



Силабус освітнього компонента Програма навчальної дисципліни



Основи соціальної інженерії

Шифр та назва спеціальності

K4 – 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

3

Мова викладання

Українська

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 статей 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

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

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.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

PH12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

PH13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

PH16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

PH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

PH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. 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 – 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 проекти, 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. Психологічні концепції у соціальній інженерії. Шість принципів впливу доктора	2

Тема 3. Етика соціальної інженерії: відповідальність та суспільні наслідки.			2
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.			2
Психологічні механізми для маніпуляції і впливу на інших людей. Різниця між здоровим впливом і маніпуляцією 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 інтелекції. 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.			2
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.			2
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.			2
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.			2
Оцінка сумарної інтенсивності впливу тієї чи іншої інституційної структури. Оцінка прогнозування рейтингу політичних сил, що базується на механізмі соціального впливу.			
Загальна кількість годин			16
Лабораторні заняття			
Теми лабораторних занять		Кількість годин	Вагові коефіцієнти α
Тема 1. Визначення фішингових атак з використанням Netcraft.		7	0,1

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
Тема 1. Методи виявлення та аналізу фішингових атак. Поняття фішингу та його різновиди. Використання інструментів Netcraft та PhishTank для ідентифікації фішингових ресурсів. Порівняння ефективності різних сервісів у боротьбі з фішингом. Приклади сучасних фішингових атак та методів їх запобігання.	0,1
Тема 2. Інструменти соціальної інженерії: SET, експлойти та методи захисту. Можливості Social Engineering Toolkit (SET). Методи збору персональних даних через фішингові сторінки. Створення та використання шкідливого навантаження (payload) для атак на Windows-системи. Заходи протидії атакам соціальної інженерії.	0,1
Тема 3. Аналіз психологічних прийомів маніпуляції в соціальній інженерії та методи протидії. Психологічні основи соціальної інженерії. Використання довіри, страху та терміновості в атаках. Приклади реальних інцидентів. Рекомендації та методи підвищення обізнаності користувачів.	0,2

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 хакінг vs злочинна діяльність. Законодавчі норми України та ЄС. Використання соціальної інженерії у тестуванні безпеки.	5
Тема 13. Сценарії атак зі шкідливими вкладеннями.	4

Використання PDF, DOCX, XLSX як інструментів атак. Приховані макроси та експлойти. Методи виявлення та запобігання.

Тема 14. Використання ШІ у соціоінженерних атаках.

4

Deepfake як інструмент маніпуляції. ChatGPT та інші генеративні моделі у фішингу. Автоматизація атак за допомогою ШІ.

Тема 15. Захист персональних даних як елемент протидії.

4

Основні правила кібергігієни. GDPR та захист даних у ЄС. Практичні методи обмеження витоку інформації.

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-](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)

[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](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 Opirskyi, 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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I , ...))

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 O 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

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