Силабус освітнього компонента
Програма навчальної дисципліни

Цифрова криміналістика

Шифр та назва спеціальності
К3 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Національна безпека у сфері кіберзахисту

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
4

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Цифрова криміналістика" є нормативною навчальною дисципліною. Вивчення дисципліни спрямоване на отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних; формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки.

Мета та цілі дисципліни

Формування знань і вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки. Вивчення дисципліни "Цифрова криміналістика" сприяє отриманню знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних, а також формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
СК2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
РН8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.
РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

Обсяг дисципліни

Загальний обсяг дисципліни 180 год. (6 кредитів ECTS): лекції – 32 год., лабораторні роботи – 48 год., самостійна робота – 100 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології та криптоаналіз, Лінійна алгебра, Основи криптографічного захисту, Дискретна математика, Інформатика, Програмування.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ. Цілі та завдання навчальної дисципліни «Цифрова криміналістика». Місце дисципліни у навчальному процесі. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.	2
Тема 2. Електронні (цифрові) докази. Цифрові дані як докази: визначення, роль, типи, характеристика, законодавчі вимоги. Характеристика криміналістичних досліджень. Типи кіберзлочинів, проблеми розслідувань, загальні правила криміналістичних досліджень. Правила поводження із електронними доказами. Типи електронних доказів. Криміналістичні дослідження як складова реагування на інциденти порушення кібербезпеки. Ролі та обов'язки осіб, що проводять криміналістичні дослідження.	2
Тема 3. Процес первинних цифрових криміналістичних досліджень. Фази первинних цифрових криміналістичних досліджень. Вимоги до обладнання, ролі учасників первинних цифрових криміналістичних досліджень.Пошук, виявлення, збір, фіксація і збереження електронних доказів. Порядок передачі та зберігання (chain of custody) електронних доказів. Створення дублікатів, відновлення даних і первинна експертиза електронних доказів. Звіт про криміналістичні дослідження і свідчення у суді.	2
Тема 4. Структура жорсткого диску та файлових систем. Типи жорстких дисків зберігання даних, їх характеристики. Фізична та логічна структура жорстких дисків. Розділи жорстких дисків. Завантаження з диску ОС Windows, Linux, Mac. Файлові системи ОС Windows, Linux, Mac. Відмінності різноманітних RAID систем зберігання. Порядок аналізу файлових систем.	2
Тема 5. Вилучення даних та створення дублікатів носіїв даних. Загальний опис процесу вилучення даних. Вилучення динамічних даних (live data). Вилучення статичних даних (static data). Послідовність у вилученні та дублюванні даних. Забезпечення незмінності оригінальних носіїв даних. Визначення підходящих методів і засобів вилучення даних. Вилучення даних з Windows і Linux комп'ютерів. Найкращі практики вилучення даних.	2
Тема 6. Методи протидії криміналістичним дослідженням. Поняття протидії криміналістичним дослідженням. Методи протидії криміналістичним дослідженням. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням. Контрзаходи протидії	2

