Силабус освітнього компонента
Програма навчальної дисципліни

Аналіз шкідливих програм

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
Наукова підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬ Ольга Григорівна
olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua

Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор понад 170 наукових і навчально-методичних праць (за даними Google Scholar, h-індекс – 12), у тому числі 3 монографій та навчального посібника з грифом.
Має у своєму доробку 10 патентів та 10 авторських свідоцтв.
Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки», «Авторське право у цифровому суспільстві».
Сфера наукових інтересів охоплює питання інтелектуальної власності, правового регулювання кіберпростору, інформаційної безпеки, криптографічних методів захисту, цифрові активи.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Курс «Аналіз шкідливого програмного забезпечення» спрямований на формування знань і практичних навичок з виявлення, дослідження та протидії сучасним шкідливим програмам. У ході вивчення дисципліни здобувачі ознайомляться з класифікацією та методами поширення шкідливого коду, особливостями створення безпечного середовища для його дослідження, а також з базовими і поглибленими підходами до статичного, динамічного та поведінкового аналізу. Окрема увага приділяється роботі з пам'яттю заражених систем, інструментам цифрової криміналістики, технікам реверс-інжинірингу та дизасемблювання. Студенти вивчать поширені методи обфускації та ухилення від виявлення, навчаться ідентифікувати індикатори компрометації та формувати аналітичні звіти для реагування на інциденти.
Курс має міждисциплінарний характер і поєднує знання з операційних систем, комп'ютерних мереж, програмування та кібербезпеки. Практичні завдання виконуються у віртуалізованому середовищі із застосуванням сучасних інструментів аналізу (Procmon, Wireshark, IDA Pro, x64dbg, Volatility, YARA тощо).
Результатом опанування курсу є здатність студентів кваліфіковано здійснювати аналіз зразків шкідливого програмного забезпечення, виявляти їхні приховані функції та механізми, а також застосовувати отримані знання у практиці реагування на кіберінциденти.

Мета та цілі дисципліни

Метою дисципліни є формування у студентів знань та практичних навичок з ідентифікації, дослідження та аналізу шкідливого програмного забезпечення, опанування сучасних методів статичного й динамічного аналізу, цифрової криміналістики та реверс-інжинірингу для підвищення рівня кібербезпеки та реагування на інциденти.
Основними завданнями курсу є: ознайомлення з видами, класифікацією та способами поширення шкідливого ПЗ; формування навичок створення та використання безпечного середовища для аналізу; засвоєння методів статичного аналізу виконуваних файлів та бібліотек; вивчення методів динамічного та поведінкового аналізу; опанування інструментів цифрової криміналістики та аналізу пам'яті; вивчення основ реверс-інжинірингу, дизасемблювання та відлагодження; ознайомлення з методами обфускації та ухилення від виявлення; розвиток навичок формування індикаторів компрометації та аналітичних звітів для реагування на кіберінциденти.
Предметом вивчення є шкідливе програмне забезпечення як об'єкт дослідження — його структура, функціональні можливості, техніки приховування та поширення, а також методи і засоби аналізу, які дозволяють ідентифікувати та нейтралізувати загрози у сучасному кіберпросторі.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
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.
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.
КФ3. Здатність досліджувати, розробляти і
супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до
інформаційних ресурсів згідно 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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних
системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну
діяльність, планувати навчання, контролювати і
супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
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.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики 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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
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.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Передумови вивчення дисципліни охоплюють засвоєння знань і навичок з базових курсів інформаційних технологій і кібербезпеки, які створюють фундамент для успішного оволодіння матеріалом. Студент повинен володіти знаннями з операційних систем (Windows, Linux), їх файлових систем та механізмів управління процесами і пам'яттю. Важливими є основи комп'ютерних мереж і протоколів TCP/IP, уміння працювати з мережевими утилітами для моніторингу та аналізу трафіку.
Необхідним є володіння базовим програмуванням (C/C++, Python, скриптові мови) для читання та аналізу вихідного і машинного коду. Потрібні знання з архітектури комп'ютерних систем і принципів роботи апаратного забезпечення. Бажаним є попереднє вивчення дисциплін «Основи інформаційної безпеки», «Криптографічні методи захисту інформації», «Мережеві технології та безпека», «Операційні системи».
Такі пререквізити забезпечують підготовленість студента до роботи з інструментами статичного й динамічного аналізу, цифрової криміналістики, а також до розуміння принципів реверс-інжинірингу та дослідження шкідливого програмного забезпечення.

