Силабус курсу

ШИФРУВАННЯ ТА БЕЗПЕКА ДАНИХ

Ступінь вищої освіти – бакалавр

Освітньо-професійна програма: “Технології інтернету речей”

Рік навчання: III **Семестр:** VI

Кількість кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП д.т.н., професор Касянчук Михайло Миколайович

Контактна інформація kmm@wunu.edu.ua

Опис дисципліни

Даний курс знайомить студентів із основними фундаментальними поняттями і законами криптографії для їх використання в сучасних кіберсистемах; принципами побудови криптографічних алгоритмів, основними криптографічними стандартами та їх використання в задачах захисту інформації; основним математичним апаратом та законами криптографії у професійній діяльності; програмними та апаратними засобами, які реалізують основні криптографічні алгоритми для вирішення типових задач захисту інформації.

Структура курсу

№	Тема	Результати навчання	Завдання
1	Вступ. Основні поняття та визначення. Законодавство України в галузі захисту інформації. Принципи криптографічного захисту інформації.	Знати основні поняття криптології (відкритий текст, шифротекст, ключ, шифр, криптоаналіз) та базові принципи криптографічного захисту інформації. Розуміти структуру та основні положення законодавства України у сфері захисту інформації, зокрема Закони «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про електронні довірчі послуги». Усвідомлювати роль криптографії серед інших методів захисту інформації (технічних, правових, організаційних) та її значення для майбутнього педагога цифрових технологій.	Тести, питання
2	Класичні симетричні криптосистеми.	Знати принципи побудови класичних шифрів підстановки та перестановки, зокрема шифри Цезаря, Віженера, Плейфера та матричний шифр. Вміти виконувати шифрування і дешифрування повідомлень за допомогою класичних методів та аналізувати їхню криптографічну стійкість. Розуміти еволюцію криптографічних методів від античності до середини XX століття та причини їхньої вразливості.	Тести, питання

3	Сучасні симетричні криптосистеми. Алгоритм DES.	Знати принципи блочного шифрування, структуру петлі Фейстеля та архітектуру алгоритму DES (Data Encryption Standard), включно з режимами його використання. Вміти пояснити процес генерації раундових ключів та етапи шифрування у DES, а також відмінності між DES і 3DES. Розуміти переваги та обмеження стандарту DES, причини його заміни та значення довжини ключа для криптографічної стійкості.	Тести, питання
4	Сучасні симетричні криптосистеми. Алгоритм IDEA, стандарт шифрування ГОСТ 28147–89. Сімейство алгоритмів RC.	Знати структуру та особливості алгоритмів IDEA, ГОСТ 28147-89 та сімейства RC (RC4, RC5, RC6). Вміти порівнювати різні симетричні алгоритми за критеріями швидкодії, довжини ключа, рівня захищеності та сфер застосування. Розуміти відмінності між потоковим та блочним шифруванням і обирати відповідний алгоритм залежно від задачі.	Тести, питання
5	Арифметика асиметричних криптосистем. Афінні шифри.	Знати математичні основи асиметричної криптографії: модульну арифметику, функцію Ейлера, теорему Ферма та поняття односторонньої функції. Вміти виконувати обчислення в модульній арифметиці та реалізовувати шифрування за допомогою афінних шифрів. Розуміти принципову відмінність між симетричними та асиметричними криптосистемами і роль математичної складності для забезпечення безпеки.	Тести, питання
6	Криптосистема RSA.	Знати алгоритм генерації ключів, шифрування та дешифрування в криптосистемі RSA, а також вимоги до практичної реалізації. Вміти виконувати шифрування/дешифрування повідомлень за алгоритмом RSA та формувати пару відкритий/закритий ключ. Розуміти, на чому ґрунтується стійкість RSA (складність факторизації великих чисел), та усвідомлювати її роль у сучасних системах захисту інформації.	Тести, питання
7	Криптосистеми Рабіна та Ель–Гамаля.	Знати принципи побудови криптосистем Рабіна та Ель-Гамаля, їхні алгоритми шифрування та дешифрування. Вміти порівнювати криптосистеми RSA, Рабіна та Ель-Гамаля за критеріями стійкості, обчислювальної складності й практичного застосування. Розуміти протокол обміну ключами Діффі-Хеллмана та його зв'язок з криптосистемою Ель-Гамаля.	Тести, питання
8	Електронний цифровий підпис.	Знати принципи формування та верифікації електронного цифрового підпису (ЕЦП), зокрема алгоритми DSA та підпис на основі RSA і Ель-Гамаля. Вміти створювати та перевіряти цифровий підпис, а також пояснити роль хеш-функцій (MD5, SHA) у процесі підписання документів. Розуміти правовий статус електронного підпису в Україні та його застосування для забезпечення автентичності й цілісності електронних документів.	Тести, питання
9	Криптографічні протоколи.	Знати основні види криптографічних протоколів: протоколи обміну ключами, протоколи автентифікації та протоколи з нульовим розголошенням. Вміти аналізувати	Тести, питання