криміналістичним дослідженням. Основні виклики у подоланні протидії криміналістичним дослідженням.	
Тема 7. Криміналістичні дослідження операційних систем. Порядок збору і огляду летючих і нелетючих даних з Windows комп'ютерів. Аналіз пам'яті і реєстру Windows. Огляд кешу, куків та історії веб-браузерів Windows. Огляд файлів і метаданих в Windows. Аналіз журналів подій Windows. Аналіз журналів подій Linux. Збір і огляд летючих і нелетючих даних з Linux комп'ютерів. Аналіз файлів і журналів подій Mac комп'ютерів.	2
Тема 8. Криміналістичні дослідження комп'ютерних мереж. Сутність криміналістичного дослідження комп'ютерних мереж. Протоколювання трафіку комп'ютерної мережі. Принципи взаємозв'язків подій. Підготовка і етапи проведення криміналістичного дослідження комп'ютерних мереж. Огляд маршрутизатору, міжмережного екрану, системи виявлення вторгнень, DHCP-сервера, баз даних. Огляд трафіку. Документування отриманих із мережі доказів. Реконструкція доказів.	2
Тема 9. Криміналістичні дослідження веб-атак. Сутність криміналістичного дослідження веб-атак. Архітектура веб-застосунків і виклики їх криміналістичного дослідження. Індикатори веб-атак і визначення загроз веб-застосункам. Етапи проведення криміналістичного дослідження веб-атак. Криміналістичне дослідження веб-атак на Windows сервери. Архітектура IIS веб-сервера і криміналістичний аналіз його лог- файлів. Архітектура Apache веб-сервера і криміналістичний аналіз його лог-файлів. Розслідування різноманітних атак на веб-застосунки.	2
Тема 10. Криміналістичні дослідження баз даних. Сутність криміналістичного дослідження баз даних. Криміналістичне дослідження MS SQL. Виявлення репозиторіїв баз даних і збір файлів-доказів. Огляд файлів з використанням SQL Management Studio і ApexSQL DBA. Криміналістичне дослідження MySQL. Архітектура MySQL і визначення структури тек даних. Інструменти криміналістичного дослідження MySQL. Криміналістичне дослідження MySQL на WordPress.	2
Тема 11. Криміналістичні дослідження хмарних сервісів. Технології хмарних обчислень. Відомі атаки на технології хмарних обчислень. Сутність криміналістичного дослідження технології хмарних обчислень. Завдання криміналістичного дослідження хмарних сервісів. Відмінності різних типів криміналістичного дослідження хмарних сервісів. Ролі зацікавлених сторін у криміналістичному дослідженні хмарних сервісів. Виклики, що виникають під час проведення криміналістичного дослідження хмарних сервісів. Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive.	2
Тема 12. Криміналістичні дослідження шкідливого програмного забезпечення. Шкідливе програмне забезпечення (ШПЗ) та шляхи його впровадження в систему. Методи розповсюдження ШПЗ. Основні складові ШПЗ. Принципи криміналістичного дослідження ШПЗ. Ідентифікація і вилучення ШПЗ з включеної і виключеної системи. Створення лабораторії і середовища з аналізу шкідливих програм. Правила лабораторного аналізу ШПЗ. Динамічний і статичний аналіз. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.	2
Тема 13. Криміналістичні дослідження електронної пошти. Архітектура системи електронної пошти, сервери і клієнти, їх характеристики. Важливість електронних повідомлень. Злочини, де використовується	2

електронна пошта. Складові листа електронної пошти, службові заголовки листа. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих. Інструменти криміналістичного дослідження електронної пошти.	
Тема 14. Криміналістичні дослідження мобільних пристроїв. Необхідність криміналістичного дослідження мобільних пристроїв. Роль апаратних і програмних платформ у криміналістичного дослідження мобільних пристроїв. Рівні архітектури оточення мобільних пристроїв. Стек архітектури Android і процеси завантаження системи. Стек архітектури iOS і процеси завантаження системи. Визначення місць збереження доказових даних. Підготовка до криміналістичного дослідження мобільних пристроїв. Криміналістичні дослідження мобільних пристроїв.	2
Тема 15. Складання звіту і представлення результатів криміналістичних досліджень. Важливість оформлення звіту щодо результатів криміналістичних досліджень. Узагальнений шаблон звіту криміналістичних досліджень. Види звітів та методика їх складання. Спеціаліст з первинних криміналістичних досліджень як свідок. Порівняння ролей експертів і технічних спеціалістів. Свідчення спеціаліста у суді.	2
Тема 16. Використання державних інформаційних систем під час вирішення криміналістичних завдань. Криміналістична реєстрація як інформаційна система. Обліки Міністерства внутрішніх справ України. Обліки інформаційно-довідкової служби. Обліки митної служби. Криміналістичні обліки міжнародних організацій. Використання інформації криміналістичних реєстраційних систем.	2
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Встановлення та налаштування спеціалізованого програмного забезпечення. Розгортання та налаштування форензичних дистрибутивів і інструментів (наприклад, Autopsy, FTK Imager, Volatility, Kali) для збору й аналізу цифрових доказів; налаштування робочого середовища, правил безпеки та збереження доказів.	6	0,1
Тема 2. Збір та аналіз цифрової криміналістичної інформації в ОС Windows. Практичні методи вилучення летючих і статичних артефактів у Windows — реєстр, журнали подій, браузерні артефакти, файли користувача; створення форензичних образів та первинний аналіз.	6	0,1
Тема 3. Збір та аналіз цифрової криміналістичної інформації в ОС Linux. Збір артефактів і логів у Linux-середовищі (файли журналів, конфігурації, cron, активні процеси, мережеві налаштування); створення образів дисків і перевірка цілісності через хешування.	6	0,1
Тема 4. Відновлення видаленого розділу та відновлення RAID. Методи відновлення видалених розділів і даних; розпізнавання типів RAID, відновлення логічних томів і збір доказів з RAID-масивів із урахуванням збереження цілісності.	6	0,1

