ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

МАТЕМАТИЧНІ МЕТОДИ КРИПТОЛОГІЇ

Викладач: *кандидат фізико-математичних наук, доцент , Зіновєєв Ігор Валерійович*
Кафедра: *Загальної математики, І корпус, ауд. 21а*
E-mail: *zinoveev@znu.edu.ua*
Телефон: *(061) 289-12-54*
Інші засоби зв'язку: *Moodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:	Математичне та програмне забезпечення криптології, Прикладна математика, Середня освіта (Математика) Бакалавр						
Статус дисципліни:	дисципліна вільного вибору студента						
Кредити ECTS	6(5)	**Навч. рік:**	2020-21	**Рік навчання**	3(4)	**Тижні**	16
Кількість годин	180 (150)	**Кількість змістових модулів**[1]	2	**Лекційні заняття – 32** **Лабораторні заняття – 32** **Самостійна робота – 116 (86)**			
Вид контролю:		залік					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=4063					
Консультації: *час консультація за розкладом консультацій (розміщено на стенді кафедри) Moodle (форум курсу), Zoom*							

ОПИС КУРСУ

Курс є необхідною складовою частиною базової теоретичної та практичної підготовки студента, що навчається за освітньою програмою «прикладна математика, Математичне та програмне забезпечення криптології», а також є основою для подальшого вивчення спеціальних дисциплін.

Програму курсу укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Курс «Математичні методи криптології» складається з 2-х змістових модулів: 1. Математичні основи криптології.; 2. Сучасні системи комп'ютерної криптології.

*Основною **метою** викладання курсу є отримання базових компетентностей в області криптології, криптографічного захисту інформації.*

*Основними **завданнями** курсу є: надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації; формування у студентів категоріальних понять з основ математики симетричної та асиметричної криптографії, криптоаналізу; формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів; стимулювання студентів до активної аналітико-пошукової роботи.*

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

*У разі успішного завершення курсу студент **зможе**:*

- *застосовувати на практиці набуті знання про джерела і способи дії загроз на об'єкти інформаційної безпеки ;*
- *здійснювати пошук навчальної та наукової інформації.*

- *використовувати фундаментальні та спеціальні знання з математики до розв'язання прикладних задач в галузі шифрування, криптоаналізу, захисту інформації;*
- *володіти алгоритмами шифрування та дешифрування інформаційних текстів та застосовувати їх;*
- *працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;*
- *створювати засобами стандартного програмного забезпечення елементи захисту інформації.*

Використання програмних засобів під час виконання практичних та лабораторних завдань розвине як загальні, так і професійні компетенції слухачів.

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани занять, методичні рекомендації до виконання індивідуальних та практичних завдань, групових творчих проектів розміщені на платформі Moodle:
https://moodle.znu.edu.ua/course/view.php?id=4063

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи

Теоретичний контроль *(кількість балів зазначено на сторінці дисципліни в moodle) – усні (до 2 балів за один контроль) та письмові (до 5 балів за один контроль) опитування на лекціях, практичних заняттях, тестування – (до 5 балів за тест).*

Практичний контроль *(кількість балів зазначено на сторінці дисципліни в moodle) – розв'язання практичних домашніх завдань, завдань самостійної роботи (до 5 балів за один контроль), письмові контрольні роботи (до 5 балів за один контроль, двічі на семестр), тестування – (до 5 балів за тест).*

Реферат *– оволодіння матеріалом, що виноситься на самостійну роботу (до 3 балів за один реферат, двічі на семестр).*

Підсумкові контрольні заходи:

Індивідуальне дослідницьке завдання, проект (ІДЗ, можливо виконання у групі з двох, трьох студентів).

ІДЗ видається за один – два місяці до завершення теоретичного навчання поточного семестру. Термін виконання не менше одного місяця. Виконане ІДЗ, на передостанньому тижні теоретичного навчання поточного семестру подається викладачеві у вигляді оформленої пояснювальної записки (постановка задачі (змістовна, концептуальна, конкретна, математична), побудова та обґрунтування адекватності математичної моделі, обґрунтування методу розв'язання, його достовірності, розв'язок задачі, інтерпретація отриманих результатів, прогнозування або рекомендації до застосування моделі).

На останньому тижні проводиться публічний захист у групі (до 20 балів).

Формат захисту ІДЗ проекту: презентація, тривалістю до 10 хвилин та відповідь на задані присутніми питання (до 5 хвилин).

Детальні вимоги та практичні рекомендації до виконання ІДЗ на сторінці курсу у Moodle та на поточних консультаціях.

Результати ІДЗ можуть стати основою для доповідей на студентських науково-практичних конференціях.

Залікове тестове завдання *(до 20 балів)– проводиться у системі Moodle або MyTestXPro із використанням (за необхідністю) розроблених програмних продуктів, MsExcel, Maple. Критерії оцінювання та вимоги до тесту наведено в інструкції до тесту та поточній консультації.*

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
1(6) семестр			
Поточний контроль (max 60%)			
Змістовий модуль 1	*Теоретичний контроль*	*Тижні 1–8*	**4**
	Лабораторні роботи	*Тижні 1–8*	**20**
	Тест за змістовим модулем	*Тиждень 8*	**6**
Змістовий модуль 2	*Теоретичний контроль*	*Тижні 9–16*	**4**
	Лабораторні роботи	*Тижні 9–16*	**20**
	Тест за змістовим модулем	*Тиждень 16*	**6**
Підсумковий контроль (max 40%)			
Заліковий тест за курс			**20**
Захист індивідуального дослідницького завдання або групового проекту			**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**	**Кільк. балів**
Змістовий модуль 1. Математичні основи криптології.			
Тижні 1–2 Лекції Лаб.роботи	*Основні поняття криптології. Арифметичні основи криптографії.* Алгоритм ділення з остачею. Найбільший спільний дільник. Взаємно прості числа. Найменше спільне кратне. Прості числа. Порівняння. Класи лишків. Функція Ейлера. Порівняння першого степеня. Первісні корені. Існування первісних коренів. Індекси за	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	5

