Силабус освітнього компонента
Програма навчальної дисципліни

Цифрова криміналістика

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Спеціальна (фахова) підготовка, Обов'язкова

Семестр
1

Мова викладання
Українська

Викладачі, розробники

МІЛОВ Олександр Володимирович
oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «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 роботи, самостійна робота, консультації. Підсумковий контроль – 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, Етичний хакінг, Безпека Інтернет речей та сервісів, Основи наукових досліджень.

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.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ.
Цілі та завдання навчальної дисципліни «Цифрова криміналістика». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.
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.
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.
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.
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.
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 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.
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.
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.

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.

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.

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.

Тема 13. Криміналістичні дослідження електронної пошти.

Архітектура системи електронної пошти, сервери і клієнти, їх характеристики. Важливість електронних повідомлень. Злочини, де використовується 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.

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.

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.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Встановлення та настройка спеціалізованого програмного забезпечення.

Тема 2. Збір та аналіз цифрової криміналістичної інформаці в ОС Windows.

Тема 3. Збір та аналіз цифрової криміналістичної інформаці в ОС Linux.
Тема 4. Відновлення видаленого розділу та відновлення Raid.
Тема 5. Аналіз файлової системи NTFS.
Тема 6. Аналіз артефактів прикладних программ у Windows.
Тема 7. Криміналістичний аналіз мережі.
Тема 8. Аналіз оперативної пам'яті.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•контрольна робота: 20% семестрової оцінки;
•залік: 40% семестрової оцінки.

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 (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент 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

28.08.2024 — Завідувач кафедри — Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП — Ольга КОРОЛЬ