КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(пост. п. 9 від «23» 12 2021 р.)
Ректор
_____ А. А. Мазаракі

ЦИФРОВА КРИМІНАЛІСТИКА /
DIGITAL FORENSICS

ПРОГРАМА /
COURSE SUMMARY

Київ 2021

Розповсюдження і тиражування без офіційного дозволу КНТЕУ заборонено

Автори: М.В. САШНЬОВА, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного забезпечення та кібербезпеки
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Т.В. САВЧЕНКО, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. САМОЙЛЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «01» листопада 2021р., протокол № 10.

Рецензенти: Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Б.Т. БЕБЕШКО, Senior Software Engineer Softorino Inc.

ЦИФРОВА КРИМІНАЛІСТИКА /
DIGITAL FORENSICS

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Програма дисципліни «Цифрова криміналістика» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», спеціалізації «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України за даною спеціальністю та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких розділів:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання дисципліни «Цифрова криміналістика» є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення захисту інформації, відновлення видалених даних та проведення комп'ютерно-технічної експертизи: розслідування цифрових злочинів обчислювальних пристроїв, включаючи мобільні пристрої, програмне забезпечення, пристрої для зберігання даних, мережі.

Завданням вивчення дисципліни «Цифрова криміналістика» є освоєння принципів та методів збору криміналістичної цифрової інформації із систем, надання студентам необхідної теоретичної та практичної підготовки для того, щоб *знати:*

- теоретичні основи і сучасні інформаційні технології аналізу та збору криміналістичної цифрової інформації;
- особливості проведення статистичного аналізу зловмисного програмного забезпечення;
- принципи роботи програмного забезпечення з відкритим кодом для збору цифрової криміналістичної інформації;
- сучасний стан і шляхи розвитку цифрової криміналістики;

вміти:

- встановлювати і настроювати програмне забезпечення для збору цифрової криміналістичної інформації;
- виконувати аналіз шкідливих програм;
- самостійно виконувати збір та аналіз цифрової криміналістичної інформації;

- розробляти методи реагування та випадки порушень кібербезпеки;
- застосовувати інструменти цифрової криміналістики та відновлення для організації захисту даних в ОС Windwos, macOS, Android, iOS.

Предметом вивчення дисципліни є основні поняття та методи цифрової криміналістики, навики збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та мобільних пристроїв, мереж.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- Основи кібербезпеки;
- Безпека операційних систем;
- Програмні комплекси захисту інформаційних систем;
- Аналіз та оцінка вразливостей інформаційних систем.

вміння:

- працювати з офісними додатками Microsoft;
- працювати з хмарними сервісами Office 365;
- працювати з пошуковою системою Google;
- зламувати паролі загальних типів офісних файлів та резервних копій мобільних пристроїв;
- робити очищення метаданих офісних та pdf документів;
- вміло користуватися шифруванням як апаратного, так і програмного забезпечення.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Цифрова криміналістика», як обов’язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою.

- ✓ ***«Безпека систем електронних комунікацій в економіці»***
  (ОС магістр, ОП 2022 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компе-тентності
Загальні компетентності за освітньою програмою		
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.	1-11
КЗ-2	Здатність проводити дослідження на відповідному рівні.	1-11
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.	1-11
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт.	1-11
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-11
Фахові компетентності за освітньою програмою		
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	4-11
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	1-3
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	4-11

КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	4-11
Програмні результати навчання за освітньою програмою		
РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	4-11
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	4-11
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	5-11
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-3
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	4-11
РН17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	1-10
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	1-11
РН21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	1-11

РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	1-11
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	5-11

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Введення в цифрову криміналістику

Основи цифрової криміналістики. Мета цифрової криміналістики. Потреба в цифровій криміналістиці. Різні види цифрової криміналістики: комп'ютерна криміналістика, мережева криміналістика, криміналістика мобільних пристроїв, криміналістика цифрових зображень, цифрове відео/аудіо криміналістика, тощо.

Обмеження та труднощі застосування цифрової криміналістики. Сучасний стан цифрової криміналістики. Цифрова криміналістика в Україні. Інструменти цифрової криміналістики: апаратне забезпечення, програмне забезпечення.

Цифровий криміналістичний процес: ідентифікація, збереження, збір, аналіз, звітність. Якими навичками повинен володіти комп'ютерний судовий експерт? Види експертиз цифрової криміналістики. Проведення експертизи цифрових доказів. Розуміння ISO 17025/17020. Стандарти комп'ютерно-технічної експертизи: SWGDE.

