Силабус освітнього компонента
Програма навчальної дисципліни

Теорія та методи соціальної інженерії в кібербезпеці

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Магістр

Тип дисципліни
Профільна, Вибіркова

Семестр
1

Мова викладання
Українська

Викладачі, розробники

Євсеєв Сергій Петрович
serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Теорія та методи соціальної інженерії в кібербезпеці" є вибірковою навчальною дисципліною. Дисципліна спрямована на набуття студентом теоретичних знань та практичних навичок щодо основи соціальної інженерії у сфері кіберзахисту.

Мета та цілі дисципліни

Засвоєння принципів використання методів соціальної інженерії. Отримання знань та умінь необхідних для успішної боротьби з атаками, які використовують методи соціальної інженерії.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК 3. Здатність до безперервного навчання, придбання нових знань і умінь, у тому числі в галузі, відмінній від професійної.
ЗК 4. Здатність виявляти, ставити та вирішувати проблеми у професійній діяльності.
ЗК 5. Здатність генерувати нові ідеї (креативність) і нестандартні підходи до їхньої реалізації, гнучке адаптування до реальних професійних ситуацій, проявляти творчий підхід, ініціативу.
ЗК 6. Здатність критично оцінювати й переосмислювати накопичений досвід (власний і чужий), аналізувати свою професійну і соціальну діяльність.
ЗК 7. Здатність працювати з інформацією: знаходити і використовувати інформацію з різних джерел, потрібну для розв'язання професійних завдань.
ЗК 11. Здатність до соціальної і професійної взаємодії та співпраці у колективі, командної роботи.
СК 1. Здатність формулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, перевіряти коректність постановки, у тому числі в умовах невизначеності.
СК 3. Здатність обирати, розробляти, досліджувати та застосовувати математичні методи для розв'язання практичних задач моделювання, проектування, керування, прогнозування, прийняття рішень.
СК 7. Здатність до пошуку, вивчення та аналізу науково-технічної інформації, вітчизняного і закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження процесів та систем.
СК 13. Здатність до розробки та експлуатації спеціалізованих програмних засобів обробки великих масивів даних на основі інформаційних технологій розподілених і хмарних обчислень.
СК 14. Здатність до використання сучасних інформаційних технологій інтелектуального аналізу даних, прогнозування, прийняття рішень, інформаційного пошуку і видобування знань.

Результати навчання

РН 1. Демонструвати знання і розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці.
РН 2. Уміти формалізувати задачі, сформульовані мовою певної предметної галузі й обирати раціональний метод вирішення; розв'язувати задачі аналітичними або чисельними методами, оцінювати точність і достовірність отриманих результатів та виконувати їхню інтерпретацію.
РН 4. Уміти поєднувати методи математичного і комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.
РН 7. Уміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.
РН 8. Уміти застосовувати у практичній роботі спеціалізовані програмні продукти і програмні системи комп'ютерної математики, аналізу великих даних тощо.
РН 13. Знати і розуміти методи розв'язання математичних задач інтелектуального інформаційного пошуку та видобування знань.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Бакалаврський рівень підготовки.

