Силабус освітнього компонента
Програма навчальної дисципліни

Поведінкова кібербезпека

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (освітньо-науковий)

Тип дисципліни
Вибіркова,

Семестр
3

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

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор більше 30 публікацій: з них 3 монографії у співавторстві 1 посібник з грифом. Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Вивчення дисципліни спрямовано на формування світогляду, розвитку інтелекту, ерудиції, формування професійних компетенцій зі спеціальності кібербезпека; оволодіння методологією наукової діяльності, теоретичними основами сучасних комп'ютерних методів наукових досліджень та інтелектуальних технологій аналітичної інформації.

Мета та цілі дисципліни

Отримання знань з аналізу різних видів діяльності осіб в системах кібербезпеки, та психологічних концепцій, покладених в основу соціальної інженерії, а також навичок проведення атак з використанням соціальної інженерії та методів захисту від атак соціальної інженерії та методів відновлення після подібних атак.

Формат занять

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

Компетентності

ЗК-1.Здатність до професійного спілкування іноземною мовою.
ЗК-3. Здатність до виявлення, генерування нових ідей, дослідження та вирішення проблем за професійним спрямуванням.

Результати навчання

РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.
РН-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

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)

Математичні основи криптології, Введення в мережі, Цифрова криміналістика.

Особливості дисципліни, методи та технології навчання

Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальною та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Що таке поведінкова кібербезпека?
Важливі поняття поведінкової кібербезпеки (предлог, розвідка з відкритих джерел, фішинг, цільовий фішинг, вейлінг, вішинг, приманка, сміттєві баки).
Тема 2. Етичні міркування у поведінковій кібербезпеці.
Етична поведінкова кібербезпека (дотримання кордонів, розуміння юридичних аспектів, особливості надання послуг третьої сторони, підбиття підсумків після вторгнення). Етичні рамки

OSINT (захист даних, дотримання законів та правил). Етичні обмеження поведінкової кібербезпеки.

Тема 3. Підготовка до атаки.

Погодження з клієнтом. Ознайомлення із завданням, Визначення цілей. Визначення методів. Розробка вдалих прийменників. Використання спеціалізованих ОС для кібербезпеки поведінки. Послідовні фази атаки.

Тема 4. Бізнес-розвідка з відкритих джерел.

Значення OSINT. Типи OSINT. Збір даних OSINT про організацію. Отримання базової бізнес-інформації із Crunchbase. Ідентифікація власників веб-сайтів за допомогою WHOIS. Збір OSINT із командного рядка за допомогою Recon-ng.

Тема 5. Соціальні медіа та публічні документи.

Аналіз соціальних мереж для збору OSINT (LinkedIn, Дошки оголошень та кар'єрні сайти, Facebook (Meta), Instagram). Використання Shodan для OSINT (використання параметрів пошуку Shodan, пошук IP-адрес, пошук доменних імен, пошук імен хостів та субдоменів). Автоматичні скріншоти за допомогою Hunchly.

Тема 6. Збір OSINT про людей.

Використання інструментів OSINT для аналізу адрес електронної пошти (з'ясування того, чи був зламаний користувач, складання списку облікових записів соціальних мереж за допомогою Sherlock). Складання списку облікових записів веб-сайтів за допомогою WhatsMyName. Аналіз паролів за допомогою Pwdlogy. Аналіз зображень мети (ручний аналіз даних EXIF, аналіз зображень з допомогою ExifTool).

Тема 7. Фішинг та інструменти керування електронною поштою.

Налаштування фішингової атаки (налаштування захищеного екземпляра VPS для фішингових цільових сторінок, вибір платформи електронної пошти). Купівля доменів для розсилки та цільових сторінок. Налаштування інфраструктури фішингу та веб-сервера. Додаткові дії для успішного фішингу (використання пікселів відстеження, автоматизація фішингу за допомогою Gophish, додавання підтримки HTTPS для фішингових цільових сторінок, використання скорочених URL-адрес у фішингу, використання SpoofCard для спуфінгу дзвінків). Угода про термін проведення атаки. Стандарти (поля «Від кого», стандарт DKIM, інфраструктура політики відправника, автентифікація повідомлень на основі домену, звітність та відповідність). Рівень TLS шифрування. MTA-STS. TLS-RPT. Технологія фільтрації електронної пошти. Інші засоби захисту.