		криптографічні протоколи з точки зору їх коректності, стійкості до атак та ефективності. Розуміти роль криптографічних протоколів у побудові захищених комунікаційних систем та їх практичне використання в мережевих технологіях.	
10	Проблема ідентифікації та аутентифікації користувача. Парольна та біометрична ідентифікація.	Знати відмінність між поняттями ідентифікації, аутентифікації та авторизації, а також основні методи парольного та біометричного захисту. Вміти аналізувати надійність парольних систем, формулювати вимоги до стійкості паролів та оцінювати ефективність біометричних методів. Розуміти сучасні підходи до багатофакторної аутентифікації та їх значення для захисту інформаційних систем у закладах освіти.	Тести, питання
11	Особливості фізичного, технічного та програмного захисту інформації.	Знати основні рівні захисту інформації — фізичний (контроль доступу до приміщень, обладнання), технічний (апаратні засоби захисту) та програмний (міжмережеві екрани, системи виявлення вторгнень). Вміти визначати комплекс заходів захисту інформації відповідно до класу загроз і рівня конфіденційності даних. Розуміти принцип ешелонованого захисту (defense in depth) та необхідність комплексного поєднання різних методів для забезпечення надійної безпеки.	Тести, питання
12	Віруси. Захист інформації від вірусів. Основні антивірусні програми.	Знати класифікацію комп'ютерних вірусів (файлові, завантажувальні, макровіруси, мережеві черв'яки, трояни, програми-вимагачі) та механізми їхнього поширення. Вміти обирати та налаштовувати антивірусне програмне забезпечення, проводити сканування системи та реагувати на виявлені загрози. Розуміти принципи роботи сучасних антивірусних програм (сигнатурний, евристичний, поведінковий аналіз) та правила кібергігієни для попередження зараження.	Тести, питання
13	Безпека сучасних мережевих технологій, методи і засоби захисту від віддалених атак через Інтернет.	Знати основні типи мережевих атак (DDoS, фішинг, man-in-the-middle, SQL-ін'єкції, XSS) та методи протидії їм. Вміти налаштовувати базові засоби мережевого захисту — міжмережеві екрани, VPN, протоколи SSL/TLS — та аналізувати мережевий трафік для виявлення підозрілої активності. Розуміти архітектуру безпеки мережевих технологій та роль криптографічних протоколів (HTTPS, SSH, IPSec) у забезпеченні конфіденційності й цілісності даних.	Тести, питання
14	Захист інформації в електронних платіжних системах (ЕПС).	Знати структуру та принципи функціонування електронних платіжних систем, стандарти безпеки PCI DSS та механізми захисту транзакцій. Вміти пояснити роль криптографічних методів (шифрування даних карток, токенізація, 3D-Secure) у забезпеченні безпеки електронних платежів. Розуміти загрози безпеці в електронній комерції (скімінг, фішинг, крадіжка даних) та усвідомлювати важливість захисту персональних фінансових даних у цифровому середовищі.	Тести, питання

Літературні джерела

1. Wong David. Real-World Cryptography. Manning Publications, 2020. — 350 p.
2. Cryptography with Coding Theory. 3rd Edition. — Pearson Education, 2020. — 977 p.
3. Stallings William. Cryptography and Network Security: Principles and Practice. 8th Edition. — Pearson Education, 2020. — 1513 p.
4. Ryabko Boris. Cryptography In The Information Society. World Scientific Publishing, 2021. — 286 p.
5. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. 3rd edition. — New York: CRC Press/Taylor & Francis Group, 2021. — 649 p.
6. Alginahi Y.M., Kabir M.N. (eds.) Authentication Technologies for Cloud Computing, IoT and Big Data. The Institution of Engineering and Technology, 2019. — 370 p.
7. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
8. Yan B., Xiang Y., Hua G. Improving Image Quality in Visual Cryptography. Springer, 2020. — 131 p.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Списування під час проведення контрольних за ходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Політика щодо визнання результатів навчання

Відповідно до «Положення про визнання в Західноукраїнському національному університеті результатів попереднього навчання» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf) здобувачам вищої освіти може бути зараховано результати навчання (неформальної/інформальної освіти, академічної мобільності тощо) на підставі підтвердних документів (сертифікати, довідки, документи про підвищення кваліфікації тощо). Рішення про зарахування здобувачу результатів (певного освітнього компонента в цілому, або ж окремого виду навчальної роботи за таким освітнім компонентом) приймається уповноваженою Комісією з визнання результатів навчання за процедурою, визначеною вищезазначеним положенням.

Оцінювання

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Шифрування та безпека даних» 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
Оцінка визначається як середнє арифметичне з отриманих оцінок	Виконання модульного завдання	Оцінка за виконання завдання	Оцінка за виконання самостійного завдання

Шкала оцінювання

За шкалою ЗУНУ	**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)