Список рекомендованих джерел

Основний: 1, 2, 3
Додатковий: 5, 6, 7
Інтернет-джерела: 12, 14, 15

Тема 2. Юридичні аспекти цифрової криміналістики

Роль криміналіста в праві. Прийняття юридичних рішень. Розуміння цифрового розслідування: Етапи процесу розслідування кіберінцидентів. Цифрова криміналістична модель розслідування (Digital

Forensic Investigation Model). Роль слідчого з цифрової криміналістики. Роль законів про кіберзлочинність. Закон про зловживання комп'ютером та як він застосовується. Процес цифрової криміналістики: експертиза, ідентифікація, аналіз, аналіз часової шкали, антицифрова криміналістика, звітування. Судово-науковий процес. Перевірка гіпотез, тестування гіпотез щодо крадіжки даних. Цілісність доказів.

Список рекомендованих джерел

Основний: 1, 2
Додатковий: 5, 6, 8
Інтернет-джерела: 14, 15

Тема 3. Розуміння ролі цифрових доказів

Цифрові докази. Визнання та збирання цифрових доказів. Збереження цифрових доказів. Перевірка даних та збереження цілісності. Основи систем та файлові системи. Різниця між даними та метаданими: формати файлів та розширення; метадані файлової системи та файлові метадані. Природа цифрових доказів: біти, фрагменти та байти, перетворення даних між двійковим, шістнадцятковим та ASCII. Структури та кодування даних: ASCII, Unicode, Base64.

Розуміння криміналістичних зображень: фізичні та логічні образи; формати криміналістичних зображень. Джерела цифрових доказів: комп'ютери та ноутбуки, сервери, віртуальні машини, планшети та мобільні пристрої, знімний носій інформації, мережеві пристрої та дані, вбудовані/IoT – пристрої, цифрові докази в хмарі, ICS/SCADA, дрони та транспортні засоби.

Настанови ISO 27042 для аналізу та інтерпретації цифрових доказів. Керівні принципи NPCC та їх застосування до збору цифрових доказів.

Список рекомендованих джерел

Основний: 1
Додатковий: 7, 9
Інтернет-джерела: 12, 13, 15

Тема 4. Цифрова криміналістика файлових систем

Аналіз функціональності файлової системи. Файлові системи (NTFS, FAT) та зберігання даних. Перевірка дисків NTFS. Розуміння шифрування диску. Атрибути метаданих NTFS. Правила часових міток Windows для $ StdInfo та $ Filename. Виявлення маніпуляції часовими позначками. Аналіз папки Prefetch. Відновлення видалених файлів чи

папок у розділі FAT, NTFS. Аналіз підписів. Криміналістична експертиза файлових зображень. Стенографія у файлах зображень.

Список рекомендованих джерел

Основний:1, 3
Додатковий: 7, 9
Інтернет-джерела: 12, 13, 15

Тема 5. Технічні засоби цифрової криміналістики

Засоби стирання, видалення даних та інформації.

Пристрої для знищення цифрової інформації з використанням програмних засобів, а також апаратні засоби для миттєве знищення даних на магнітних носіях без можливості відновлення. Устаткування для віддаленого і екстреного знищення інформації на жорстких дисках.

Засоби копіювання даних.

Засоби копіювання даних на HDD. Копіювання даних на мобільних телефонах. Системи тиражування дисків HDD. Виготовлення необмеженої кількості копій (клонів) жорстких дисків за короткий час.

Засоби блокування запису. Обладнання для блокування запису.

Принципи функціонування апаратних блокаторів запису. Принципи функціонування апаратних блокаторів запису. Принципи тестування апаратних блокаторів запису. Методика тестування апаратних блокаторів запису. Блокатори запису для запобігання випадкового або навмисного внесення змін до комп'ютерних даних.

Аналіз зібраної інформації.

Аналізатори протоколів. Пристрої для аналізу протоколів інтерфейсу ATA, призначені для реєстрації та відображення команд і даних, що передаються між будь-якими пристроями з інтерфейсами Parallel ATAабо Serial ATA.

Відновлення даних.

Системи відновлення даних комп'ютерної криміналістик: спеціалізовані пристрої відновлення даних з комп'ютерної техніки, систем зберігання даних, відеореєстраторів, мобільних телефонів та інших портативних пристроїв. Проблема відновлення даних з флеш-накопичувачів. Проблема відновлення даних з пошкоджених жорстких дисків.

Список рекомендованих джерел

Основний: 1, 3
Додатковий: 5, 7, 9
Інтернет-джерела:12, 13, 16

Тема 6. Спеціалізоване програмне забезпечення для цифрової криміналістики

Базові методи використання спеціалізованого програмного забезпечення. Необхідність спеціалізованого програмного забезпечення. Огляд рекомендованих програмних комплектів. Рекомендації по використанню певних програмних інструментів для спеціальних завдань.