Тема 8. Клонування цільової сторінки.

Приклад клонованого сайту (сторінка входу, сторінка критичних питань). Клонування веб-сайту (пошук сторінок входу та профілю користувача, клонування сторінок за допомогою HTTrack, зміна коду поля входу, додавання веб-сторінок на сервер Apache).

Тема 9. Виявлення, вимірювання та звітність. Методи виявлення загроз.

Виявлення. Вимірювання (вибір показників, відносини, медіани, середні значення та стандартні відхилення, кількість відкриттів листів електронної пошти, кількість переходів, введення інформації у форми, дії жертви, час виявлення, своєчасність коригуючих дій, ефективність дій у відповідь, кількісна оцінка ризику). Складання звітів. Використання Alien Labs OTX. Аналіз фішингового листа в OTX (створення імпульсу, аналіз джерела електронної пошти, введення індикаторів, тестування потенційно шкідливого домену в Burp, аналіз файлів, що завантажуються). Проведення OSINT для аналізу загроз (пошук у базі VirusTotal, виявлення шкідливих сайтів у WHOIS, виявлення фішингу за допомогою PhishTank, перегляд ThreatCrowd, консолідація інформації у ThreatMiner).

Тема 10. Випереджальні засоби захисту.

Програми підвищення обізнаності (як і коли проводити навчання, некаральна політика, заохочення за хорошу поведінку, проведення фішингових кампаній). Репутація та OSINT-моніторинг (реалізація програми моніторингу, аутсорсинг). Реагування на інциденти (процес реагування на інциденти за версією SANS, реагування на фішинг, реагування на вішинг, реагування на збір OSINT, управління увагою ЗМІ, як користувачі повинні повідомляти про інциденти, технічний контроль та ізоляція).

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Виявлення фішингу за допомогою Netcraft.
Тема 2. Виявлення фішингу за допомогою PhishTank.
Тема 3. Тестування на проникнення соціальної інженерії з використанням інструментарію соціальної інженерії (SET).
Тема 4. Збір даних OSINT про організацію. Отримання базової бізнес-інформації із Crunchbase.
Тема 5. Аналіз соціальних мереж без інструментів (LinkedIn, Instagram, Facebook, Twitter).
Тема 6. Аналіз соціальних мереж без інструментів (LinkedIn, Instagram, Facebook, Twitter).

Самостійна робота

Самостійна робота аспіранта є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам 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. URL: https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf
2. Joe Gray. Practical Social Engineering. A Primer for the Ethical Hacker // No Strach Press, 2022, 230 pp. URL: https://books.google.com.ua/books/about/Practical_Social_Engineering.html?id=DtOQEAAAQBAJ&redir_esc=y
3. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с. ГКДж https://drive.google.com/file/d/1694khGjEN1-2PvXFQY27IPPc8Sn4BsLC/view?usp=sharing

Додаткова література

4. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010. URL: https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
6. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. URL: https://drive.google.com/file/d/1xVAWLoZMLes_XiXEd7E_6KT-QA4w2Hw7/view?usp=sharing.
7. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: http://monograph.com.ua/pctc/catalog/view/64/52/231-1
8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
9. 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. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

10. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с. URL: https://drive.google.com/file/d/1s4hIVxbj0a-c9Bw4eFMoK66hqLLjwWPr/view?usp=sharing
11. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с. URL: https://drive.google.com/file/d/14fS7nVtD3xieqA8f_rFBiiqcr96_piTe/view?usp=sharing

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

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

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

28.08.2024 — Завідувач кафедри Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП Олександр МІЛОВ