відео), шифрування (AES, RSA), контейнери (VeraCrypt, BitLocker). Стеганографічні інструменти: steghide, OpenStego. Виявлення стеганографії: steganalysis. Видалення даних: secure delete (overwriting), шредери файлів (Eraser, BleachBit). Багатопрохідне перезаписування: DoD 5220.22-M, Gutmann method. SSD та проблеми secure delete: TRIM, wear leveling. Альтернативні потоки даних (ADS) у NTFS: приховування файлів у ADS. Виявлення ADS: streams утиліта, forensic tools. Використання у malware. Rootkits: kernel-mode та user-mode rootkits. Приховування процесів, файлів, мережевих з'єднань. Виявлення rootkits: GMER, RootkitRevealer, memory forensics. Bootkits: модифікація завантажувачів, MBR bootkits, UEFI bootkits. Firmware malware. Приховані загрози: fileless malware (in-memory execution), living off the land (LOLBins). Виявлення: memory analysis, behavioral detection.

Тема 12. Аналітика та моделі розслідування кіберзлочинів

Моделі розслідування кіберзлочинів: IDIP (Integrated Digital Investigation Process): Readiness, Deployment, Physical Investigation, Digital Forensics, Review. EIDIP (Enhanced IDIP): додавання Traceback phase. HOBFDIP (Harmonized Digital Forensic Investigation Process): 7 фаз. Порівняння моделей: переваги, недоліки, сфери застосування. Аналіз цифрового місця злочину: crime scene analysis, reconstruction. Timeline analysis: створення хронології подій. Correlation analysis: зв'язок між різними артефактами. Атрибуція кіберзлочинців: технічна атрибуція

(IP, malware analysis, TTPs) vs юридична атрибуція. Проблеми та виклики: анонімізація, false flags, attribution uncertainty. Методи аналізу: TTPs (Tactics, Techniques, Procedures) analysis, MITRE ATT&CK mapping. Behavioral analysis: modus operandi зловмисників. Кореляція даних: link analysis, pattern recognition. Network analysis: зв'язки між IP, домени, malware samples. Автоматизовані системи аналізу: SIEM (Splunk, ELK Stack), SOAR platforms. Machine learning в цифровій криміналістиці: anomaly detection, classification. Threat intelligence: використання CTI (Cyber Threat Intelligence) у розслідуваннях. Платформи: MISP, OpenCTI, ThreatConnect.

Тема 13. Експертні висновки та звітність у кіберрозслідуваннях

Структура експертного висновку: вступна частина, дослідницька частина, висновки. Вимоги до експертних висновків: об'єктивність, повнота, науковість, зрозумілість. Мова експертного висновку: технічна vs юридична термінологія. Документування методології: інструменти, версії, налаштування. Chain of custody в звітності: хто, коли, що робив з доказами. Фіксація всіх дій експерта. Візуалізація результатів: screenshots, діаграми, таблиці, timeline charts. Додатки до висновку: логи, хеші, metadata. Судова експертиза: призначення експертизи, експертне завдання, права експерта. Процесуальні аспекти: ст. 242-245 КПК України. Допит експерта: підготовка до суду, presentation skills. Пояснення технічних аспектів нефахівцям. Етичні аспекти: об'єктивність, конфіденційність, професійна етика. Стандарти та сертифікації: ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence), ACPO (Association of Chief Police Officers) Good Practice Guide. Професійні сертифікації: EnCE (EnCase Certified Examiner), GCFA (GIAC Certified Forensic Analyst), CFCE (Certified Forensic Computer Examiner). Continuous learning: оновлення знань, нові технології, нові загрози.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назви змістових модулів і тем	Кількість годин			
		денна форма			
		всього	лекційні	практичні	самостійне вивчення
1	*2*	*3*	*4*	*5*	*6*
Змістовий модуль 1. Основи кіберрозслідувань					
Тема 1	Вступ до розслідування кіберзлочинів	8	4	2	2
Тема 2	Основні поняття та методи кіберрозслідувань	8	4	2	2
Тема 3	Правові аспекти та процедури кіберрозслідувань	6	2	2	2
Разом за змістовим модулем 1		**22**	**10**	**6**	**6**
Змістовий модуль 2. Комп'ютерна криміналістика					
Тема 4	Основи комп'ютерної криміналістики	8	4	2	2
Тема 5	Процеси завантаження та низькорівневий аналіз	8	4	2	2
Тема 6	Цифрові докази: типи, збір та аналіз	8	2	4	2
Разом за змістовим модулем 2		**24**	**10**	**8**	**6**
Змістовий модуль 3. Технічні методи розслідування					
Тема 7	Методологія збору доказів на місці події	6	2	2	2
Тема 8	Технічні засоби цифрової криміналістики	6	2	2	2
Тема 9	Мережеві кіберзлочини та їх розслідування	6	2	2	2
Тема 10	Розслідування кіберзлочинів на мобільних пристроях	6	2	2	2
Разом за змістовим модулем 3		**24**	**8**	**8**	**8**
Змістовий модуль 4. Технічні аспекти та аналітика кіберзлочинів					
Тема 11	Антикриміналістика та приховування слідів	**6**	2	2	2
Тема 12	Аналітика та моделі розслідування кіберзлочинів	6	2	2	2
Тема 13	Експертні висновки та звітність у кіберрозслідуваннях	8	2	4	2
Разом за змістовим модулем 4		**20**	**6**	**8**	**6**
Всього годин		**90**	**34**	**30**	**26**
Підготовка до екзамену		**30**			
Всього годин		**120**			