Тема 5. Аналіз файлової системи NTFS. Дослідження структури NTFS (MFT, журнал USN, метадані), виявлення слідів видалення/перезапису, аналіз атрибутів файлів і відновлення видалених об'єктів.	6	0,1
Тема 6. Аналіз артефактів прикладних програм у Windows. Виявлення та інтерпретація артефактів від поштових клієнтів, месенджерів, офісних програм і браузерів; робота з кешами, історією і метаданими для відтворення хроніки користувацької активності.	6	0,1
Тема 7. Криміналістичний аналіз мережі. Збір і аналіз мережевого трафіку (PCAP), реконструкція сесій, ідентифікація зловмисної активності, кореляція подій з логами мережевих пристроїв і підготовка доказової бази.	6	0,1
Тема 8. Аналіз оперативної пам'яті. Зняття дампу оперативної пам'яті, статичний і динамічний аналіз процесів, виявлення запущеного шкідливого коду, мережевих з'єднань і прихованих артефактів; застосування інструментів типу Volatility для витягання доказів..	6	0,1
Загальна кількість годин	**48**	$\sum_{i=1}^{n} a_i$=0,8

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Первинні цифрові криміналістичні дослідження та вилучення електронних доказів. Перевірка практичних і теоретичних знань студентів з організації первинних криміналістичних дій: пошук, фіксація, вилучення і дублювання носіїв; робота з летючими й статичними даними; забезпечення ланцюга зберігання (chain of custody) та збереження цілісності доказів.	0,1
Тема 2. Криміналістичні дослідження мереж, шкідливого ПЗ і хмарних сервісів. Оцінка вмінь аналізувати мережеві докази та шкідливе програмне забезпечення, проводити розслідування веб-атак і дослідження подій у хмарних середовищах; розробка плану розслідування, збір і інтерпретація мережевих логів і артефактів.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи цифрової криміналістики. Огляд принципів, завдань та етапів цифрового розслідування, ролі цифрових доказів і вимог до їх збереження.	10
Тема 2. Типи цифрових доказів та методи їх збору. Вивчення класифікації цифрових доказів, способів їх ідентифікації, збору,	10

документування та забезпечення цілісності.	
Тема 3. Правові та етичні аспекти цифрової криміналістики. Розгляд законодавчих вимог до збору, зберігання і використання цифрових доказів, а також питань конфіденційності та етики.	10
Тема 4. Форензичний аналіз мобільних пристроїв. Вивчення принципів отримання даних із мобільних пристроїв, аналіз журналів викликів, повідомлень, геолокації, додатків.	10
Тема 5. Методи вилучення та аналізу лог-файлів. Розбір структури системних і мережевих логів, методи їх інтерпретації для виявлення інцидентів безпеки.	10
Тема 6. Форензичний аналіз шкідливого програмного забезпечення. Дослідження методів ідентифікації, динамічного та статичного аналізу зразків шкідливого коду.	10
Тема 7. Відновлення видалених або зашифрованих даних. Вивчення інструментів і технік відновлення втрачених файлів, розділів, а також розшифрування зашифрованих об'єктів.	10
Тема 8. Мережевий форензичний аналіз. Огляд методів збору та аналізу мережевого трафіку, виявлення зловмисних дій, аналіз файлів PCAP і логів IDS/IPS.	10
Тема 9. Хмарна криміналістика. Дослідження особливостей збору цифрових доказів у хмарних середовищах, збереження метаданих і трасування користувацької активності.	10
Тема 10. Інструменти автоматизації цифрового розслідування. Огляд сучасних засобів автоматизації процесів аналізу цифрових доказів (Autopsy, Magnet AXIOM, X-Ways Forensics, Volatility).	10
Загальна кількість годин	**100**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.
https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf
2 Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf

Додаткова література

3. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно	F

(потрібне повторне вивчення)

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Андрій ТКАЧОВ