Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра системного проєктування

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Освітня програма	Інтелектуальні сервіс-орієнтовані розподілені обчислювання
Статус дисципліни	Нормативна
Форма навчання	очна(денна)/дистанційна/змішана
Рік підготовки, семестр	4 курс, осінній семестр
Обсяг дисципліни	105 годин/3.5 кредити ЄКТС: лекції – 36 г., лабораторні – 18 г., СРС – 51 г.
Семестровий контроль/ контрольні заходи	Залік / модульна контрольна робота
Розклад занять	
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: к.т.н. Кирюша Богдан Анатолійович, bogdankyrysha@gmail.com Лабораторні: ас. Яременко В.С.
Розміщення курсу	https://ecampus.kpi.ua

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Основна мета курсу – ознайомлення студентів з найбільш поширеними погрозами безпеці використання інформаційних систем та сучасними методами та засобами боротьби з ними. Розглядаються криптографічні методи і засоби закриття інформації та їх реалізація з використанням симетричних і асиметричних криптосистеми. Основні класи сучасних симетричних криптосистем. Загальні відомості про блокові шифри. Алгоритми блокового шифрування. Алгоритми DES і AES та їх модифікації. Режими використання блокових шифрів. Принципи побудови та реалізація криптографічних асиметричних систем шифрування. Криптографічні хеш-функції та їх використання для ідентифікації блоків даних в пошукових системах, перевірки цілісності файлів, захисту паролів, побудови кодів аутентифікації. Технології та засоби захисту документів з використанням цифрових підписів в системах електронного документообігу. Комп'ютерна стеганографія в системах безпеки інформаційних технологій, захисту авторських прав на програмні і мультимедійні продукти з допомогою цифрових водяних знаків. Методи та засоби ідентифікації та аутентифікації користувачів в системах безпеки інформаційних систем. Метою кредитного модуля є формування у студентів здатностей: – аналізувати науково-технічну, природничо-наукову та загально наукову інформацію в галузі комп'ютерних наук та інформаційних технологій, пов'язану з безпекою використання інформаційних технологій та систем; – користуватися сучасними методами та засобами боротьби з погрозами інформаційній безпеці в сучасних інформаційних технологіях і системах;. – ефективного застосування методів та засобів боротьби з погрозами інформаційній безпеці при розробці та впровадженні сучасних інформаційних систем і технологій. Студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

• знання найбільш поширених погроз безпеці використання інформаційних технологій, криптографічні методи та засоби закриття інформації, технології та засоби захисту документів з використанням цифрових підписів в системах електронного документообігу, захисту авторських прав на програмні і мультимедійні продукти з допомогою цифрових водяних знаків, методи та засоби ідентифікації та аутентифікації користувачів в системах безпеки інформаційних систем;

• уміння роботи з програмними та апаратно-програмними засобами захисту інформаційних систем від несанкціонованого доступу до інформаційних ресурсів ;

• досвід застосування сучасних засобів підвищення рівня безпеки при використанні інформаційних систем.

Згідно з вимогами освітньо-професійної програми, засвоєння навчальної дисципліни забезпечує оволодіння здобувачами вищої освіти такими компетентностями та програмними результатами навчання:

Загальні компетентності:

ЗК 2 Здатність застосовувати знання у практичних ситуаціях.

Фахові компетентності спеціальності:

ФК 14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Програмні результати навчання:

ПРН 16 Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Забезпечуючи дисципліни: «Архітектура обчислювальних систем», «Проектування та аналіз обчислювальних алгоритмів», «Дискретна математика», «Алгоритми та структури даних», «Технології створення програмних сервісів», «Операційні системи».

3. Зміст навчальної дисципліни

Тема 1 Мета та завдання курсу, його структура, зміст та методичні. рекомендації по вивченню, терміни, означення, основні поняття інформаційної безпеки.

Тема 2 Погрози інформаційній безпеці.

Тема 3 Криптографічні методи та засоби безпеки інформаційних систем.

Тема 4 Симетричні криптосистеми.

Тема 5 Асиметричні криптосистеми.

Тема 6 Криптографічні хеш-функції.

Тема 7 Цифрові підписи в системах електронного документообігу.