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. Деструктивні методи соціальної інженерії як фактор загрози інформаційної безпеки.
Сутність соціальної інженерії. Розуміння поведінки людей. Розробка стратегій впливу. Виявлення вразливостей. Підходи до визначення сутності соціальної інженерії. Філософія соціального проектування: кардинальні ідеї і положення. Принципи соціальної інженерії. Деструктивні аспекти методів соціальної інженерії. Загрози безпеки, пов'язані з електронною поштою і з використанням служби миттєвого обміну повідомленнями. Вторгнення і заходи протидії. Фішинг (цільовий Фішинг). Плечовий серфінг. Троянська програма. Зворотна соціальна інженерія. Аналіз і попередження обману методами соціальної інженерії.
Тема 2. Історія та еволюція соціальної інженерії.
Розвідка з відкритих джерел. Сфери застосування концепції OSINT. Психологічні концепції у соціальній інженерії. Шість принципів впливу доктора Чалдіні.
Тема 3. Етика соціальної інженерії: відповідальність та суспільні наслідки.
Етична відповідальність у соціальній інженерії та її основні принципи. Суспільні наслідки недостатньої етичної уваги при використанні соціальної інженерії. Кроки для зменшення можливих негативних впливів соціальної інженерії на приватність та безпеку індивідів. Культурні та етичні відмінності при застосуванні соціальної інженерії в різних частинах світу. Розуміння юридичних аспектів. Етичні рамки OSINT. Загальне положення про захист даних (GDPR). Збір даних від імені правоохоронних органів. Збір даних як приватних осіб.
Тема 4. Психологія маніпуляції та впливу на людей.
Психологічні механізми для маніпуляції і впливу на інших людей. Різниця між здоровим впливом і маніпуляцію в міжособистих відносинах. Практичні стратегії для захисту від маніпуляції та негативного впливу. Основні фактори і властивості особистості людей більш схильних до маніпуляції. Емоційна та соціальна інтелігенції. Підготовка до атаки. Використання спеціалізованих ОС для соціальної інженерії. Послідовні фази атаки на основі загроз соціальної інженерії. Цикл спостереження-орієнтації-рішення-дії (НОРД) для збору даних OSINT.
Тема 5. Вплив соціальної інженерії на суспільний вибір та політичні процеси.
Вплив соціальної інженерії на сприйняття суспільством політичної інформації та новин. Інструменти соціальної інженерії для маніпулювання суспільним вибором. Захист суспільства від негативного впливу соціальної інженерії на політичні процеси. Вплив соціальної інженерії на формування політичних поглядів та переконань громадян.
Тема 6. Соціальна інженерія в сфері кібербезпеки: фішинг та соціальний інженеринг.
Основні види фішингу. Використання соціального інженеринга в атаках на кібербезпеку. Основні техніки соціального інженерингу.
Тема 7. Вплив соціальної інженерії на суспільний вибір та політичні процеси.
Вплив соціальної інженерії на суспільний вибір під час виборів та референдумів. Методи соціальної інженерії для маніпулювання політичною інформацією та формування громадської думки. Використання соціальної інженерії для поширення дезінформації та фейкових новин у політичних процесах. Захист суспільства від негативного впливу соціальної інженерії на політичні процеси та суспільний вибір.
Тема 8. Метод прогнозування оцінки соціального впливу у регіональних спільнотах.
Оцінка сумарної інтенсивності впливу тієї чи іншої інституційної структури. Оцінка прогнозування рейтингу політичних сил, що базується на механізмі соціального впливу.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Визначення фішингових атак з використанням Netcraft.
Тема 2. Визначення фішингових атак з використанням PhishTank.
Тема 3. Отримання особистих даних для доступу до соціальних мереж з використанням Social Engineering Toolkit (SET).

Тема 4. Створення зловмисного навантаження використовуючи SET та експлуатація Windows-машини.
Тема 5. Дослідження методу прогнозування оцінки соціального впливу у регіональних спільнотах.

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 та іспиту.

Література та навчальні матеріали

Основна література

1. Ozkaya, Erdal. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd, 2018. – 557 p. – ISBN-10 1788837924. – ISBN-13 978-1788837927.
2. Alexander, Michael; Wanner, R. Methods for understanding and reducing social engineering attacks. SANS Inst., 2016, 1: 1-32.
https://www.giac.org/paper/gccc/270/methods-understanding-reducing-social-engineering-attacks/147205
3. Грищук Р. В., Даник Ю. Г. Основи кібербезпеки: монографія / відп. ред. проф. Ю. Г. Даник, Житомир : ЖНАЕУ, 2016. – 636 с.
4. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 – 330 p.
https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf
5. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information Paperback – 2021. – 666 p. – ISBN-10 1530508908. – ISBN-13 978-1530508907.
6. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p. – ISBN-13 979-8668892228.
7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа /.– Львів: «Магнолія», 2018. – 320 с.
https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf
8. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
https://doi.org/10.15587/978-617-7319-57-2

Додаткова література

9. Serhii Yevseiev, Yurii Ryabukha, Oleksandr Milov, Stanislav Milevskyi, Serhii Pohasii, Yevheniia Ivanchenko, Ihor Ivanchenko, Yevgen Melenti, Ivan Opirskyy, Igor Pasko. Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies. 2021. 6/2 (114). P. 30–47.
https://doi.org/10.15587/1729-4061.2021.249313

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	Дата погодження, підпис 31.08.2023 р.		Завідувач кафедри Сергій ЄВСЕЄВ
	Дата погодження, підпис 31.08.2023 р.		Гарант ОП Олексій ГАЛУЗА