Особливості дисципліни, методи та технології навчання

У процесі викладання дисципліни використовуються пояснювально-ілюстративний та репродуктивний методи навчання, а також проблемно-пошуковий і дослідницький підхід. Для активізації навчальної діяльності застосовуються практичні лабораторні заняття з використанням спеціалізованого програмного забезпечення (Procmon, Wireshark, IDA Pro, x64dbg, Volatility, Cuckoo Sandbox), інтерактивні презентації, кейс-стаді, групові та індивідуальні проєкти.
Особлива увага приділяється навчанню через практику: аналіз реальних зразків шкідливого ПЗ у контрольованому середовищі, моделювання кіберінцидентів, проведення симуляцій реагування на атаки. Застосовуються майстер-класи та практикуми, орієнтовані на розвиток навичок реверс-інжинірингу, цифрової криміналістики та формування індикаторів компрометації.
У навчанні активно використовуються онлайн-ресурси, зокрема відкриті бази зразків шкідливого ПЗ, ресурси з аналітики загроз (MITRE ATT&CK, VirusTotal, Hybrid Analysis), стандарти ISO/IEC та NIST, а також наукові публікації й технічна документація міжнародних організацій з кібербезпеки.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Класифікація шкідливого програмного забезпечення, правові та етичні аспекти його дослідження. Поняття та класифікація шкідливого ПЗ; методи поширення; правові та етичні аспекти аналізу.	4
Тема 2. Середовище аналізу. Віртуалізація, пісочниці, інструменти безпечного дослідження. Методи створення ізольованого середовища для дослідження ШПЗ, використання віртуальних машин, sandbox-інструментів та засобів забезпечення операційної безпеки.	4
Тема 3. Основи програмування для аналізу ШПЗ. Огляд мов та інструментів, необхідних для реверс-інжинірингу. Розглядаються базові знання програмування на C/C++ та Python, принципи роботи асемблера, необхідні для аналізу виконуваних файлів.	4
Тема 4. Основи статичного аналізу. Структура виконуваних файлів, інструменти та методи первинного дослідження. Вивчення структури PE-файлів, огляд заголовків, імпортованих та експортованих функцій, використання утиліт для первинного аналізу. Застосування дизасемблерів (IDA Pro, Ghidra), створення правил YARA, аналіз коду для виявлення вбудованих алгоритмів і функцій.	4
Тема 5. Основи динамічного аналізу. Методи безпечного виконання, поведінкове спостереження, антидебаг-техніки. Дослідження роботи шкідливого ПЗ у реальному часі, спостереження за системними змінами, виявлення та обходження механізмів протидії аналізу.. Аналіз мережевої активності, системних змін, журналів подій, обходження антиемуляції. Методи моніторингу мережевого трафіку, змін у файловій системі та реєстрі, використання інструментів Wireshark, Procmon, RegShot.	4
Тема 6. Аналіз пам'яті заражених систем. Інструменти цифрової криміналістики, дослідження дампів пам'яті, виявлення rootkit- та stealth-компонентів. Робота з Volatility та Rekall, методи виявлення прихованих процесів, бібліотек та ознак руткітів у пам'яті.	4
Тема 7. Методи обфускації та ухилення від виявлення. Упаковщики, криптори, шифрування та методи їх обходу. Вивчення поширених технік обфускації, аналіз використаних упаковщиків, методи розкриття та відновлення оригінального коду.	4
Тема 8. Аналіз сучасних кіберзагроз. Spyware, ransomware, APT, формування індикаторів компрометації (IoC) та практичне реагування на інциденти. Розгляд актуальних кіберзагроз, приклади атак, побудова індикаторів компрометації, методи реагування на інциденти й створення аналітичних звітів.	4
Загальна кількість годин	**32**

