Назва курсу	**«Апаратні засоби захисту інформації»**
Викладач (-і)	Дубчак Леся Орестівна
Профайл викладача (- ів)	http://www.wunu.edu.ua/educational-subdivisions/fkit/department-ki-fkit/
Контактний тел.	(0352) 52-46-43
E-mail:	dlo@wunu.edu.ua

Коротка анотація до курсу

Апаратні засоби захисту інформації є дисципліною вибіркового блоку професійної підготовки студентів спеціальності «Системний аналіз». Сучасні засоби і компоненти захисту комп'ютерних систем розв'язують безліч складних задач, які потребують динамічного переналаштування та мінімум затрат як економічних, так і ресурсних. Під час вивчення даної дисципліни студенти вчаться розробляти алгоритми захисту інформації; проводити синтез і аналіз цифрових пристроїв та проектувати компоненти криптопристроїв, тобто розробляти та реалізовувати алгоритми автоматизованої обробки інформації на основі сучасних платформ. Отож дана навчальна дисципліна покликана сприяти формуванню у студентів здібностей до вибору платформ, розробки, моделювання, симуляції та реалізації сучасних компонентів захисту комп'ютерних систем.

Мета та цілі курсу

Програма та тематичний план дисципліни орієнтовані на отримання студентами навиків та знань щодо апаратних засобів захисту інформації.

Завдання курсу полягає в ознайомленні студентів з основними криптографічними алгоритмами, а також прищеплення практичних навиків їх використання.

Студенти вивчають методику роботи основних криптоалгоритмів, ефективність застосування прикладного програмного забезпечення, яке використовується при реалізації криптографічних перетворень.

Результати навчання:

– отримати теоретичні знання, вміння та навики для вибору криптографічного алгоритму та його реалізації;

– отримати практичні навики використання сучасних технологій програмування у застосуванні до криптографічних задач;

– вміти розробляти політику безпеки системи.

Загальна інформація про дисципліну

Ступінь вищої освіти	**Бакалавр**
Спеціальність	**124 – Системний аналіз**
Курс (рік навчання)	**4**
Семестр	**7**
Нормативна \ вибіркова	**вибіркова**
Загальна кількість кредитів	**5**

Перелік тем

Тема 1. Вступ. Шифри перестановки та простої заміни.
Тема 2. Шифри складної заміни. Шифр одноразового блокноту.
Тема 3. Сучасні симетричні криптосистеми.
Тема 4. Арифметика асиметричних криптосистем, генерація ключів.
Тема 5. Криптосистема RSA.
Тема 6. Криптосистеми Рабіна та Ель–Гамаля.
Тема 7. Алгоритми електронного цифрового підпису.
Тема 8. Криптографічні протоколи.
Тема 9. Класичні та сучасні методи криптоаналізу.
Тема10. Сучасні апаратні засоби захисту інформації.
Тема 11. Середовища проектування апаратних засобів захисту інформації.
Тема 12. Етапи розробки політики безпеки.

Рекомендовані джерела інформації

Основна література

1. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник. О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020. – 126 с.

2. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.

3. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект : навчально-методичний посібник / О. А. Самойленко. - Одеса, 2020. - 133 с.

4. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.

5. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П.. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб.— К.: Видавництво Ліра-К, 2020. — 554 с.

Додаткова література

1. А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. Володілець інформації; Засоби захисту інформації. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції. — Київ : Ваіте, 2018. — С. 175; 273. — ISBN 978-617-7627-10-3.

2. Гуз А.М., Касперський І.П., Ткачук Т.Ю. Організація захисту інформації з обмеженим доступом : навчальний посібник. Київ : НА СБУ, 2018. С. 33–58.

3. CCTA Risk Analysis and Management Method [Електронний ресурс] – Режим доступу: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysismanagement-tool-cramm/103133 (дата звернення: 21.01.2022)

4. Ластівка Г.І. Технічний захист інформації в інформаційних та телекомунікаційних системах: навчальний посібник / Г.І. Ластівка, П.М. Шпатар. Чернівці, Чернівецький національний університет, 2018. – 252 с.

5. Гребенніков В. Комплексні системи захисту інформації. Проектування впровадження, супровід / В. Гребенніков. – «Издательские решения», 2018. – 249 с.

6. Jason Andress. Foundations of Information Security: A Straightforward Introduction. No Starch Press,US. 2019. – P. 380.

Система оцінювання та вимоги

Підсумковий бал (за 100-бальною шкалою) з дисципліни "Апаратні засоби захисту інформації" визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінг	Самостійна робота
Середнє арифметичне з оцінок, отриманих на заняттях по темах 1-12	Оцінка за модульну контрольну роботу	Оцінка за виконання тренінгу	Оцінка за виконання самостійної роботи

Будь-яке завдання, за яке студент отримав оцінку, яка його незадовільняє, може бути повторно перездано протягом наступних двох тижнів.

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

Навчальні ресурси

№	Найменування	Номер теми
1.	Операційні системи	3, 5, 7
2.	Microsoft Word	9
3.	Java, C++	6, 7
4.	Active-HDL, Xilinx	10, 11

Політики курсу

Академічна доброчесність. **Дотримання академічної доброчесності студентами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування. Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватися в он-лайн формі за погодженням із керівником курсу.