Тема 8 Комп’ютерна стеганографія в системах безпеки інформаційних систем.

Тема 9 Аутентифікація об’єктів в системах безпеки інформаційних технологій.

4. Навчальні матеріали та ресурси

Базова література:

1. Корченко О. Г. Прикладна криптологія: системи шифрування / В. П. Сіденко, Ю. О. Дрейс. — К.: ДУТ, 2014. – 448 с.
2. Яковенко Є. Інформаційна безпека/ Горбатий І., Бондарєв А., Львівська політехніка: 2019. — 567с.

Додаткова література:

1. Безпека інформаційних систем і технологій: Навч. посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.
2. Корченко О. Г. Охорона конфіденційної інформації підприємства : Навч. посіб. / О. Г. Корченко, Ю. О. Дрейс. – Житомир: ЖВІ НАУ, 2011. – 172 с.
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.
4. Математичні основи криптоаналізу : Навч. посіб. / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов. – Д.: Національний гірничий університет, 2010. – 465 с.: іл.
5. Стеганографія: Навч. посіб. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 232 с.
6. Honeynet project. https://www.honeynet.org/
7. Labrea: “Sticky” honeypot and ids. http://labrea.sourceforge.net/labrea-info.html
8. National vulnerability database. https://nvd.nist.gov/
9. Openvas. http://www.openvas.org/
10. Deraison, R.: The Nessus project. http://www.nessus.org
11. Almeshekah, M.H.: Using deception to enhance security: a taxonomy, model, andnovel uses. Ph.D. dissertation, Purdue University (2015)
12. Chatterjee, S.: Dragon: a framework for computing preferred defense policies from logical attack graphs. Ph.D. dissertation, Iowa State University (2014)
13. Cohen, F.: Deception tool kit. http://all.net/dtk/
14. Durkota, K., Lis`y, V., Bo˘sansk`y, B., Kiekintveld, C.: Optimal network security hardening using attack graph games. In: Proceedings of IJCAI, pp. 7–14 (2015)
15. Huber, K.E.: Host-based systemic network obfuscation system for windows. Technical report, DTIC Document (2011)
16. Khaitan, S., Raheja, S.: Finding optimal attack path using attack graphs: a survey. Int. J. Soft Comput. Eng. 1(3), 2231–2307 (2011)
17. Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., Tambe, M.: Stackelberg vs. nash in security games: an extended investigation of interchangeability, equivalence, and uniqueness. J. Artif. Intell. Res. (JAIR) 41, 297–327 (2011)
18. Manshaei, M.H., Zhu, Q., Alpcan, T., Bac¸sar, T., Hubaux, J.-P.: Game theory meets network security and privacy. ACM Comput. Surv. (CSUR) 45(3), 25 (2013)
19. Murphy, S., McDonald, T., Mills, R.: An application of deception in cyberspace: Operating system obfuscation1. In: International Conference on Information Warfare and Security, p. 241. Academic Conferences International Limited (2010)
20. Sarraute, C., Buffet, O., Hoffmann, J.: POMDPs make better hackers: accounting for uncertainty in penetration testing. arXiv preprint arXiv:1307.8182 (2013)

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, завдання на СРС з посиланням на літературу)
1	Тема 1. Вступ. Лекція 1.