5. ТЕМИ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ заняття	Вид навчальної діяльності	Назва теми	Кількість годин
Змістовий модуль 1. Вступ до розслідування кіберзлочинів				**22**
1	**Основи кіберрозслідувань та цифрової криміналистики**			**8**
	1	лекція 1	Визначення та класифікація кіберзлочинності. Будапештська конвенція. Типи кіберзлочинів: хакерство, фішинг, ransomware, DDoS-атаки.	2
		самостійне вивчення	Вивчення статистики кіберзлочинів в Україні та світі за останній час. Аналіз резонансних кейсів кіберзлочинів.	2
	2	лекція 2	Роль цифрової криміналістики. Принципи digital forensics. Різниця між incident response та digital forensics. Методології: IDIP, EIDIP, HOBFDIP.	2
	3	практична робота 1	Аналіз реального кейсу кіберзлочину. Ідентифікація типу злочину, визначення методології розслідування.	2
2	Основні поняття та методи кіберрозслідувань			8
	4	лекція 3	Цифрові докази: визначення, властивості. Волатильність даних. Order of Volatility. Основні заходи розслідування.	2
		самостійне вивчення	Вивчення типів цифрових доказів та їх властивостей. Аналіз принципу Order of Volatility.	2
	5	лекція 4	Chain of custody: документування, захист від фальсифікації. Доказова база у кіберзлочинах. Класифікація кіберзлочинів.	2
	6	практична робота 2	Документування Chain of Custody для модельного кейсу. Складання протоколів вилучення цифрових доказів.	2
3	Правові аспекти та процедури кіберрозслідувань			**6**
	7	лекція 5	Законодавство України у сфері кіберзлочинів. Кримінальний кодекс (ст. 361-363-1). Будапештська конвенція. Повноваження правоохоронних органів. Процедури обшуків та вилучення. Судова експертиза. Міжнародне співробітництво.	2
		самостійне вивчення	Детальне вивчення статей КК України щодо кіберзлочинів (361-363-1). Аналіз Будапештської конвенції та її імплементація в Україні. Вивчення процедур отримання санкцій на обшуки. Аналіз Закону "Про основні засади забезпечення кібербезпеки України". Вивчення процедур міжнародної правової допомоги (MLA). Огляд директив ЄС щодо кіберзлочинів.	2

