ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
Силабус навчальної дисципліни

СУЧАСНА КРИПТОГРАФІЯ

Викладач: *к.ф.-м.н., доцент Скрипник Ірина Анатоліївна*
Кафедра: *програмного забезпечення автоматизованих систем, 9 корпус, ауд. 41а*
E-mail: *sia@zsea.edu.ua*
Телефон: *(061) 277-12-31* (*ОЦ1, 41а*)
Інші засоби зв'язку: *Moodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Інженерія програмного забезпечення Магістр					
Статус дисципліни:		За вибором					
Кредити ECTS	5	**Навч. рік:**	2022-2023	**Рік навчання**	1	**Тижні**	12
Кількість годин	150	**Кількість змістових модулів**[1]	8	**Лекційні заняття** – 12 **Лабораторні заняття** – 36 **Самостійна робота** – 102			
Вид контролю:		Іспит					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=8632					
Консультації: *особисті – за домовленістю, 9 корпус, ауд. 41а;* *дистанційні – календар Microsoft Teams*							

ОПИС КУРСУ

*Курс має на **меті** вивчення теорії інформаційної безпеки комп'ютерних систем, необхідної для їх надійного і безпечного функціонування, принципів захисту інформації, що передається віддаленим користувачам, від несанкціонованого доступу, криптографічних методів захисту інформації; набуття навичок розробки криптографічних протоколів та їх реалізації.*

Зокрема, ознайомлення з методами і алгоритмами класичної криптографії, вивчення принципів інформаційної безпеки комп'ютерних систем, криптографічних методів захисту інформації, симетричних та асиметричних криптографічних систем, криптографічних протоколів, методів ідентифікації та автентифікації, генерації та перевірки цифрових підписів, генерації ключової інформації, протоколів застосування ключів та керування ними для забезпечення цілісності інформації, ознайомлення з комп'ютерними вірусами, їх типами та принципами дії.

Оволодіння знаннями та навичками в області сучасної криптографії стане основою розвинення професійних компетенцій майбутніх магістрів.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент <u>зможе</u>:
вміти:

- *створювати криптографічні системи;*
- *застосовувати алгоритми симетричного шифрування до будь-якої інформації;*
- *застосовувати алгоритми асиметричного шифрування до будь-якої інформації;*
- *виконувати ідентифікацію та автентифікацію*;

[1] **1 змістовий модуль = 15 годин (0,5 кредита ECTS)**

- *генерувати криптографічні ключі;*
- *застосовувати технології розробки криптографічних протоколів;*
- *за допомогою існуючих (стандартних) або розроблених криптографічних засобів виконувати безпечний інформаційний обмін.*

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, конспект лекцій, методичні рекомендації до виконання лабораторних робіт та контрольні заходи розміщені на платформі Moodle:
https://moodle.znu.edu.ua/course/view.php?id=8632

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи

Обов'язкові види роботи:
Лабораторна робота *(max від 6 до 10 балів) – передбачається 10 лабораторних робіт, які студент повинен представити для захисту у вигляді комп'ютерної програми та файлу, що виконується, у СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632*. Захист лабораторної роботи відбувається або в комп'ютерному класі або online (при умові дистанційного навчання). При оцінюванні захисту лабораторної роботи викладач враховує правильність відповіді студента на теоретичні питання, що відносяться до теми лабораторної роботи, та повноту і якість роботи відповідної програми. Вчасність виконання лабораторної роботи враховується з допомогою множника, що зменшується у діапазоні (1–0.1) з кроком 0.1 за кожен прострочений тиждень. Всі лабораторні завдання індивідуальні, тому викладач приймає лабораторну роботу у студента тільки з завданням відповідного варіанту.*