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, завдання на СРС з посиланням на літературу)
	Мета та завдання курсу, його структура, зміст та методичні рекомендації по вивченню, терміни, означення, основні поняття безпеки інформаційних технологій. Критерії інформаційної безпеки. Основні категорії моделі інформаційної безпеки: конфіденційність, цілісність, доступність, аутентичність, апельованість. Методи та засоби забезпечення інформаційної безпеки. Навчально-методичні матеріали: 13 (стор. 3-10). Завдання на СРС: Повторення лекційного матеріалу
2	Тема 2. Погрози безпеці інформаційних систем Лекція 2. Поняття загрози. Види супротивників або «порушників». Види можливих порушень інформаційної системи. Аналіз погроз інформаційній безпеці. Класифікація видів погроз інформаційній безпеці за різними ознаками (за природою виникнення, ступені навмисності і т.п.). Приклади реалізації погроз інформаційній безпеці. Загрози розкриття параметрів системи, загроза порушення конфіденційності, загроза порушення цілісності, загроза відмови служб. Захист інформації. Основні принципи забезпечення інформаційної безпеки в інформаційних системах. Навчально-методичні матеріали: 13 (стор. 11-20), 9 (с.8-26). Завдання на СРС: Повторення лекційного матеріалу.
3	Тема 3. Криптографічні методи закриття інформаціїї Лекція 3. Методи криптографії. Основні поняття і визначення. Історія криптографії, основні етапи розвитку. Засоби криптографічного закриття інформації. Криптографічні перетворення. Шифрування і дешифрування інформації. Вимоги до криптографічних систем. Короткі відомості про криптоаналіз. Навчально-методичні матеріали: 13 (стор. 21-30). Завдання на СРС: Повторення лекційного матеріалу.
4	Тема 4. Симетричні криптосистеми. Лекція 4. Історія розвитку симетричних алгоритмів шифрування. Історичні шифри: шифри зсуву, заміни. Моноалфавітні та поліалфавітні шифри заміни, шифр Віженера .Криптоаналіз історичних шифрів. Навчально-методичні матеріали: 1 (стор. 71-87). Завдання на СРС: Повторення лекційного матеріалу.
5	Лекція 5. Основні класи сучасних симетричних криптосистем. Загальні відомості про блокові шифри. Алгоритми блокового шифрування. Алгоритм DES і його модифікації. Навчально-методичні матеріали: 1 (стор.122-136). Завдання на СРС: Повторення лекційного матеріалу.
6	Лекція 6. Алгоритм Rijndael. Стандарт AES. Алгоритм RC6.Режими застосування блокових шифрів. Навчально-методичні матеріали: 1 (стор. 138-148). Завдання на СРС: Повторення лекційного матеріалу.
7	Лекція 7. Потокові шифри. Загальні відомості про потокові шифри.Синхронні шифри. Приклади потокових шифрів: RC4, SEAL, WAKE та ін. Шифри, що самосинхронизирующиеся. Області застосування симетричних шифрів. Оцінка вразливості та засоби покращення симетричних шифрів. Навчально-методичні матеріали: 1 (стор. 151-157). Завдання на СРС: Повторення лекційного матеріалу.

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, завдання на СРС з посиланням на літературу)
8	Тема 5. Асиметричні криптосистеми Лекція 8. Принципи побудови криптографічних асиметричних систем шифрування. Математичні основи формування сучасних асиметричних алгоритмів шифрування. Однонаправлені функції та їх використання для побудови асиметричних систем шифрування. Навчально-методичні матеріали: 1 (стор. 183-191),13 (конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
9	Лекція 9. Криптосистема шифрування даних RSA, принципи побудови, криптостійкість. Навчально-методичні матеріали: 1 (стор. 193-198), 13(конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
10	Лекція 10. Криптосистеми Ель-Гамаля та Рабіна, принципи побудови, криптостійкість, застосування. Навчально-методичні матеріали: 1 (стор.200-208). Завдання на СРС: Повторення лекційного матеріалу
11	Тема 6. Криптографічні хеш-функції. Лекція 11. Основні вимоги до криптографічних функцій хешування. Принципи побудови та використання в інформаційних технологіях і системах. Алгоритми хешування MD5, SHA-1, SHA-2. Криптостійкість хеш-функцій та їх використання для ідентифікації блоків даних в пошукових системах, перевірки цілісності файлів, захисту паролів, побудови кодів аутетифікації, системах цифрового підпису. Навчально-методичні матеріали: 1 (стор. 104-116), 13(конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
12	Тема 7 Цифрові підписи в системах електронного документообігу Лекція 12. Алгоритми електронного цифрового підпису. Цифрові підписи, засновані на асиметричних криптосистемах, сучасні стандарти цифрового підпису. Навчально-методичні матеріали: 1 (стор. 261-279), 13 (конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
13	Лекція 13. Цифрові підписи, засновані на симетричних криптосистемах. Навчально-методичні матеріали: 13 (конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
14	Тема 8 Комп’ютерна стеганографія в системах безпеки інформаційних технологій Лекція 14. Класифікація стеганографічних методів приховування інформації. Комп’ютерна та цифрова стеганографія. Основні методи вбудовування даних в стеганографічні контейнери. Атаки на стегосистеми. Навчально-методичні матеріали: 4 (стор. 14-17, 70-110, 176-243). Завдання на СРС: Повторення лекційного матеріалу.
15	Лекція 15. Стеганографія і цифрові водяні знаки. Використання цифрових водяних знаків в системах захисту авторських прав та DRM системах, захисту від копіювання цифрових даних. Навчально-методичні матеріали: 13 (конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
16	Тема 9 Аутентифікація об’єктів в системах безпеки інформаційних технологій Лекція 16.