	8	практична робота 3	Складання процесуальних документів: клопотання про проведення обшуку, протоколу вилучення, постанови про призначення експертизи.	2
Змістовий модуль 2: Комп'ютерна криміналістика				**24**
4	**Основи комп'ютерної криміналістики**			**8**
	9	лекція 6	Типи накопичувачів: HDD, SSD, USB flash, SD-карти. Принципи роботи HDD та SSD. Різниця в контексті цифрової криміналістики.	2
		самостійне вивчення	Вивчення фізичної структури HDD: сектори, треки, циліндри. Порівняння технологій HDD vs SSD: wear leveling, TRIM. Аналіз проблем відновлення даних з SSD.	2
	10	лекція 7	Логічна та фізична структура дисків. Методи адресації: CHS, LBA. Розбиття дисків: MBR, GPT. Файлові системи: FAT32, NTFS, ext3/ext4, HFS+, APFS.	2
	11	практична робота 4	Аналіз структури диска за допомогою hex-редактора. Ідентифікація MBR/GPT, файлових систем, пошук hidden partitions.	2
5	**Процеси завантаження та низькорівневий аналіз**			**8**
	12	лекція 8	Процеси завантаження Windows, Linux, macOS. Legacy BIOS vs UEFI. Secure Boot. Аналіз маніпуляцій із завантажувачем.	2
		самостійне вивчення	Детальне вивчення етапів завантаження Windows. Порівняння GRUB та LILO в Linux. Аналіз bootkit-атак та методів їх виявлення	2
	13	лекція 9	Приховані розділи диска. DCO (Device Configuration Overlay) та HPA (Host Protected Area). Використання у кіберзлочинах. Методи виявлення.	2
	14	практична робота 5	Аналіз процесу завантаження. Виявлення прихованих розділів, DCO/HPA за допомогою спеціалізованих утиліт.	2
6	**Цифрові докази: типи, збір та аналіз**			**8**
	15	лекція 10	Класифікація цифрових доказів. Місця зберігання: локальні пристрої, хмарні сховища, соціальні мережі. Аналіз логів та історії браузера. EXIF-метадані. Геолокація.	2
		самостійне вивчення	Вивчення структури Windows Event Logs та syslog. Аналіз форматів історії браузерів (Chrome, Firefox, Safari, Edge). Дослідження структури cookies та кешу. Вивчення EXIF-метаданих: типи, структура, інструменти аналізу. Аналіз GPS-даних та методів геолокації (Wi-Fi, cell towers).	2

			Вивчення структури даних WhatsApp, Telegram, Viber.	
	16	практична робота 6	Аналіз браузерної активності: видобуток історії, cookies, автозаповнення. Аналіз EXIF-метаданих фото.	2
	17	практична робота 7	Аналіз даних із соціальних мереж та месенджерів. Timeline analysis. Кореляція геолокації з іншими доказами.	2
Змістовий модуль 3: Технічні методи розслідування				**24**
7	**Методологія збору доказів на місці події**			**6**
	18	лекція 11	Принцип обміну Локарда. Робота на місці кіберзлочину. Фіксація та документування. Live forensics vs Dead forensics. Порядок вилучення доказів. Аналіз комп'ютерів, мобільних, хмарних сервісів.	2
		самостійне вивчення	Вивчення принципу Локарда в цифровому контексті. Аналіз процедур first responder. Вивчення методів RAM dump та аналізу volatile даних. Дослідження legal holds для хмарних сервісів.	2
	19	практична робота 8	RAM dump та аналіз volatile даних. Створення forensic image диска. Верифікація хешами.	2
8	**Технічні засоби цифрової криміналістики**			**6**
	20	лекція 12	Програмні засоби: EnCase, FTK, Autopsy, X-Ways. Апаратні засоби: write blockers, forensic duplicators. Побітові копії та формати образів. Хеш-функції. Відновлення видалених даних. Аналіз реєстру Windows та Event Logs.	2
		самостійне вивчення	Порівняльний аналіз EnCase, FTK, Autopsy, X-Ways Forensics. Вивчення форматів образів: raw (dd), E01, AFF. Дослідження методів file carving. Детальне вивчення структури реєстру Windows.	2
	21	практична робота 9	Створення forensic image за допомогою FTK Imager. Верифікація хешами. Монтування та аналіз образу. Відновлення видалених файлів	2
9	**Мережеві кіберзлочини та їх розслідування**			**6**
	22	лекція 13	Основи мережевого аналізу. Методи збору мережевих доказів: PCAP, NetFlow. Аналіз атак: DDoS, MITM, SQLi, XSS. Локалізація зловмисників: IP, VPN, TOR. Інструменти: Wireshark, Zeek, Suricata.	2
		самостійне вивчення	Вивчення моделей OSI та TCP/IP в контексті forensics. Аналіз ознак мережевих атак у трафіку. Дослідження методів деанонімізації TOR-користувачів. Вивчення можливостей Wireshark для forensics.	2

