Силабус освітнього компонента
Програма навчальної дисципліни

Цифрова криміналістика

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Спеціальна (фахова) підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
1

Мова викладання
Українська, англійська

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

Вивчення дисципліни спрямовано на освоєння основних понять та методів цифрової криміналістики, навиків збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux.

Мета та цілі дисципліни

Формування знань і вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки. Основними завданнями вивчення дисципліни "Цифрова криміналістика" є отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних, а також формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки. Предметом навчальної дисципліни є основні поняття та методи цифрової криміналістики, навики збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux.

Формат занять

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

Компетентності

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
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.

Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
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.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
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.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

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.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
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.
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.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Основи криптографічного захисту, Основи програмування, Аналіз шкідливих програм.

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. Основні поняття та визначення у сфері кібербезпеки. Еволюція комп'ютерної криміналістики. Комп'ютерні криміналістичні методики. Широкі тести доказів. інциденти, що заважають бізнесу. Руйнівні випадки комп'ютерної злочинності. Криміналістична готовність. кіберзлочинність.	6
Тема 2. Лабораторії комп'ютерної криміналістики. Аспекти фізичної безпеки лабораторії. Рекомендації з фізичної безпеки для криміналістичної лабораторії. Загальна конфігурація лабораторії судової експертизи. Устаткування, необхідне судово-медичної експертизи. Основні вимоги до робочої станції у судово-медичній лабораторії. Необхідні криміналістичні інструменти.	6
Тема 3. Процес комп'ютерного розслідування. Розробка політики та процедур розслідування. Стандартні кроки під час підготовки судової справи. Оцінка справи. Попереджувальні банери. Збір доказів. Підтримка професійної поведінки. Закриття справи.	4
Тема 4. Процедури швидкого реагування. Роль першого відповідача. Електронні пристрої: види та збір можливих доказів. Інструментарій швидкого реагування. Реакція на інцидент: різні ситуації. Охорона та оцінка місця електронного злочину. Проведення попередніх інтерв'ю. Документування місця електронного злочину. Збір та збереження	4

електронних доказів. Порядок волатильності. Упаковка та транспортування електронних доказів.	
Тема 5. Обробка інцидентів. Основні умови. Типи інцидентів. Як ідентифікувати інцидент. Як запобігти інциденту. Визначення зв'язку між реакцією на інцидент, інцидентом. Обробка та управління інцидентами. Управління інцидентами. Звіт про інциденти. реагування на інциденти. Процедура обробки інцидентів. CSIRT.	4
Тема 6. Зломщики паролів додатків. Термінологія пароля. Методи зламу пароля. Зламування системного пароля. Інструменти для зламу пароля. Захист пароля.	4
Тема 7. Розуміння файлових систем. Ключові терміни. Жорстки диски. Файлова система.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Встановлення та настройка спеціалізованого програмного забезпечення. Практична робота з інсталяції та початкового налаштування інструментів цифрової криміналістики (аналізатори образів дисків, інструменти для зняття пам'яті, утиліти для створення хешів, SIEM-клієнти). Відпрацювання конфігурацій безпечного робочого середовища (ізольовані лабораторії, налаштування мережевих правил, збереження логів).	2	-
Тема 2. Збір та аналіз цифрової криміналістичної інформації в ОС Windows. Методика збору летючих і нелетючих даних із Windows-систем: створення образів диска, експорту реєстру, збір журналів подій, аналіз браузерних артефактів і тимчасових файлів. Практичні вправи з використанням інструментів для вилучення та первинного аналізу.	2	0,1
Тема 3. Збір та аналіз цифрової криміналістичної інформації в ОС Linux. Збір і аналіз даних у Linux-середовищі: вилучення логів (syslog, auth), знімки процесів, мережеві логи, дослідження файлових систем і прав доступу. Практика створення образів і аналізу слідів у сервісах та демонах.	2	0,1
Тема 4. Відновлення видаленого розділу та відновлення RAID. Методи виявлення та відновлення видалених розділів і таблиць розділів, підходи до реконструкції RAID-масивів (RAID0, RAID1, RAID5) та відновлення даних із пошкоджених масивів. Практичні кейси — відновлення структури та вилучення файлів.	2	0,1
Тема 5. Аналіз файлової системи NTFS. Детальний огляд NTFS: MFT, записів файлів, атрибутів, журналу	2	0,1