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, завдання на СРС з посиланням на літературу)
	Основні способи аутентифікації об'єктів в комп'ютерних системах. Аутентифікація з використанням паролей та логінів, PIN-кодів, електронних сертифікатів , пластикових карток, біометричних пристроїв. Навчально-методичні матеріали: 5, 13 (конспект лекцій). Завдання на СРС: Повторення лекційного матеріалу.
17	Лекція 17. Аутентифікація з використанням одноразових та багаторазових паролів. Протоколи аутентифікації NTLM, Kerberos. Навчально-методичні матеріали: 5, 13 (конспект лекцій). Завдання на СРС: Повторення матеріалів курсу.
18	Лекція 18. Підсумки. Модульна контрольна робота.

Лабораторні заняття

№ з/п	Назва лабораторної роботи	
1	Дослідження класичних шифрів заміни та методів їх криптоаналізу з допомогою програмних засобів CrypTool.	4
2	Дослідження сучасних алгоритмів симетричного шифрування з допомогою програмних засобів CrypTool та їх програмної реалізації	4
3	Дослідження сучасних алгоритмів асиметричного шифрування з допомогою програмних засобів CrypTool та їх програмної реалізації	4
4	Дослідження криптографічних хеш-функцій.	4
5	Дослідження стеганографічних методів приховування даних в мультимедійних файлах.	2
	Разом	18

6. Самостійна робота студента/аспіранта

№ з/п	Види робіт, що виносяться на самостійне опрацювання	Кількість годин СРС
1	Повторення лекційного матеріалу та підготовка до лекційних занять	17
2	Підготовка до виконання лабораторних робіт та їх захисту	20
3	Підготовка до модульної контрольної роботи	14
	Разом	51

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Вимоги, яких має дотримуватися студент в рамках даної дисципліни:

- під час проведення занять мобільні телефони мають бути переведені у беззвучний режим; лабораторні роботи мають бути виконані та захищені особисто, під час захисту студент повинен
- відповісти на питання викладача, що стосуються як самої лабораторної роботи, так і теоретичного матеріалу, на якому вона базується;
- заохочувальні бали можуть призначатися за активність на лекціях;
- штрафні бали можуть призначатися за несвоєчасне виконання лабораторних робіт;
- при виконанні лабораторних робіт потрібно дотримуватися графіка, який доводиться до відома студентів викладачем на початку семестру;
- обов'язковим є дотримання академічної доброчесності.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: лабораторна робота № 1 (15 балів), лабораторна робота № 2 (15 балів), лабораторна робота № 3 (15 балів), лабораторна робота № 4 (15 балів), МКР (40 балів).
Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
Семестровий контроль: залік.
Умова допуску до семестрового контролю: зарахування усіх лабораторних робіт, рейтинг за виконання лабораторних робіт не менше 36 балів (60% від усіх можливих балів за лабораторні роботи).
Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Приклади питань, які виносяться на модульну контрольну роботу:

1. За погодженням з викладачем, студент має можливість пройти дистанційні чи онлайн курси за відповідною тематикою та зарахувати отримані сертифікати як додаткові бали до рейтингу (не більше 10 балів).
2. Алгоритм кодування RSA.
3. Алгоритми дискретного множення, ділення, піднесення до степені.
4. Статистичні розподіли української та англійської мови.

Робочу програму навчальної дисципліни (силабус):

Складено доцент, к. т. н. Кирюша Богдан Анатолійович

Ухвалено кафедрою системного проєктування (протокол № 13 від 17.06.2024)

Погоджено методичною комісією НН ІПСА (протокол № 10 від 24.06.2024)