Лаб.№ 1 Побудова кодових систем. Реалізація алгоритму побудови кодової системи Хаффмена. Метод зонного стиску.
Лаб.№ 2 Дослідження стандартів шифрування з секретним ключем. Реалізація алгоритму DES (Data Encryption Standard).
Лаб.№ 3 Дослідження стандартів шифрування з секретним ключем. Реалізація алгоритму ДСТУ: ГОСТ 28147-2009.
Лаб.№ 4 Дослідження стандартів шифрування з відкритим ключем. Реалізація алгоритму RSA.
Лаб.№ 5 Розробка хеш-функції та цифрового підпису.
Лаб.№ 6 Розробка протоколів ідентифікації та автентифікації.
Лаб.№ 7 Дослідження криптографічних протоколів. Розробка протоколів ключового обміну.
Лаб.№ 8 Розробка протоколів передачі інформації.

Тест змістового модулю *передбачає відповіді на запитання у СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632 з матеріалу змістового модуля *максимальним балом 10.*

Підсумкові контрольні заходи:

Тест з дисципліни у *СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632

Передбачає відповідь на 30 запитань вибраних випадковим чином із банку питань множинного типу. Всі питання відповідають тематиці курсу. За необхідності після тесту може проводитися додаткове опитування. Максимальна кількість балів – 30.

Індивідуальні екзаменаційні завдання *представлені у вигляді задач, які треба вирішити та розмістити у СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632 *у вигляді текстового файлу. За результатами розв'язання задач проводиться опитування щодо методів та алгоритмів захисту даних, розроблених класів, криптографічних протоколів.*
Максимальна кількість балів – 10. Не правильно вирішені задачі не зараховуються

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)			
Змістовий модуль 1 (розділ 1)	*Лабораторна робота №1*	*1-2 тиждень*	**6**
Змістовий модуль 2 (розділ 2)	*Лабораторна робота №2*	*3-4 тиждень*	**10**
Змістовий модуль 3 (розділ 3)	*Лабораторна робота №3*	*5 тиждень*	**8**
Змістовий модуль 4 (розділ 4)	*Лабораторна робота №4*	*6-7 тиждень*	**8**
Змістовий модуль 5 (розділ 5)	*Лабораторна робота №5*	*8-9 тиждень*	**8**
Змістовий модуль 6 (розділ 6)	*Лабораторна робота №6*	*10 тиждень*	**5**
Змістовий модуль 7 (розділ 7)	*Лабораторна робота №7*	*11 тиждень*	**5**
Змістовий модуль 8 (розділ 8)	*Лабораторна робота №8 Тест*	*12 тиждень*	**10**
Підсумковий контроль (max 40%)			
Тест у СЕЗН Moodle		Іспит	**30**
Індивідуальне завдання		Іспит	**10**
Разом			**100%**

Шкала оцінювання: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Тиждень і вид заняття	**Тема заняття**	**Контрольне завдання**	**Кількість балів**
Змістовий модуль 1. ***Основи класичної криптографії.***			
Тиждень 1 Лекція 1	*Поняття і характеристики джерела інформації. Кодові системи. Кодові системи Хаффмена, алфавітні, оптимальні.*	*Захист лабораторної роботи № 1*	6
Тиждень 1 Лаб. роб. 1	*Побудова кодової системи Хаффмена.*		
Тиждень 1 Лаб. роб. 1	*Реалізація алгоритму Хаффмена побудови кодової системи.*		
Тиждень 2 Лекція 2	*Обгрунтування алгоритмів побудови кодових систем. Кодове дерево. Умови однозначного декодування.*		
Тиждень 2 Лаб. роб. 1	*Побудова алфавітної кодової системи. Побудова кодових дерев.*		
Змістовий модуль 2. ***Симетричні криптографічні системи. DES.***			
Тиждень 3 Лекція 3	*Складові комп'ютерної безпеки. Принципи побудови криптографічних систем. Алгоритми блочного шифрування.*	*Захист лабораторної роботи № 2*	10
Тиждень 3 Лаб. роб. 2	*Побудова симетричної криптографічної системи.*		
Тиждень 3 Лаб. роб. 2	*Алгоритми симетричного шифрування DES. Генерація ключової інформації.*		
Тиждень 4 Лекція	*Стандарти симетричного блокового шифрування.*		
Тиждень 4 Лаб. роб. 2	*Реалізація алгоритму DES. Стійкість DES.*		
Змістовий модуль 3. ***Симетричні криптографічні системи. Стійке шифрування.***			
Т*иждень 5 Лекція 5*	*Стандарт шифрування* ДСТУ: ГОСТ 28147-2009. *Режими шифрування. Гамування.*	*Захист лабораторної роботи № 3*	8
Тиждень 5 Лаб. роб.3	*Потокові алгоритми шифрування. Властивості.*		
Тиждень 5 Лаб. роб. 3	*Реалізація алгоритму* ДСТУ: ГОСТ 28147-2009. *Стійкість алгоритму.*		
Змістовий модуль 4. ***Асиметричні криптографічні системи.***			
Тиждень 6 Лекція 6	*Елементи теорії чисел. Арифметика лишків. Алгоритм*	*Захист лабораторної роботи № 4*	8