Лабораторні заняття

Аналіз шкідливих програм

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Налаштування безпечного середовища для аналізу шкідливого ПЗ. Створення віртуальної лабораторії, використання віртуалізації та sandbox, ізоляція зразків, базові налаштування інструментів аналізу.	4	1
Тема 2. Первинний статичний аналіз виконуваних файлів. Визначення хешів, робота з утилітами PEview, Detect It Easy, Exeinfo PE; аналіз заголовків, імпортованих та експортованих функцій.	4	1
Тема 3. Використання YARA та сигнатурних методів. Створення власних правил YARA для виявлення зразків; тестування сигнатур; аналіз ефективності пошуку.	4	1
Тема 4. Динамічний аналіз у контрольованому середовищі. Моніторинг процесів, файлової системи та реєстру; використання Procmon, RegShot; виявлення системних змін.	4	1
Тема 5. Складання заявки на патент (корисна модель / винахід) у сфері IT-безпеки. Опис винаходу (сфера застосування, рівень техніки, відмінні ознаки). Формулювання формули корисної моделі. Використання прикладів з практики.	4	1
Тема 6. Аналіз мережевої активності шкідливих програм. Застосування Wireshark, TCPView, Fiddler; виявлення C2-комунікацій; аналіз протоколів і зашифрованого трафіку.	4	1
Тема 7. Аналіз пам'яті заражених систем. Дампування пам'яті зараженої системи; використання Volatility; виявлення прихованих процесів, DLL, мережевих з'єднань.	4	1
Тема 8. Виявлення та обходження методів обфускації. Робота з упаковщиками та криптораами; аналіз шифрованих рядків; техніки декодування та відновлення оригінального коду.	4	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Статичний аналіз шкідливого програмного забезпечення. Поняття та методи статичного аналізу, структура виконуваних файлів, робота з хешами та сигнатурами, створення правил YARA, виявлення прихованої функціональності.	0,5
Тема 2. Динамічний аналіз і поведінкове дослідження шкідливих програм.	0,5

Методи безпечного запуску у віртуальному середовищі, моніторинг системних змін та мережевої активності, виявлення засобів антидебагу та антиемуляції.	
Тема 3. Методи обфускації та протидії виявленню. Упаковщики, криптори, шифрування та декодування даних, практичні методи обходу.	0,5
Тема 4. Сучасні кіберзагрози та індикатори компрометації. Spyware, ransomware, APT, формування індикаторів компрометації (IoC), застосування IoC у практиці реагування на інциденти.	0,5
Загалом	$\sum_{i=1}^{m} b_i = 2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Історія розвитку шкідливого програмного забезпечення: від перших комп'ютерних вірусів до сучасних загроз. Перші комп'ютерні віруси, етапи еволюції загроз, тенденції розвитку сучасних атак.	9
Тема 2. Огляд шкідливого програмного забезпечення для мобільних платформ (Android, iOS), особливості аналізу. Особливості роботи зразків під Android та iOS, методи поширення, інструменти аналізу.	9
Тема 3. Rootkits та bootkits: класифікація, методи приховування активності, сучасні приклади. Механізми приховування в системі, робота на рівні ядра та завантажувача, приклади сучасних руткітів.	9
Тема 4. Безфайлові шкідливі програми (fileless malware): механізми роботи та методи виявлення. Принципи функціонування у пам'яті, використання PowerShell, WMI, макросів, методи виявлення.	9
Тема 5. Інструменти зловмисників для маскування та ухилення (anti-VM, anti-debug, anti-sandbox). Автоматична зміна коду при кожному запуску, техніки обходу сигнатурного аналізу, складності детектування.	9
Тема 6. Архітектура ботнетів: принципи роботи, протоколи керування, способи виявлення. Засоби анти-VM, анти-debug, анти-sandbox, перевірка оточення, уповільнення виконання.	9
Тема 7. Програмне забезпечення для шпигунства (spyware, stalkerware): функціональність, правові аспекти, реальні кейси. Будова керуючої інфраструктури, протоколи C2 (IRC, HTTP, P2P), методи протидії та нейтралізації.	8
Тема 8. Програмне забезпечення для шпигунства (spyware, stalkerware): функціональність, правові аспекти, реальні кейси. Можливості шпигунських програм, збір персональних даних, соціально-правові	8