	23	практична робота 10	Аналіз PCAP-файлів за допомогою Wireshark. Ідентифікація типу атаки. Extraction файлів з трафіку. Локалізація джерела атаки.	2
10	**Розслідування кіберзлочинів на мобільних пристроях**			**6**
	24	лекція 14	Особливості мобільних пристроїв: Android, iOS. Методи видобутку: logical, file system, physical extraction, chip-off, JTAG. Аналіз даних: дзвінки, SMS, GPS, додатки. Виявлення jailbreak/root. Інструменти: Cellebrite, Oxygen Forensics, XRY.	2
		самостійне вивчення	Порівняння архітектури Android та iOS. Вивчення методів обходу шифрування мобільних пристроїв. Аналіз структури баз даних WhatsApp, Telegram, Viber. Дослідження інструментів Cellebrite UFED, Oxygen Forensics.	2
	25	практична робота 11	Видобуток даних із Android-пристрою (logical extraction). Аналіз SMS, дзвінків, контактів. Extraction даних із месенджерів. Timeline analysis.	2
Змістовий модуль 4: Технічні методи розслідування				**20**
11	**Антикриміналістика та приховування слідів**			**6**
	26	лекція 15	Визначення anti-forensics. Методи уникнення сліду: TOR, VPN, проксі. Стеганографія та шифрування. Видалення даних: secure delete, overwriting. ADS у NTFS. Rootkits та bootkits. Fileless malware.	2
		самостійне вивчення	Детальне вивчення TOR та методів деанонімізації. Аналіз стеганографічних інструментів: steghide, OpenStego. Вивчення методів secure delete: DoD 5220.22-M, Gutmann. Дослідження rootkits та методів їх виявлення: GMER, memory forensics. Аналіз fileless malware та living off the land техніки.	2
	27	практична робота 12	Виявлення стеганографії в зображеннях. Пошук ADS у NTFS. Аналіз слідів використання secure delete утиліт.	2
12	**Аналітика та моделі розслідування кіберзлочинів**			**6**
	28	лекція 16	Моделі IDIP, EIDIP, HOBFDIP: порівняння. Аналіз цифрового місця злочину. Timeline analysis. Атрибуція: технічна vs юридична. TTPs analysis, MITRE ATT&CK. Кореляція даних. Автоматизовані системи: SIEM, SOAR. Threat intelligence.	2
		самостійне вивчення	Детальне вивчення моделей IDIP, EIDIP, HOBFDIP. Аналіз фреймворку MITRE ATT&CK для атрибуції. Вивчення методів link analysis та pattern recognition. Дослідження платформ Threat Intelligence: MISP, OpenCTI. Аналіз можливостей SIEM систем у розслідуваннях.	2

	29	практична робота 13	Timeline analysis для комплексного кейсу. Кореляція артефактів з різних джерел. Mapping атаки на MITRE ATT&CK.	2
13	**Експертні висновки та звітність у кіберрозслідуваннях**			**8**
	30	лекція 17	Структура експертного висновку. Вимоги до висновків. Документування методології. Chain of custody в звітності. Візуалізація результатів. Судова експертиза. Допит експерта. Етичні аспекти. Стандарти: ISO/IEC 27037, ACPO. Сертифікації: EnCE, GCFA, CFCE.	2
		самостійне вивчення	Вивчення стандарту ISO/IEC 27037. Аналіз ACPO Good Practice Guide. Дослідження вимог до експертних висновків за КПК України (ст. 242-245). Вивчення професійних сертифікацій: EnCE, GCFA, CFCE. Аналіз прикладів експертних висновків.	2
	31	практична робота 14	Складання експертного висновку для модельного кейсу. Документування всіх етапів розслідування. Візуалізація timeline.	2
	32	практична робота 15	Presentation skills: підготовка до допиту експерта. Пояснення технічних аспектів нефахівцям. Захист висновку.	2
			Разом	90
			Підготовка до екзамену	30
			Всього	120

