Силабус освітнього компонента

Програма навчальної дисципліни

Інтернет-розвідка

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж»., гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інтернет-розвідка" є нормативною навчальною дисципліною. Дисципліна спрямована на підвищення рівня формування у студентів знань та умінь, які створять теоретичний і практичний фундамент, необхідний для процесу збору, аналізу та інтерпретації інформації із загальнодоступних джерел для отримання розвідувальних даних та аналітичної інформації.

Мета та цілі дисципліни

Отримання студентами необхідних знань для отримання конкретної інформації про людей, організаціях, продуктах, послугах, подіях і тенденціях через загальнодоступні онлайн-джерела.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

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.
РН4. Вільно спілкуватися державною мовою.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної 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).
РН19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно- комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Фізичні основи технічних засобів розвідки, Цифрова криміналістика.

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 в навчальну дисципліну. Введення в теорію розвідувальної інформації.	4

Характеристики та вимоги до розвідувальної інформації. Джерела та методи отримання інформації.	
Тема 2. Основні принципи ведення розвідки з відкритих джерел. Основні поняття та визначення. Характеристики функцій розвідки при бойових операціях. Вимоги до планування та оцінка процесу збору інформації. Процес прийняття рішень.	4
Тема 3. Планування і підготовка розвідки з відкритих джерел. Планування діяльності OSINT. Підготовка процесу ведення розвідки у відкритих джерелах. Чинники, що впливають на процес планування та підготовки.	4
Тема 4. Збір розвідданих з відкритих джерел. Збір загальнодоступної інформації. Дослідження даних.	2
Тема 5. Проведення розвідки з відкритих джерел. Категорій розвідувальних даних. Аналіз інформації. Процес обробки інформації. Процес надання та розповсюдження інформації. Чинники, що впливають процес надання та розповсюдження.	2
Тема 6. Соціальні онлайн мережі в системі сучасних форматів ведення війни. Сучасна гібридна війна та її відображення у віртуальній реальності. Гібридна війна: структура та базові прийоми. Сучасні інноваційні засоби ведення гібридних війн. Інтернет-технології та соціальні онлайн мережі в структурі гібридної війни.	2
Тема 7. Мережеві онлайн проекти в гібридній війні: структура та принципи функціонування. Формат та специфіка онлайн мережевих проектів. Методи та засоби управління проектами. Медіа-віруси та їх використання в якості інформаційної зброї.	2
Загальна кількість годин	**20**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Використання розширеного пошуку Google. Збір даних з відкритих джерел. Здобувач знайомиться з техніками розширеного пошуку Google (Google Dorks), операторами фільтрації та методами формування точних запитів. Під час виконання роботи здійснюється збір базової інформації з відкритих джерел (OSINT): пошук документів, даних про домени, витоків інформації, цифрових слідів користувачів.	5	0,2
Тема 2. Використання програмного забезпечення Maltego для збору та візуалізації інформації. У лабораторній роботі студенти вивчають можливості Maltego як інструмента для графічного аналізу зв'язків та агрегування даних з багатьох джерел. Проводиться побудова інформаційних графів, пошук зв'язків між доменами, IP-адресами, організаціями, акаунтами в соцмережах тощо.	5	0,2
Тема 3. Збір інформації за допомогою мережевих сканерів Nmap та Nessus. Студент навчиться використовувати Nmap для виявлення	5	0,1

відкритих портів, служб та базової мережевої топології цілей. Після цього застосовується Nessus для робочого аналізу вразливостей та створення звітів. Лабораторна робота формує розуміння методів технічного OSINT і оцінювання безпеки мережевих ресурсів на основі отриманих даних.		
Тема 4. Інформаційні технології для пошуку та аналізу даних із соціальних мереж. Здобувачі освоюють інструменти і методи збору даних із соціальних мереж (Facebook, Instagram, X/Twitter, LinkedIn та інші). Розглядаються сервіси OSINT для аналізу профілів, історії активності, зв'язків та геолокаційних даних.	5	0,1
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи теорії розвідувальної інформації та планування OSINT-операцій. Контрольна робота спрямована на перевірку знань базових понять розвідувальної інформації, її характеристик та джерел. Охоплює основні принципи ведення розвідки з відкритих джерел, особливості планування та фактори, що впливають на успішне проведення OSINT-операцій. Студент повинен продемонструвати розуміння процесів підготовки, аналізу джерел, а також уміння формувати план OSINT-розвідки.	0,2
Тема 2. Методи збору, аналізу та застосування OSINT у контексті сучасних гібридних війн. Контрольна робота охоплює процес збору даних із відкритих джерел, їх класифікацію, аналіз і методи обробки. Особливу увагу приділено ролі соціальних мереж у сучасних війнах, структурі мережевих онлайн-проєктів, поняттю медіа-вірусів та їх використанню як інформаційної зброї. Студент повинен продемонструвати здатність аналізувати інформаційний простір, виявляти ознаки інформаційних операцій та оцінювати їх вплив.	0,2
Загалом	$\sum_{i=1}^{m} b_i = 0{,}4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Методи анонімізації в мережі та інструменти приховування цифрового сліду. Tor, VPN, проксі, браузерні розширення, оперативна безпека (OPSEC).	8
Тема 2. Витоки даних (Data Breaches) та інструменти їх аналізу. Пошук у злитих базах, робота з платформами HaveIBeenPwned, DeHashed, Intelligence X.	8
Тема 3. Аналіз доменів та DNS-структури.	8

WHOIS, DNSdumpster, PTR-запити, пасивний DNS, ідентифікація власників ресурсів.	
Тема 4. Збір метаданих із документів та зображень. EXIF-аналіз, аналіз PDF-структур, визначення авторів, локацій, часу створення файлів.	8
Тема 5. Геолокаційний OSINT: інструменти та методи. Google Earth, Sentinel Hub, GeoGuessr-OSINT техніки, аналіз ландшафтів та тіней.	8
Тема 6. Пошук інформації у даркнеті. Протоколи доступу, каталоги, форуми, безпека роботи, специфіка джерел.	8
Тема 7. Reverse Image Search та аналіз візуального контенту. Google Images, TinEye, Bing Vision, визначення монтажу, первинного джерела та хронології.	8
Тема 8. OSINT-інструменти для аналізу поведінки користувачів у соціальних мережах. Аналіз активності, бот-мережі, фейкові профілі, психологічні патерни взаємодії.	8
Тема 9. Використання штучного інтелекту в OSINT-дослідженнях. Моделі обробки тексту, автоматизація моніторингу, класифікація даних.	8
Тема 10. Основи інформаційних операцій та методи їх ідентифікації. Дезінформаційні кампанії, психологічні впливи, алгоритми поширення контенту.	8
Загальна кількість годин	**80**

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.Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с.
http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf

2. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.
https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0052980.pdf

Додаткова література

1. Гібридна війна: сутність, виклики та загрози: зб. матер. круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 189 с.

https://nasbu.edu.ua/uploads/p_57_28744724.pdf
2. Open Source Intelligence Methods and Tools [Електронний ресурс]. – Режим доступу: https://osint.link/osint-book/
3. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/ research_reports/RR1964.html
4. National defense authorization act for fiscal year 2006. URL: http://www.dod.gov/dodgc/olc/docs/PL109-163.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** Роман КОРОЛЬОВ