	Евкліда. Функція Ейлера.		
Тиждень 6 *Лаб. роб. 4*	*Односторонні функції. Асиметричні алгоритми. Ключова інформація.*		
Тиждень 7 *Лекція 7*	*Алгоритм RSA. Стандарт асиметричного шифрування. Стійкість RSA.*		
Тиждень 7 *Лаб. роб. 4*	*Побудова односторонньої функції. Реалізація розширеного алгоритму Евкліда.*		
Тиждень 7 *Лаб. роб.4*	*Реалізація алгоритму RSA.*		
Змістовий модуль 5. ***Електронні цифрові підписи***			
Тиждень 8 *Лекція 8*	*Поняття цифрового підпису (ЦП). Концепція формування. Хеш-функції. RSA.*	*Захист лабораторної роботи № 5.*	8
Тиждень 8 *Лаб. роб. 5*	*Побудова хеш-функції. SHA, MD5.*		
Тиждень 9 *Лекція 9*	*Стандарти генерації та перевірки ЦП. RSA, DSA.*		
Тиждень 9 *Лаб. роб.5*	*Еліптичні криві. Скінченні поля. Поле Галуа. Алгоритм ECDSA.*		
Тиждень 9 *Лаб. роб.5*	*Стандарт ЦП ДСТУ 4045. Розробка ЦП.*		
Змістовий модуль 6. ***Ідентифікація. Автентифікація.***			
Тиждень 10 *Лекція 10*	*Ідентифікація. Автентифікація. Схеми ідентифікації.*	*Захист лабораторної роботи № 6*	5
Тиждень 10 *Лаб. роб. 6*	*Протоколи ідентифікації. Розробка протоколу ідентифікації.*		
Змістовий модуль 7. ***Криптографічні протоколи.***			
Тиждень 11 *Лекція 11*	*Поняття криптографічного протоколу. Вимоги. Учасники. Класифікації.*	*Захист лабораторної роботи № 7*	8
Тиждень 11 *Лаб. роб. 6*	*Протоколи ключового обміну. Протоколи автентифікації.*		
Тиждень 11 *Лаб. роб. 7*	*Протоколи ЦП, передачі інформації.*		
Змістовий модуль ***8. Аналіз протоколів.***			
Тиждень 12 *Лекція 12*	*Формальний аналіз протоколів. Специфікації протоколів. BAN-логіка. Ідеалізована форма протоколів.*	*Захист лабораторної роботи № 7* *Тест в Moodle*	10
Тиждень 12 *Лаб. роб. 7*	*Побудова автоматної моделі протоколу автентифікації.*		

ОСНОВНІ ДЖЕРЕЛА

1. Скрипник І.А. Методи захисту інформації в комп'ютерних системах. Навчально- методичний посібник. Запоріжжя : ЗДІА, 2016. 88 с.
2. Шнайер Б. Прикладна криптографія: протоколи, алгоритми і вихідний код на С. 2-е вид. Вильямс, 2017. 1040 с.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[2]