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

№	*Тема дисципліни*	*Вид завдання (реферати, дослідницькі, розрахункові роботи тощо)*	*Календарні строки і форма контролю*
1	Ransomware-атаки: методи розслідування та запобігання	реферат	квітень
2	Методології цифрового розслідування: порівняльний аналіз IDIP, EIDIP, HOBFDIP	реферат	квітень
3	Chain of Custody у цифровій криміналістиці: стандарти та практика	реферат	квітень
4	Правові аспекти збору цифрових доказів в Україні	реферат	квітень
5	Порівняння HDD та SSD у контексті цифрової криміналістики	реферат	квітень
6	Файлові системи NTFS та ext4: структура та можливості для розслідування	реферат	квітень
7	Приховані розділи дисків: DCO, HPA та їх використання у кіберзлочинах	реферат	квітень
8	Процеси завантаження операційних систем та bootkit-атаки	реферат	квітень
9	Slack space та unallocated space: приховані джерела цифрових доказів	реферат	квітень
10	Live forensics vs Dead forensics: переваги, недоліки та сценарії застосування	реферат	квітень
11	Аналіз браузерної активності у цифровому розслідуванні	реферат	квітень
12	EXIF-метадані та геолокація у розслідуванні кіберзлочинів	реферат	квітень
13	Windows Event Logs: структура, аналіз та виявлення аномалій	реферат	квітень
14	Forensic tools: порівняльний аналіз EnCase, FTK, Autopsy, X-Ways Forensics	реферат	квітень
15	Формати forensic images: raw (dd), E01, AFF - переваги та недоліки	реферат	квітень
16	Аналіз реєстру Windows у криміналістичних розслідуваннях	реферат	квітень
17	Мережевий трафік як джерело доказів: PCAP-аналіз за допомогою Wireshark	реферат	квітень
18	DDoS-атаки: механізми, виявлення та розслідування	реферат	квітень
19	Деанонімізація користувачів TOR: методи та обмеження	реферат	квітень
20	Mobile forensics: порівняння методів logical, file system та physical extraction	реферат	квітень
21	Аналіз даних з месенджерів: WhatsApp, Telegram, Viber у контексті розслідування	реферат	квітень
22	Cellebrite vs Oxygen Forensics: можливості та обмеження інструментів	реферат	квітень

23	Стеганографія у кіберзлочинах: методи приховування та виявлення	реферат	квітень
24	Alternate Data Streams (ADS) у NTFS: використання та виявлення	реферат	квітень
25	Rootkits та fileless malware: техніки приховування та методи детекції	реферат	квітень
26	Memory forensics: аналіз оперативної пам'яті для виявлення зловмисної активності	реферат	квітень
27	MITRE ATT&CK framework у розслідуванні кіберзлочинів: TTPs та атрибуція	реферат	квітень
28	Криптовалюти у кіберзлочинах: blockchain-аналіз та трасування транзакцій	реферат	квітень
29	Хмарна криміналістика: особливості збору доказів з AWS, Azure, Google Cloud	реферат	квітень
30	Deepfake-технології: методи виявлення та криміналістичний аналіз	реферат	квітень

7. ПЕРЕЛІК ПИТАНЬ НА ЕКЗАМЕН

1. Що таке кіберзлочин і як його визначає Будапештська конвенція?
2. Які основні типи кіберзлочинів виділяють у міжнародній практиці?
3. У чому полягає різниця між хакерством та кібершпигунством?
4. Що таке ransomware та які основні механізми його роботи?
5. Поясніть різницю між DDoS та DoS атаками
6. Що таке фішинг та які його основні різновиди?
7. У чому полягає суть цифрової криміналістики (digital forensics)?
8. Поясніть різницю між incident response та digital forensics
9. Які основні принципи цифрової криміналістики ви знаєте?
10. Що таке методологія IDIP та які її основні етапи?
11. Опишіть методологію EIDIP та її відмінності від IDIP
12. Що таке методологія HOBFDIP та коли вона застосовується?
13. Які професійні організації та сертифікації існують у сфері цифрової криміналістики?
14. Що таке цифрові докази та які їх основні властивості?
15. Поясніть поняття волатильності даних
16. Що таке Order of Volatility та навіщо він потрібен?
17. Що означає принцип Chain of Custody?
18. Які документи необхідно оформлювати для підтримки Chain of Custody?
19. Які наслідки порушення Chain of Custody для судового процесу?
20. Які статті Кримінального кодексу України регулюють відповідальність за кіберзлочини?
21. Що передбачає стаття 361 КК України?
22. Що передбачає стаття 362 КК України?
23. Що передбачає стаття 363 КК України?
24. Які повноваження має Кіберполіція України?

