Силабус освітнього компонента
Програма навчальної дисципліни

Основи соціальної інженерії

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
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
3

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

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

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

ВОРОПАЙ Наталя Ігорівна

voropay.n@gmail.com
Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 30 наукових та навчально-методичних праць.. Провідний лектор з дисциплін: «Технології програмування Ч.1», «Децентралізовані системи», «Захист об´єктів критичної інфраструктури» , «Антивірусний захист інформації», «Блокчейн та смарт-технології в електронному документообігу».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи соціальної інженерії" є обов'язковою 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 заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

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)

Основи гуманітарно-філософських знань у професійній діяльності, Інформаційна безпека держави.

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. 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.	2
Тема 2. Історія та еволюція соціальної інженерії. Розвідка з відкритих джерел. Сфери застосування концепції OSINT.	2

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.	2
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.	2
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.	2
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.	2
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.	2
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.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Визначення фішингових атак з використанням	7	0,1

Netcraft. Поняття та види фішингових атак. Інструменти сервісу Netcraft для виявлення фішингових сайтів. Практичні приклади перевірки підозрілих доменів. Методи захисту від фішингу за допомогою Netcraft.		
Тема 2. Визначення фішингових атак з використанням PhishTank. Огляд проєкту PhishTank та його призначення. Механізми виявлення фішингових ресурсів у PhishTank. Практичне використання бази даних фішингових URL-адрес. Порівняння ефективності PhishTank і Netcraft.	7	0,1
Тема 3. Отримання особистих даних для доступу до соціальних мереж з використанням Social Engineering Toolkit (SET). Огляд Social Engineering Toolkit та його можливостей. Техніки збору облікових даних користувачів. Використання фішингових сторінок у SET. Етичні аспекти використання SET у навчальних цілях.	6	0,1
Тема 4. Створення зловмисного навантаження використовуючи SET та експлуатація Windows-машини. Генерація payload у SET. Види атак на Windows-системи. Практичне тестування експлойтів. Методи протидії атакам та безпечна конфігурація Windows.	6	0,1
Тема 5. Дослідження методу прогнозування оцінки соціального впливу у регіональних спільнотах. Соціальна інженерія як інструмент впливу на суспільство. Методи прогнозування соціальної поведінки та впливу. Аналіз даних з відкритих джерел (OSINT). Використання прогнозування для протидії маніпуляціям у соцмережах.	6	0,2
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i$=0,6

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Topic 1. Methods of detection and analysis of phishing attacks. The concept of phishing and its varieties. Using Netcraft and PhishTank tools to identify phishing resources. Comparison of the effectiveness of different services in the fight against phishing. Examples of modern phishing attacks and methods of their prevention.	0,1
Topic 2. Tools of social engineering: SET, exploits and protection methods. Features of the Social Engineering Toolkit (SET). Methods of collecting personal data through phishing pages. Creating and using a malicious load (payload) for attacks on Windows systems. Countermeasures against social engineering attacks.	0,1
Topic 3. Analysis of psychological methods of manipulation in social engineering and countermeasures. Psychological foundations of social engineering. Using trust, fear and urgency in attacks. Examples of real incidents. Recommendations and methods for increasing user awareness.	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. Історія розвитку соціальної інженерії та відомі кейси атак. Витоки соціальної інженерії у кіберпросторі. Відомі приклади зламу організацій за допомогою людського фактору. Аналіз найбільш резонансних атак XXI століття.	5
Тема 2. Соціальна інженерія у кібербезпеці: психологічні аспекти впливу. Основні принципи психологічного маніпулювання. Методи впливу на довіру користувачів. Використання страху, терміновості та авторитету.	5
Тема 3. Класифікація методів соціальної інженерії. Фішинг (email, сайти-клони). Вішинг (телефонні дзвінки). Смішинг (SMS-повідомлення). Shoulder surfing та dumpster diving.	5
Тема 4. Фішинг у соціальних мережах. Підроблені акаунти та сторінки. Використання соціальних мереж для масових атак. Захист облікових записів.	5
Тема 5. Соціальна інженерія у корпоративному середовищі. Атаки на співробітників (внутрішні загрози). Spear-phishing (цільові атаки). Використання LinkedIn та інших бізнес-мереж для збору даних.	5
Тема 6. Техніка «pretexting» (вигаданий привід). Сутність pretexting та його приклади. Психологічні тригери довіри. Відомі кейси використання pretexting у компаніях.	5
Тема 7. Використання методів OSINT у соціальній інженерії. Основні інструменти OSINT (Maltego, Shodan, Recon-ng). Методи збору відкритої інформації. Приклади практичного застосування для атак.	5
Тема 8. Соціальна інженерія в телефонних та email-атаках. Техніки телефонного шахрайства. Email-атаки та підробка адрес відправника. Методи фільтрації та захисту.	5
Тема 9. Аналіз відомих випадків зламу великих компаній за допомогою соціальної інженерії. Аналіз атаки на Twitter (2020). Використання соціальної інженерії в атаці на Google і Facebook. Lessons learned – які помилки допустили жертви.	5
Тема 10. Методи захисту від соціальної інженерії. Навчання персоналу. Використання багатофакторної автентифікації. Політики безпеки та тренінги.	5
Тема 11. Психологія довіри: чому жертви піддаються маніпуляціям. Чому люди схильні до маніпуляцій. Основні «гачки» соціальних інженерів. Методи протидії психологічному впливу.	5
Тема 12. Етика та правові аспекти соціальної інженерії. Етичний хакинг vs злочинна діяльність. Законодавчі норми України та ЄС. Використання соціальної інженерії у тестуванні безпеки.	5
Тема 13. Сценарії атак зі шкідливими вкладеннями. Використання PDF, DOCX, XLSX як інструментів атак. Приховані макроси та	4

експлойти. Методи виявлення та запобігання.	
Тема 14. Використання ШІ у соціоінженерних атаках. Deepfake як інструмент маніпуляції. ChatGPT та інші генеративні моделі у фішингу. Автоматизація атак за допомогою ШІ.	4
Тема 15. Захист персональних даних як елемент протидії. Основні правила кібергігієни. GDPR та захист даних у ЄС. Практичні методи обмеження витоку інформації.	4
Загальна кількість годин	**72**

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. Онлайн-курс CISCO «Cybersecurity Essentials»
https://www.netacad.com/courses/cybersecurity-essentials/1000?courseLang=en-US

Література, навчальні матеріали та інформаційні ресурси

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.
https://h.twirpx.link/file/2523887/
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. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с.
https://kr-labs.com.ua/books/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8+%D1%82%D0%B0+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8_+%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA..PDF
4. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 - 330 p.
http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf
5. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information Paperback – 2021- 666 p.
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.
https://books.google.com.ua/books/about/Ethical_Hacking.html?id=7D3AzQEACAAJ&redir_esc=y
7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: [Підручник] В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа /. – Львів: "Магнолія 2006", 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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.

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	F

(потрібне повторне вивчення)

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** Сергій ЄВСЕЄВ