транзакцій, метаданих та їх ролі як джерела доказів. Практичні вправи з витяганням артефактів (відновлення видалених файлів, аналіз часів змін, зв'язки між MFT-записами).		
Тема 6. Аналіз артефактів прикладних програм у Windows. Дослідження артефактів відомих прикладних програм — веб-браузерів, поштових клієнтів, месенджерів, пакету Office — і способів отримання доказових даних (історія, кеші, локальні бази, метадані документів). Практичні вправи з інструментами витягання артефактів.	2	0,1
Тема 7. Криміналістичний аналіз мережі. Збір і аналіз мережевих доказів: захоплення трафіку (pcap), аналіз мережевих сесій, відновлення передачі файлів, кореляція подій мережевого обладнання (маршрутизатори, міжмережеві екрани, IDS). Практичні завдання з реконструкції інциденту за мережевими даними.	2	0,1
Тема 8. Аналіз оперативної пам'яті. Методи збору та аналізу оперативної пам'яті (RAM): створення дампів, пошук процесів, відкритих з'єднань, ключів ідентифікації шкідливого ПЗ, витяг метаданих і об'єктів у пам'яті. Практична робота з інструментами для статичного й динамічного аналізу пам'яті.	2	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Процес комп'ютерного розслідування та криміналістична готовність організації. Розглядаються основні етапи розслідування кіберінцидентів — від виявлення до закриття справи. Аналізується поняття криміналістичної готовності організації: політики, процедури, документація, навчання персоналу. Завдання включають опис процесу збору цифрових доказів, створення політики реагування на інциденти та моделювання сценарію розслідування.	0,1
Тема 2. Управління інцидентами та роль CSIRT у забезпеченні цифрової безпеки. Вивчається процес управління інцидентами — класифікація, ідентифікація, реагування та звітність. Окрема увага приділяється ролі команди реагування на інциденти безпеки (CSIRT), її структурі, функціям і взаємодії з іншими підрозділами. Практична частина може включати розробку алгоритму реагування на кіберінцидент або шаблону звіту CSIRT.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин

Тема 1. Основні принципи цифрової криміналістики. Вивчення базових понять, принципів збереження доказів, непорушності даних та етичних норм у криміналістичній практиці.	8
Тема 2. Міжнародні стандарти цифрової криміналістики. Ознайомлення з міжнародними стандартами (ISO/IEC 27037, 27041, 27042, 27043), їхнім призначенням та використанням у практиці розслідувань.	8
Тема 3. Цифрові докази та ланцюг зберігання (Chain of Custody). Дослідження процедур документування, передачі та зберігання цифрових доказів, що забезпечують їхню достовірність у суді.	7
Тема 4. Криміналістичні інструменти з відкритим кодом. Вивчення найпопулярніших безкоштовних засобів криміналістичного аналізу (Autopsy, FTK Imager, Volatility, Wireshark) та принципів їх роботи.	7
Тема 5. Особливості дослідження мобільних пристроїв. Аналіз архітектури Android та iOS, методів вилучення даних, резервних копій, а також виявлення цифрових артефактів у смартфонах.	7
Тема 6. Методи виявлення шкідливого програмного забезпечення. Розгляд методів динамічного та статичного аналізу шкідливих програм, створення безпечного середовища для досліджень.	7
Тема 7. Особливості криміналістики хмарних обчислень. Вивчення процесів збору цифрових доказів у хмарних середовищах, обмежень, що виникають через віртуалізацію та розподілення даних.	7
Тема 8. Криміналістичний аналіз мережевого трафіку. Розгляд принципів збору, збереження та аналізу мережевого трафіку з метою відтворення дій користувача або зловмисника.	7
Тема 9. Електронна пошта як джерело доказів. Вивчення структури електронних листів, методів аналізу заголовків (headers), визначення джерела повідомлення та перевірки достовірності.	7
Тема 10. Судова експертиза у сфері кіберзлочинів. Ознайомлення з етапами проведення судової експертизи цифрових доказів, ролями експертів і процедурою представлення результатів у суді.	7
Загальна кількість годин	**72**

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

1. 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».

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D

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

60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

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** Ольга КОРОЛЬ