СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи побудови і аналізу криптосистем»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	магістр
	Галузі знань ……	12 Інформаційні технології 17 Електроніка, автоматизація та електронні комунікації
	Тривалість викладання	3,4 чверті
	Заняття:	весняний семестр
	лекції:	2 години
	практичні заняття:	1 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: »:https://do.nmu.org.ua/course/view.php?id=5228

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів:

Котух Євген Володимирович	професор, к.т.н.
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/kotykh.php
E-mail:	**kotukh.e.v@nmu.one**

Сафаров Олександр Олександрович	к.т.н.
Персональна сторінка	**https://bit.nmu.org.ua/ua/pro_kaf/prepods/saforov.php**
E-mail:	safarov.o.o@nmu.one

1. Анотація до курсу

Методи побудови і аналізу криптосистем - це дисципліна для вивчення криптосистем, які призначені для захисту інформації, що зберігається, оброблюється

або передається по телекомунікаційним каналам. Найчастіше криптосистеми застосовують безпосередньо шифрування інформації.

2. Мета та завдання курсу

Мета дисципліни – надати теоретичні та практичні знання математичних основ побудови та криптоаналізу, сучасних методів пошуку вразливостей криптоалгоримтів та протоколів, оцінки криптостійкості алгоритмів шифрування.

Завдання курсу:

У результаті вивчення курсу студенти повинні вивчити: відомі криптосистеми, навчитися їх використовувати та здійснювати аналіз.

3. Результати навчання:

Отримання знань та навичок у використанні сучасних методів побудови і аналізу криптосистем.

У результаті навчання студенти навчаться наступному:

Використовувати математичні та технічні методи, засоби й заходи для реалізації проектних рішень з побудови систем та методів криптоаналізу.

Використовувати різні сучасні інформаційні технології та проводити криптоаналіз відомих шифрів.

Подавати криптографічні протоколи та систему цифрового підпису.

4. Структура курсу.

ЛЕКЦІЇ 80

Тема 1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки

Основні поняття і визначення. Правові аспекти захисту інформації. Властивості інформації з точки зору її захисту. Рівні формування режиму інформаційної безпеки.

Тема 2. Традиційні криптографічні системи

Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем.

Тема 3. Криптографічна стійкість шифрів

Поняття криптографічної стійкості. Межі застосування «грубої сили» до атак на шифри. Абсолютна криптостійкість шифрів. Основи квантової криптографії.

Тема 4. Блокові шифри як основа сучасних криптосистем

Блокові алгоритми і режими шифрування. Режим електронної кодової книги (ECB). Режим зціплення блоків по криптотексту (CBC). Режим з оберненим зв’язком по криптотексту (CFB). Режим з оберненим зв’язком по виходу (OFB). Режим з лічильником (CTR). SP-мережа. Мережі Фейстеля.

Тема 5. Криптосистема DES

Загальна характеристика. Алгоритм шифрування. Структура функції F. Стійкість DES. Похідні від DES шифри. DES і шифрована файлова система EFS.

Тема 6. Модель асиметричної системи

Передумови виникнення асиметричних систем. Модель криптосистеми з публічними ключами. Поняття односторонньої функції-пастки.

Задача рюкзака.

Тема 7. Протоколи асиметричної криптографії
Протокол Діффі-Хеллмана. Шифр Шаміра. Шифр Ель-Гамаля. Шифр RSA. Цифровий (електронний) підпис.

ПРАКТИЧНІ ЗАНЯТТЯ 40

Практична робота №1

Тема: Шифр Цезаря.
Мета роботи:Розробка програмної імплементації шифру Цезаря.
Завдання:Розробитипрограмну імплементацію шифру Цезаря.

Практична робота №2

Тема: Шифр Тритеміуса.
Мета роботи:Розробка програмної імплементації шифру Тритеміуса.
Завдання:Розробити програмну імплементацію шифру Тритеміуса.

Практична робота №3

Тема:Шифр гамування.
Мета роботи:Розробка програмної імплементації шифру гамування.
Завдання:Розробити програмну імплементацію шифру гамування.

Практична робота №4

Тема:Шифр DES.
Мета роботи:Розробка програмної імплементації шифру DES.
Завдання:Розробити програмну імплементацію шифру DES.

РАЗОМ 120

5. Технічне обладнання та/або програмне забезпечення.

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	40	30	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

10 балів – Достатня зрозумілість відповіді

7 бали – Добра зрозумілість відповіді

4 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/IBesJEc.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни. За участь у анкетуванні здобувач вищої освіти отримує 5 балів.

8 . Рекомендовані джерела інформації

1. Гапак О.М. Захист інформації в комп'ютерних системах. Підручник / О.М. Гапак, С.І. Балога .- Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021. – 184 с.
2. Криптоаналіз. Криптографічні протоколи : навч. посіб. для студ. спец. 123 «комп'ютерна інженерія» / уклад. : О. М. Гапак ; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК", 2021. – 93 с. : табл. – Бібліогр.: с. 75 с.
3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
4. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. — 120 с.

5. Nadalin Alessandro. WASEC: Web Application Security for the everyday software engineer: Everything a web developer should know about application security: concise, condensed and made to last/ A. Nadalin. — Leanpub, 2020. — 161 p.— ISBN 1670062449, 9781670062444.