Відвідування занять. Регуляція пропусків.
Теоретико-практичний характер курсу передбачає обов'язкове відвідування лекцій і лабораторних занять. Студенти, які за певних обставин не можуть відвідувати заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущенні завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання шляхом виконання індивідуального письмового завдання.
Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Політика академічної доброчесності
Усі письмові роботи, що виконуються слухачами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення UniCheck. Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перефразування чужої праці без згадування оригінального автора). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на Moode: https://moodle.znu.edu.ua/mod/resource/view.php?id=103857
Виконавці індивідуальних дослідницьких завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).
Роботи, у яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем.
Висока академічна культура та європейські стандарти якості освіти, яких дотримуються у ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел:
Електронні ресурси Національної бібліотеки ім. Вернадського: http://www.nbuv.gov.ua
Цифрова повнотекстова база даних англомовної наукової періодики JSTOR: https://www.jstor.org/

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки

[2] **Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, і т.д. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!**

правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.
Під час виконання заходів контролю (термінологічних диктантів, контрольних робіт, іспитів) використання гаджетів заборонено. У разі порушення цієї заборони роботу буде анульовано без права перескладання.

Комунікація

Базовою платформою для комунікації викладача зі студентами є Moodle.
Важливі повідомлення загального характеру – зокрема, оголошення про терміни подання контрольних робіт, коди доступу до сесій у Microsoft Teams та ін. – регулярно розміщуються викладачем на форумі курсу та в календарі Microsoft Teams. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на сторінці курсу у Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам».
Якщо за технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу sia@zsea.edu.ua.
У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2020-2021

ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р. (гіперпосилання на сторінку сайта)

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Студенти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених ***Кодексом академічної доброчесності ЗНУ***: https://tinyurl.com/ya6yk4ad. *Декларація академічної доброчесності здобувача вищої освіти* (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): https://tinyurl.com/y6wzzlu3.

ОСВІТНІЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до *Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ*: https://tinyurl.com/y9tve4lk**.**

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається *Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ*: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються *Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ*: https://tinyurl.com/ycds57la.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється *Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті*: https://tinyurl.com/y8gbt4xs.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються *Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ*: https://tinyurl.com/ycyfws9v. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: *Положення про порядок призначення і виплати академічних стипендій у ЗНУ*: https://tinyurl.com/yd6bq6p9; *Положення про призначення та виплату соціальних стипендій у ЗНУ*: https://tinyurl.com/y9r5dpwh.

ЗАПОБІГАННЯ КОРУПЦІЇ. Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога (061)228-15-84 (щоденно з 9 до 21).

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь-ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ. Наукова бібліотека: http://library.znu.edu.ua. Графік роботи абонементів: понеділок – п`ятниця з 08.00 до 17.00; субота з 09.00 до 15.00.

ЕЛЕКТРОННЕ ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): HTTPS://MOODLE.ZNU.EDU.UA
Якщо ви забули пароль і вказали електронну адресу в профілі системи Moodle ЗНУ,
то використовуйте посилання для відновлення паролю
https://moodle.znu.edu.ua/mod/page/view.php?id=133015
Перевіряйте папку СПАМ

Якщо ви забули логін для входу в систему СЕЗН ЗНУ, то
пишіть лист за адресами:

для здобувачів:

- **moodle.znu@znu.edu.ua**

з темою "Забув логін", в листі вкажіть:

- ***Прізвище, ім'я, по-батькові українською мовою;***
- ***шифр групи (студенту)/ кафедру (викладачу);***
- ***електронну адресу.***

Центр інтенсивного вивчення іноземних мов: http://sites.znu.edu.ua/child-advance/
Центр німецької мови, партнер Гете-інституту: https://www.znu.edu.ua/ukr/edu/ocznu/nim
Школа Конфуція (вивчення китайської мови): http://sites.znu.edu.ua/confucius.