Обробка цифрової криміналістики в програмному забезпеченні. Аналіз реєстру Windows. Використання Hex-редактора. Отримання та збереження доказів. Імпорт доказів. Пошук і фільтрація.

Програмно-апаратні засоби моніторингу використання ресурсів Інтернет, запобігання витоку інформації, аналіз та відновлення втрачених даних.

Список рекомендованих джерел

Основний: 1, 3
Додатковий: 7, 9
Інтернет-джерела:12, 13, 16

Тема 7. Цифрова криміналістика операційних систем: OS WINDOWS

Вступ до криміналістики WINDOWS. Функції безпеки та шифрування, загальні для операційної системи Windows.

Аналіз реєстру Windows на предмет доказів. Інформація в реєстрі, що має судову цінність. Докази бездротового зв'язку в реєстрі. Реєстр IP -адрес інтерфейсів користувача. Зберігання артефактів у реєстрі. Програмне забезпечення SAM, Система NTUSER.dat тощо. Аналіз даних HTTP за допомогою Wireshark. Аналіз артефактів веб-браузера.

Концепції, ідентифікація та аналіз артефактів Windows: використання додатків, взаємодія з користувачами, журнали подій, тіньові копії томів, тощо. Знайомство з модульним інструментом сортування, збору та аналізу артефактів судово-медичної експертизи в реальних та змонтованих системах (KAPE).

Список рекомендованих джерел

Основний: 1, 3, 4
Додатковий: 10
Інтернет-джерела: 16, 17, 18, 19

Тема 8. Цифрова криміналістики операційних систем: macOS

Огляд версій macOS: особливості криміналістичної важливості в різних версіях macOS та час їх появи. Розуміння технології файлової системи MAC – огляд усієї технології файлової системи, що підтримується macOS, наприклад: APFS, Core Storage, Fusion Drives та macOS Extended. Intel Mac Technology and Bootcamp – криміналістичне значення технології Mac Intel. M1 Silicon Mac Technology – унікальні проблеми та криміналістичне значення технології M1 Silicon. Проблеми безпеки MAC та атаки FileVault. Відкриті паролі прошивки – OFP: встановлення та видалення OFP. Imaging Mac RAM – проблеми із захопленням оперативної пам’яті через функції безпеки macOS. Встановлення криміналістичних зображень у macOS – безпечне встановлення криміналістичних зображень для обробки та аналізу. Пошук доказів – як ідентифікувати, аналізувати та витягати macOS та артефакти додатків, такі як електронна пошта, графіка, Інтернет-артефакти, документи, системні артефакти, миттєві повідомлення, журнали, тощо. Вивчення баз даних SQLite та файлів PLIST – вивчення основ зберігання даних MAC.

Список рекомендованих джерел

Основний: 1, 3, 4
Додатковий: 7
Інтернет-джерела: 12, 13, 16, 17

Тема 9. Криміналістика мобільних пристроїв

Мобільна криміналістика: яку інформацію може надати мобільний пристрій. Отримання файлової системи та фізичних зображень з мобільних телефонів. Файлові системи в iOS, Android. Флеш-пам'ять, архітектура NAND Ram: як мобільні телефони зберігають свої дані на фізичному рівні. Отримання та обробка файлів резервних копій iOS, включаючи ручне декодування, синтаксичний аналіз та взлом зашифрованих зображень файлів резервних копій. Перегляд та інтерпретація файлів iOS, таких як списки, для отримання цінних доказів. Криміналістика Android. Модель безпеки Android, методи виявлення. Криміналістичне дослідження додатків Android. SQLite-аналіз BlackBerry Messenger на Android. Обробка інцидентів із мобільними загрозами. Pithus – мобільна розвідка про загрози з відкритим кодом. Інструменти: APKiD, ssdeep, AndroGuard, MobSF.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 11
Інтернет-джерела: 12, 13, 16, 20, 21

Тема 10. Мережева криміналістика

Основні інструменти криміналістичної мережі: tcpdump та Wireshark. Типи та джерела мережевих доказів. Архітектурні проблеми мережі. Розслідування OPSEC та загроза Intel. Аналіз мережевих протоколів: протокол передачі гіпертексту (HTTP), служба доменних імен (DNS), протокол передачі файлів (FTP), блок повідомлень сервера (SMB) та відповідні протоколи Microsoft, простий протокол передачі пошти (SMTP). Інструменти судової експертизи комерційної мережі.