25. Які процедури необхідно виконати для проведення обшуку при кіберзлочині?
26. Що таке судова комп'ютерно-технічна експертиза?
27. Які міжнародні механізми правової допомоги існують при розслідуванні кіберзлочинів?
28. Що таке HDD та як він працює?
29. У чому різниця між HDD та SSD?
30. Що таке wear leveling у SSD?
31. Що таке TRIM команда і як вона впливає на можливість відновлення даних?
32. Чому відновлення даних з SSD складніше ніж з HDD?
33. Поясніть різницю між логічною та фізичною структурою диска
34. Що таке сектор, трек та циліндр у HDD?
35. Що таке методи адресації CHS та LBA?
36. У чому різниця між MBR та GPT розбиттям диска?
37. Які обмеження має MBR порівняно з GPT?
38. Що таке файлова система FAT32 та її особливості?
39. Опишіть структуру файлової системи NTFS
40. Що таке MFT (Master File Table) у NTFS?
41. Як працює журналювання у файлових системах ext3/ext4?
42. Що таке slack space і як він виникає?
43. Що таке unallocated space та чому він важливий для розслідування?
44. Опишіть процес завантаження Windows
45. У чому різниця між Legacy BIOS та UEFI?
46. Що таке Secure Boot та як він працює?
47. Що таке bootkit та як він відрізняється від rootkit?
48. Опишіть процес завантаження Linux (GRUB)
49. Що таке DCO (Device Configuration Overlay)?
50. Що таке HPA (Host Protected Area)?
51. Як зловмисники можуть використовувати DCO та HPA?
52. Які методи виявлення прихованих розділів існують?
53. Які типи цифрових доказів ви знаєте?
54. Що таке Windows Event Logs і які типи логів існують?
55. Як структуровані лог-файли syslog у Linux?
56. Які артефакти браузерної активності можна використовувати як докази?
57. Що таке cookies та як їх аналізувати?
58. Що таке EXIF-метадані?
59. Які типи геолокаційних даних можна отримати з мобільних пристроїв?
60. Як працює геолокація через Wi-Fi та cell towers?
61. Що таке timeline analysis та навіщо він потрібен?
62. Що таке принцип обміну Локарда у цифровому контексті?
63. У чому різниця між live forensics та dead forensics?
64. Що таке RAM dump і навіщо він потрібен?

65. Який порядок вилучення доказів відповідно до Order of Volatility?
66. Що таке write blocker і навіщо він використовується?
67. Що таке forensic duplicator?
68. Які формати forensic images ви знаєте?
69. У чому переваги формату E01 порівняно з raw (dd)?
70. Що таке хеш-функції та навіщо вони використовуються при створенні образів?
71. Які хеш-алгоритми найчастіше використовуються у цифровій криміналістиці?
72. Що таке file carving?
73. Опишіть структуру реєстру Windows
74. Які ключі реєстру найбільш важливі для розслідування?
75. Що таке EnCase та які його основні можливості?
76. Що таке FTK (Forensic Toolkit)?
77. Що таке Autopsy та його переваги?
78. Що таке X-Ways Forensics?
79. Що таке PCAP-файл?
80. Що таке NetFlow та як він використовується у розслідуванні?
81. Опишіть основні ознаки DDoS-атаки у мережевому трафіку
82. Що таке MITM (Man-in-the-Middle) атака?
83. Що таке SQL Injection?
84. Що таке Cross-Site Scripting (XSS)?
85. Як працює мережа TOR?
86. Які методи деанонімізації TOR-користувачів існують?
87. Що таке Wireshark та його основні можливості?
88. У чому різниця між Android та iOS з точки зору цифрової криміналістики?
89. Що таке logical extraction з мобільного пристрою?
90. Що таке physical extraction?
91. Що таке chip-off метод видобутку даних?
92. Що таке JTAG та як він використовується у mobile forensics?
93. Що таке jailbreak та root?
94. Як виявити наявність jailbreak на iOS пристрої?
95. Що таке Cellebrite UFED?
96. Що таке Oxygen Forensics?
97. Що таке anti-forensics?
98. Які методи приховування слідів використовують зловмисники?
99. Що таке стеганографія?
100. Які інструменти стеганографії ви знаєте?
101. Що таке secure delete?
102. Опишіть метод DoD 5220.22-M для знищення даних
103. Що таке метод Gutmann для знищення даних?
104. Що таке ADS (Alternate Data Streams) у NTFS?
105. Що таке rootkit та які його типи існують?