	модулем p^k і $2p^k$. Символ Лежандра. Квадратичний закон взаємності. Символ Якобі.		
Тижні 3–4 Лекції Лаб.роботи	*Алгебраїчні основи криптографії.* Поняття групи. Підгрупи груп. Циклічні групи. Гомоморфізм груп. Групи підстановок. Дії групи на множині. Кільця і поля. Підкільця. Гомоморфізм кілець. Евклідові кільця. Прості і максимальні ідеали. Скінченні розширення полів. Поле розкладу. Скінченні поля. Порядки незвідних многочленів. Лінійні рекурентні послідовності. Послідовності максимального періоду	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 5–6 Лекції Лаб.роботи	Генератори псевдовипадкових чисел. Принципи використання генераторів псевдовипадкових чисел під час потокового шифрування. Генератори псевдовипадкових чисел. Потокові шифри A5, RC4 та опис їх алгоритмів.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 7–8 Лекції Лаб.роботи	*Класичні алгоритми криптографії.* Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками Тест за змістовим модулем	5 6
Змістовий модуль 2. Сучасні системи комп'ютерної криптології			
Тижні 9–10 Лекції Лаб.роботи	Стандарти симетричних алгоритмів блокового шифрування даних. Принципи та структура побудови алгоритму *DES* (Data Encription Standard). Генерація раундових ключів. Процес шифрування даних. Функція *DES*. Аналіз алгоритму.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	5
Тижні 11–12 Лекції Лаб.роботи	Симетричний алгоритм блокового шифрування даних *IDEA* (International Data Encryption Algorithm). Принципи та структура побудови алгоритму *IDEA*. Генерація раундових ключів для зашифрування та розшифрування даних . Процес шифрування даних. Аналіз алгоритму *IDEA*.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 13–14	Стандарт симетричного алгоритму блокового шифрування даних ДСТУ	Фронтальне опитування (усне, письмове).	2

Лекції Лаб.роботи	ГОСТ 28147:2009 Принципи побудови алгоритму. Структура криптографічної системи шифрування даних у режимі простої заміни. Шифрування даних у режимі гамування. Аналіз шифру. Криптографічна стійкість.	Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	5
Тижні 15–16 Лекції Лаб.роботи	Асиметричні криптографічні системи шифрування Основні ідеї та принципи. Перша криптографічна система з відкритим ключем — система Діффі–Хеллмана. Криптографічна система Шаміра. Криптографічна система Ель-Гамаля. Криптографічна система RSA. Криптографічна система Рабіна. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками Тест за змістовим модулем	 5 6
Тижні 15–16	Підсумковий контроль	Захист ІДЗ	20
Тижні 16	Підсумковий контроль Залік	Тестування (проводиться у системі Moodle або MyTestXPro)	20
Всього			**100**

ОСНОВНІ ДЖЕРЕЛА

1. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009
2. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых.-К: Изд. «Политехника», 2004. - 224с.
3. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Книга 1: Алгебраические и алгоритмические основы. Изд.2, доп. 2012. 360 с. https://fileskachat.com/download/42276_2f1434dd0df4cd2ff87d8a7c2c417a7d.html
4. В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005, 785с.
5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2006. – 336 с.
6. Задірака В.К. Комп’ютерна криптологія / В.К.Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
7. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП. – 2001. – 254с.
8. Молдовян А.А., Молдовян В.А., Советов В.Я. Криптография. – Серия “Учебники для вузов. Специальная литература”. – Спб.: Издательство “Лань”, 2006. – 224 с.
9. О.В.Вербіцький. Вступ до криптології. Видавництво НТЛ., Львів, 2008, с.248.
10. Фергюссон Н. Практическая криптография / Н. Фергюссон, Б. Шнайер. – М.: Вильямс, 2005. – 424 с.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ

Відвідування занять. Регуляція пропусків.
Відвідування занять обов'язкове.
Завдання мають бути виконанні в зазначені терміни.
Пропуски занять, незалежно від причини підлягають відпрацюванню у години консультацій.
За умови систематичних пропусків може бути застосована процедура повторного вивчення дисципліни (див. посилання на Положення у додатку до силабусу).

Політика академічної доброчесності
Кожний студент зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства – це *плагіат*. Використання будь-якої інформації (текст, фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора! Якщо ви не впевнені, що таке плагіат, фабрикація, фальсифікація, порадьтеся з викладачем. До студентів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані різні дисциплінарні заходи (див. посилання на Кодекс академічної доброчесності ЗНУ в додатку до силабусу).

Використання комп'ютерів/телефонів на занятті
Під час занять персональні електронні пристрої (телефони, ПК) можна використовувати лише за умови виробничої необхідності (за погодженням з викладачем). Мобільні телефони повинні бути переведені на беззвучний режим. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо.

Комунікація
Очікується, що студенти перевірятимуть свою електронну пошту і сторінку дисципліни в Moodle та реагуватимуть своєчасно. Всі робочі оголошення можуть надсилатися через старосту, на електронну на пошту та розміщуватимуться в Moodle. Будь ласка, перевіряйте повідомлення вчасно. *Ел. пошта має бути підписана справжнім ім'ям і прізвищем*.

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.