ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

ОСНОВИ КРИПТОЛОГІЇ

Викладач: *кандидат технічних наук, доцент Решевська Катерина Сергіївна*
Кафедра: *комп'ютерних наук, І корпус, ауд. 39*
E-mail: *reshka82zp@gmail.com*
Телефон: *(061) 289-12-57*
Інші засоби зв'язку: *Moodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Комп'ютерні науки Бакалавр					
Статус дисципліни:		Нормативна					
Кредити ECTS	3	**Навч. рік:**	2020-2021	**Рік навчання**	4	**Тижні**	10
Кількість годин	90	**Кількість змістових модулів**[1]	4	**Лекційні заняття** – 10 **Лабораторні заняття** – 20 **Самостійна робота** – 60			
Вид контролю:		Екзамен					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=4199					
Консультації:							

ОПИС КУРСУ

Метою *викладання навчальної дисципліни «Основи криптології» є засвоєння математичних та термінологічних основ з криптології, вивчення студентами процесу проведення аналізу погроз безпеці інформації, основних методів, механізмів, алгоритмів та протоколів криптографічного захисту інформації в інформаційно-комунікаційних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.*

Основними завданнями вивчення дисципліни «Основи криптології» є: формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики криптографічного захисту інформації та криптографічного аналізу.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Згідно вимогам освітньої програми студенти повинні досягти таких результатів навчання.

Знати:

— *канали уразливості та витоку інформації, явища, що притаманні їх прояву та існуванню;*

— *основні методи, механізми, протоколи та алгоритми криптографічного захисту інформації;*

— *критерії та показники оцінки якості криптографічного захисту інформації;*

— *методи криптографічних перетворень інформації та способи їх здійснення;*

— *методи та засоби аналізу та криптоаналізу асиметричних та симетричних крипто перетворень;*

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

— *методи, механізми та протоколи безпечного встановлення, узгодження, підтвердження, розподілення і транспортування ключів та розподілення таємниці;*

— *основні протиріччя, проблеми, тенденції та напрями розвитку теорії та практики криптографічного захисту інформації, прогнозування їх можливостей та можливостей порушників (крипто аналітиків);*

— *функціональні можливостіта порядок застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптогрфічних бібліотек.*

Вміти:

— *обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів;*

— *обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів;*

— *розробляти вимоги та обирати для застосування криптографічні перетворення та протоколи, що мінімізують впливи порушників;*

— *розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу криптографічних алгоритмів та протоколів захисту інформації;*

— *моделювати крипто аналітичні атаки та здійснювати крипто аналіз;*

— *аналізувати криптографічні протоколи на їх рівень безпечності (повноту, коректність та нульове розголошення тощо);*

— *оцінювати захищеність від несанкціонованого доступу до інформації;*

— *обґрунтовувати вимоги до ключових даних та ключової інформації, здійснювати аналіз їх властивостей;*

— *застосовувати стандартні пакети при розв'язанні прикладних задач моделювання криптографічних перетворень, ключових даних та протоколів;*

— *використовувати математичний апарат для освоєння теоретичних основ і практичного використання криптографічних методів;*

— *використовувати професійно профільовані знання й практичні навички в галузі математики, математичного аналізу для освоєння загальної та прикладної криптографії;*

— *володіти спеціалізованими програмними пакетами.*

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, методичні рекомендації до виконання лабораторних робіт та індивідуального завдання, тести у системі Moodle

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи

Поточний контроль передбачає такі ***теоретичні*** завдання:

- *усне опитування з теоретичного матеріалу за темою на початку кожного лабораторного заняття. Перелік питань з кожної лабораторної роботи розміщено у файлі з завданням до лабораторної роботи у системі Moodle.*
- *поточний тест за пройденим матеріалом.*

Поточний контроль передбачає таке ***практичне*** завдання:

- *виконання лабораторних робіт.*

Підсумкові контрольні заходи:

Індивідуальне завдання *– розробка презентації та підготовка доповіді на теме: «Алгоритм блочного шифрування …» (1. Blowfish 2. IDEA 3. Camelia 4. Feal 5. Khufu 6. Serpent 7. Mars 8. Towfish 9. RC2 10.RC5 11.RC6 12.Khazad)*

Підсумковий тест *– підсумкове тестування з курсу за обмежений час у системі Moodle.*

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)			
Змістовий модуль 1 (розділ 1)	*Опитування з теоретичного матеріалу*	*Тиждень 1,2,*	**3**
	Лабораторна робота 1	*Тиждень 1,2*	**7**
Змістовий модуль 2 (розділ 1)	*Опитування з теоретичного матеріалу*	*Тиждень 3,4*	**3**
	Лабораторна робота 2	*Тиждень 3,4*	**7**
	Поточний тест 1	*Тиждень 5*	**10**
Змістовий модуль 3 (розділ 2)	*Опитування з теоретичного матеріалу*	*Тиждень 6,7*	**3**
	Лабораторна робота 3	*Тиждень 6,7*	**7**
Змістовий модуль 4 (розділ 2)	*Опитування з теоретичного матеріалу*	*Тиждень 8,9*	**3**
	Лабораторна робота 4	*Тиждень 8,9*	**7**
	Поточний тест 2	*Тиждень 10*	**10**
Підсумковий контроль (max 40%)			
Підсумковий тест			**20**
Індивідуальне завдання			**20**
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.			
Тиждень 1 Лекція 1	Предмет і задачі криптографії. С и метричні криптосистеми		
Тиждень 1,2 Лабораторна робота 1	Блочні шифри. Алгоритм DES	Усне опитування з теми. Виконання завдань лабораторної роботи	10
Змістовий модуль 2.			
Тиждень 3,5 Лекція 2	Блочні шифри. Алгоритми шифрування AES та DES		
Тиждень 3, 4 Лабораторна робота 2	Алгоритм шифрування AES	Усне опитування з теми. Виконання завдань лабораторної роботи	10
Тиждень 5 Поточний тест 1		Тестові завдання в системі Moodle	10
Змістовий модуль 3.			
Тиждень 7 Лекція 3	Асиметричні алгоритми шифрування.		
Тиждень 6, 7 Лабораторна робота 3	Системи шифрування з відкритим ключем	Усне опитування з теми. Виконання завдань лабораторної роботи	10
Змістовий модуль 4.			
Тиждень 9 Лекція 4	Електронно-цифровий підпис		
Тиждень 9 Лабораторна робота 3	Криптоалгоритми засновані на дискретному логарифмі	Усне опитування з теми. Виконання завдань лабораторної роботи	10
Тиждень 10 Поточний тест 2		Тестові завдання в системі Moodle	10

ОСНОВНІ ДЖЕРЕЛА

1. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування. Житомир : Державниий університет телекомунікацій (ДУТ), 2014. 448 с.

2. Іваночко С.Г. Криптологія. Львів: Національний Університет Львівська Політехніка, 2008. 46 с.

3. Гребенніков В.В. Історія криптології & секретного зв'язку Ужгород: Ліра, 2012. — 664 с.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[2]

Відвідування занять. Регуляція пропусків.
Відвідування лекційних і лабораторних занять є обов'язковим. Студенти, які за певних обставин не можуть відвідувати лабораторні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять.
.

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.
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 лабораторних занять дозволяється виключно у навчальних цілях. Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.
Під час виконання заходів контролю (поточних та підсумкового тестів) 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 здачі індивідуального завдання, коди доступу до сесій у Cisco Webex та Zoom. – регулярно розміщуються викладачем на форумі курсу. 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,

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

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 reshka82zp@gmail.com. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
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 забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:
· для студентів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
· для студентів Інженерного інституту ЗНУ - alexvask54@gmail.com, Василенко Олексій Володимирович
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

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.