106. Що таке fileless malware?
107. Що таке living off the land техніка?
108. Що таке технічна атрибуція у кіберзлочинах?
109. Що таке юридична атрибуція?
110. Що таке TTPs (Tactics, Techniques, and Procedures)?
111. Що таке фреймворк MITRE ATT&CK?
112. Що таке Threat Intelligence?
113. Що таке SIEM система?
114. Що таке SOAR платформа?
115. Які вимоги до структури експертного висновку?
116. Що таке стандарт ISO/IEC 27037?
117. Що таке ACPO Good Practice Guide?
118. Які вимоги до експертних висновків встановлені КПК України?
119. Що таке сертифікація EnCE?
120. Що таке сертифікація GCFA?
121. Розробіть алгоритм створення forensic image диска за допомогою FTK Imager
122. Пропишіть послідовність дій для верифікації цілісності forensic image за допомогою хеш-функцій
123. Опишіть алгоритм монтування forensic image для подальшого аналізу
124. Розробіть методику відновлення видалених файлів з NTFS розділу
125. Пропишіть алгоритм аналізу MBR диска за допомогою hex-редактора
126. Опишіть послідовність дій для виявлення прихованих розділів на диску
127. Розробіть алгоритм перевірки наявності DCO або HPA на диску
128. Пропишіть методику виконання RAM dump на працюючій системі
129. Опишіть алгоритм аналізу дампу оперативної пам'яті
130. Розробіть процедуру документування Chain of Custody при вилученні цифрових доказів
131. Пропишіть алгоритм складання протоколу огляду місця події при кіберзлочині
132. Опишіть методику видобутку історії браузера Chrome
133. Розробіть алгоритм аналізу cookies браузера
134. Пропишіть послідовність дій для витягування EXIF-метаданих з фотографії
135. Опишіть алгоритм аналізу Windows Event Logs для виявлення інцидентів
136. Розробіть методику пошуку артефактів у реєстрі Windows
137. Пропишіть алгоритм створення timeline аналізу для розслідування
138. Опишіть послідовність дій для аналізу PCAP-файлу у Wireshark
139. Розробіть методику ідентифікації типу мережевої атаки за трафіком
140. Пропишіть алгоритм витягування файлів з мережевого трафіку
141. Опишіть процедуру виконання logical extraction з Android пристрою

142. Розробіть методику аналізу бази даних WhatsApp
143. Пропишіть алгоритм витягування SMS та дзвінків з мобільного пристрою
144. Опишіть послідовність дій для виявлення стеганографії у зображенні
145. Розробіть алгоритм пошуку ADS у файловій системі NTFS
146. Пропишіть методику виявлення слідів використання secure delete утиліт
147. Опишіть алгоритм аналізу bootloader на наявність модифікацій
148. Розробіть методику file carving для відновлення фрагментованих файлів
149. Пропишіть алгоритм кореляції артефактів з різних джерел для timeline analysis
150. Опишіть послідовність дій для виконання mapping атаки на MITRE ATT&CK фреймворк
151. Розробіть структуру експертного висновку за результатами розслідування
152. Пропишіть алгоритм візуалізації timeline події для судового процесу
153. Опишіть методику підготовки до допиту експерта у суді
154. Розробіть алгоритм пояснення технічних аспектів розслідування нефахівцям
155. Пропишіть процедуру документування всіх етапів криміналістичного дослідження відповідно до стандартів

8. Методи навчання

Під час вивчення дисципліни «Розслідування інцидентів кіберзлочинів» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, лекція, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, самостійне виконання завдань лабораторної роботи, виконання вправ.

9. Контроль результатів навчання

9.1. Форми та засоби поточного і підсумкового контролю

Контроль знань здобувачів освіти здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування, фронтальне опитування;
- поточне тестування;
- підсумкове тестування з кожного змістовного модуля;
- директорська контрольна робота;

- екзамен.

Зміст курсу дисципліни «Розслідування інцидентів кіберзлочинів» поділений на два змістових модулі. Кожний модуль включає в себе лекції, практичні заняття та самостійну роботу студентів і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу. У змістовий модуль 1 (ЗМ1) входять теми 1-3, у змістовий модуль 2 (ЗМ2) – теми 4-6, у змістовий модуль 3 (ЗМ3) – теми 7-10, у змістовий модуль 4 (ЗМ4) – теми 11-13. Після завершення відповідно змістового модуля проводяться модульні контрольні роботи (МК). До модульної контрольної роботи допускаються студенти, які опрацювали весь обсяг теоретичного матеріалу в т. ч і матеріал самостійно, виконали практичні роботи. Рейтингову кількість балів студента формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання практичних робіт і відпрацювання семінарських занять. Участь студентів в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов’язково включають матеріал, який передбачено до самостійного опрацювання студентами. Студент, який не виконав вимоги щодо самостійної роботи чи будь якого іншого виду навчальної діяльності, не допускається до складання МК і даний модуль йому не зараховується. Семестрові бали (семестровий рейтинг) студент отримує як середнє арифметичне балів змістових модулів з усіх тем трьох змістових модулів. Оцінка навчальної успішності студентів здійснюється під час семестрового оцінювання у формі екзамену, який передбачає виконання тестових завдань та вирішення практичного завдання.

