Силабус освітнього компонента
Програма навчальної дисципліни

Інтернет-розвідка

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджанс» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: «Нейронні мережі", "Моделювання систем інформаційної безпеки", "Штучний інтелект і бізнес-аналітика", "Стандартизація та сертифікація в галузі інформаційної безпеки" та інших у студентів бакалавріата та магістратури.
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 роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ФК-2. Здатність аналізувати та визначати політику та
стратегії забезпечення захисту інформації.

Результати навчання

ПРН–3. 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.
ПРН-4. Вільно спілкуватися державною мовою.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН–10. 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).
ПРН–19. 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.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно- комунікаційних систем.
ПРН-22. 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 – 36 год., лабораторні роботи – 24 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Організація документообігу з обмеженим доступом, Математичні основи криптології та криптоаналіз, Фізичні основи технічних засобів розвідки.

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

Теми лекційних занять

Тема 1. Вступ в навчальну дисципліну. Введення в теорію розвідувальної інформації.
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.
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.
Тема 4. Збір розвідданих з відкритих джерел.
Збір загальнодоступної інформації. Дослідження даних.
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.
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.
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.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Використання розширеного пошуку Google. Збір даних з відкритих джерел.
Тема 2. Використання програмного забезпечення по збору інформації Maltego.
Тема 3. Збір інформації за рахунок використання мережевих сканерів Nmap та Nessus.
Тема 4. Інформаційні технології для пошуку та аналізу даних з соціальних мереж.

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.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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•іспит: 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
Роман КОРОЛЬОВ