наслідки, приклади інцидентів.	
Тема 9. Використання MITRE ATT&CK у дослідженні та класифікації шкідливих програм. Структура матриці, використання для класифікації тактик і технік шкідливих програм, приклади практичного застосування.	8
Тема 10. Використання відкритих ресурсів для дослідження шкідливого ПЗ: VirusTotal, Hybrid Analysis, Any.Run, MalwareBazaar. Організації колективного управління (ОКУ) та цифрові реєстри. Захист баз даних авторів і творів. Використання blockchain і smart contracts у системах роялті. Ризики кіберзагроз для ОКУ.	8
Загальна кількість годин	**86**

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 Malware Analysis and Reverse Engineering – Cybrary
https://www.cybrary.it/course/malware-analysis-and-reverse-engineering
Основи статичного та динамічного аналізу, реверс-інжиніринг виконуваних файлів.
2 Malware Analysis and Memory Forensics – Open Security Training
http://opensecuritytraining.info/MalwareAnalysis.html
Поглиблений курс з аналізу пам'яті, методів дослідження шкідливого ПЗ, Volatility Framework.
3 Reverse Engineering Malware – SANS Institute (FOR610)
https://www.sans.org/cyber-security-courses/reverse-engineering-malware/
Один із найавторитетніших курсів у світі з практичними лабораторіями по аналізу зразків.
4 Practical Malware Analysis & Triage – Malware Unicorn (GitHub-курс)
https://malwareunicorn.org/workshops/re101.html
Безкоштовний практичний воркшоп з реверсу й триажу шкідливого ПЗ.
5 Applied Malware Analysis – Udemy
https://www.udemy.com/course/applied-malware-analysis
Застосування інструментів (IDA, Ghidra, Wireshark, Procmon) для аналізу сучасних загроз.
6 Incident Response & Advanced Forensics – EC-Council
https://iclass.eccouncil.org/our-courses/computer-hacking-forensic-investigator-chfi
Методи реагування на інциденти, цифрова криміналістика, аналіз наслідків шкідливого ПЗ.
7 Analyzing Malware for .NET and Java – Pluralsight
https://www.pluralsight.com/courses/malware-analyzing-dotnet-java
Спеціалізований курс із розбору шкідливих програм для платформ .NET і Java.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1 Sharp, R. *Malware*. Technical University of Denmark, 2017. 72 p. [Електронний ресурс]. – Режим доступу: https://orbit.dtu.dk/files/139067614/malware.pdf

2 Mundie, D. A. *The MAL: A Malware Analysis Lexicon*. Carnegie Mellon University, 2013. 39 p. [Електронний ресурс]. – Режим доступу: https://www.sei.cmu.edu/documents/2247/2013_004_001_40250.pdf
3 Kara, I. *A basic malware analysis method*. ResearchGate, 2019. 11 p. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/333834813_A_basic_malware_analysis_method
4 Zhang, H., Wu, J., & Xu, H. *Analyzing PDFs like Binaries: Adversarially Robust PDF Malware Analysis via Intermediate Representation and Language Model*. arXiv preprint, 2025. 18 p. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2506.17162
5 Egele, M., Scholte, T., Kirda, E., & Kruegel, C. *A Survey of Stealth Malware: Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions*. arXiv preprint, 2016. 27 p. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/1603.06028

Додаткова література

8. Tkachuk N., Tkachuk V., Titarchuk A., Khvostenko V. Justification of directions for improving authentication protocols in information and communication systems // Захист інформації. – 2023. – Т. 25, № 1. – С. 60–68. – [Електронний ресурс]. – Режим доступу: https://jrnl.nau.edu.ua/index.php/ZI/article/download/17593/24867
Tkachuk N., Tkachuk V., Stasyuk D., Gosachynskyi S., Khvostenko V. The concept of building security of the network with elements of the semiotic approach // Scientific Journal «Information Security». – 2023. – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/370708289_The_concept_of_building_security_of_the_network_with_elements_of_the_semiotic_approach/fulltext/645e8fb2434e26474fe1327d/The-concept-of-building-security-of-the-network-with-elements-of-the-semiotic-approach.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
0,6	0,4		

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 (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** Станіслав МІЛЕВСЬКИЙ