



Силабус освітнього компонента Програма навчальної дисципліни



Основи соціальної інженерії

Шифр та назва спеціальності

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Національна безпека у сфері кіберзахисту

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

3

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](#)



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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

КЗ-9. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.

ФК-2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

ФК-11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

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-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

ПРН-8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ПРН-10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

ПРН-12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.

ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.

ПРН-17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

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.

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

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. Втручання 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 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 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, 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. 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%B)

[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%B](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%B)

[E%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-GBG006AnvjQHU1SdBl3xCaUju>

Додаткова література :

1. Serhii Yevseiev, Yurii Ryabukha, Oleksandr Milov, Stanislav Milevskiy, 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

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;
- залік: 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

Андрій ТКАЧОВ