Бездротові мережі. Криміналістичні артефакти від бездротового трафіку. Поширені методи атаки та виявлення. Журнал даних для доповнення обстежень мережі. Syslog. Брандмауери, системи виявлення вторгнень (IDSes) та платформи моніторингу безпеки мережі (NSM). Збір, агрегування та аналіз журналів.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 7
Інтернет-джерела: 12, 13, 16

Тема 11. Онлайн криміналістика: криміналістичне розслідування електронної пошти, вебсайту та соціальних мереж. Хмарна криміналістика

Вивчення ролі електронної пошти в криміналістичних розслідуваннях. Криміналістика злочинів та порушень електронної пошти. Використання спеціалізованих інструментів криміналістики електронної пошти. Застосування цифрової криміналістичної експертизи в соціальних мережах. Криміналістика вебсайту: архіви, статистика вебсайту.

Хмарна криміналістика. Огляд хмарних обчислень. Юридичні аспекти в хмарній криміналістиці. Технічні аспекти в хмарній криміналістиці. Проведення хмарного криміналістичного розслідування. Інструменти для проведення хмарної криміналістичної експертизи.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 7
Інтернет-джерела: 12, 13, 16

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Nihad A. Hassan. Digital Forensics Basics: A Practical Guide Using Windows OS. New York, USA, 2019. – 347 Pages. – ISBN-13 (pbk): 978-1-4842-3837-0

2. Шеремет А.П. Криміналістика: навч. пос. [для студ. вищ. навч. закл.] / А.П. Шеремет– [2-ге вид.]. – К.: Центр учбової літератури, 2009. – 472 с. – ISBN 978-966-364-822-4

3. Bill Nelson, Amelia Phillips, Christopher Steuart. Guide to Computer Forensics and Investigations Fifth Edition. Cengage Learning, Boston, 2016. – 690 Pages. – ISBN: 978-1-285-06003-3

4. Dr. Darren R. Hayes. A Practical Guide to Computer Forensics Investigations – Pearsoncmg. Pearson Education, Inc., USA, 2015. – 120 Pages. ISBN-13: 978-0-7897-4115-8

Додатковий

5. Удовенко Ж.В. Криміналістика: конспект лекцій. За заг. Ред. Галана В.І. / Ж.В. Удовенко – К. : «Центр учбової літератури», 2016. – 320 с. – ISBN 978-617-673-452-9

6. Криміналістика: підруч. Для студ. вищ. навч. закл. / [К.О. Чаплинський, О.В. Лускатов, І.В. Пиріг, В.М. Плетенець, Ю.А. Чаплинська]. – 2-евид, перероб. І доп. – Дніпро : Дніпроп. держ. ун-т внутр. справ ; ЛіраЛТД, 2017. – 480 с.

7. Terrence V. Lillard. Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data. Elsevier Inc., 2010 - 339 Pages. – ISBN 978-1-59749-537-0 (pbk. : alk. paper)

8. 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. – 164 с. ISBN 978-966-937-842-2

9. Computer Forensics: Investigating Data and Image Files. Investigating Data and Image Files: EC-Council | Press. Course Technology/Cengage Learning Cengage Learning, USA, 2010. – 227 Pages.ISBN – 13: 978-1-4354-8351-4

10. Harlan A. Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry. Elsevier Inc., Cambridge, 2016 - 204 Pages. ISBN: 978-0-12-803291-6.

11. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.*

Інтернет-джерела

12. Irfan Shakeel. Introduction to Computer Forensics & Digital Investigation. URL: https://www.academia.edu/15604772/Introduction_to_Computer_Forensics_and_Digital_Investigation

13. Робоча група Науково на цифрових доказів (SWGDE). URL: https://www.swgde.org/documents/published

14. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № №4651-VI. Дата оновлення: 18.10.2019. URL: https://zakon.rada.gov.ua/laws/show/4651–17

15. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів [Текст]. – На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Чинний від 2019-01-01.−Київ : УкрНДНЦ, 2018.−VI, 31 с.: рис., табл. (Національний стандарт України). URL: https://budstandart.ua/normativ-document.html?id_doc=74978

16. Become a Cyberwarrior.URL: https://www.hackers-arise.com/post/2016/10/10/Digital-Forensics-Part-3-Recovering-Deleted-Files

17. WORLD LEADERS IN DIGITAL FORENSICS TRAINING & CERTIFICATION. URL: https://www.iacis.com/

18. KAPE. URL: https://aboutdfir.com/toolsandartifacts/windows/kape/

19. Вступ до криміналістики Windows. URL: https://www.youtube.com/playlist?list=PLlv3b9B16ZadqDQH0lTRO4kqn2P1g9Mve

20. Обробка інцидентів із мобільними загрозами. URL: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobilethreatsincidenthandlingtoolset.pdf

21. Pithus. URL: https://beta.pithus.org/about/

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*