9.2 Критерії оцінювання результатів начиння

Оцінка «відмінно» виставляється студенту, який має стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію дисципліни (предмета), усвідомлює взаємозв’язок окремих розділів дисципліни, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів;**

- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів;**

Оцінка «добре» виставляється студенту, який знає викладений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів;**

- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів;**

Оцінка «задовільно» виставляється студенту, який посередньо володіє матеріалом, виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну відповідь на окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти. - питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів;**

- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів;**

Оцінка «незадовільно» виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити, не виконує практичне завдання у визначений термін, із значними помилками заповнює і складає документи, не робить узагальнення і висновки та не охайно оформляє виконані завдання та звіти.

- відповідь має значні помилки елементарного рівня – **1-30 бали;**

- відсутність відповіді на питання – **0 балів.**

9.3. Оцінювання за формами контролю

	Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4	Заліковий модуль (екамен)	Разом
%	20	20	20	20	40	100
Мінімум	0	0	0	0	0	0
Максимум	50	50	50	50	50	50

9.4 Шкала оцінювання

Відсоток формування компетентностей та набуття програмних результатів навчання	**Рейтинг за п'ятдесятибальною шкалою**	**Оцінка за п'ятибальною шкалою**	**Запис у заліковій книжці студента та відомості**
96-100	48, 49, 50	5	відмінно
90-95	45, 46, 47	5	відмінно
84-89	42, 43, 44	4	добре
75-83	38, 39, 40, 41	4	добре
67-74	34, 35, 36, 37	3	задовільно
60-66	30, 31, 32, 33	3	задовільно
менше 60	0-29	2	незадовільно

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

- Витяг з навчального плану
- Програма навчальної дисципліни
- Плани занять
- Конспект лекцій з дисципліни
- Завдання для обов'язкової контрольної роботи
- Інструкційно-методичні матеріали до практичних занять
- Питання до екзамену з модулів
- Контрольні тестові завдання до екзамену з модулів
- Питання до екзамену
- Екзаменаційні білети
- Навчальний посібник
- Роздавальний матеріал
- Презентації до тем

11. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література:

- Гончаров, С. В. *Цифрова криміналістика : навч. посіб.* / С. В. Гончаров. – Харків : ХНУВС, 2020. – 248 с.
- Романюк, Л. М. *Основи комп'ютерної криміналістики* / Л. М. Романюк, А. С. Коваленко. – Київ : НАВС, 2021. – 312 с.
- Nelson, B. *Guide to Computer Forensics and Investigations* / B. Nelson, A. Phillips, C. Steuart. – Boston : Cengage Learning, 2019. – 832 p.
- Nikkel, B. *Digital Forensics: Threatscape and Best Practices* / B. Nikkel. – Hoboken : Wiley, 2020. – 352 p.

Допоміжні

- Sammons, J. The Basics of Digital Forensics / J. Sammons. – 3rd ed. – Syngress, 2020. – 240 p.
- Altheide, C. Digital Forensics with Open Source Tools / C. Altheide, H. Carvey. – 2nd ed. – Syngress, 2020. – 288 p.
- Holt, T. J. Cybercrime and Digital Forensics / T. J. Holt, A. M. Bossler. – 3rd ed. – New York : Routledge, 2022. – 400 p.
- Quick, D. Digital Forensics and Investigation / D. Quick, K.-K. R. Choo. – Springer, 2020. – 275 p.
- Kenneally, E. E. (ed.) Applied Cyber Forensics / ed. E. E. Kenneally. – Springer, 2021. – 298 p.
- Bidgoli, H. (ed.) Handbook of Digital Forensics and Investigation / ed. H. Bidgoli. – Boston : Cengage, 2020. – 540 p.