Національний транспортний університет	**ОК39 «МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ТРАНСПОРТНОЇ ГАЛУЗІ»** **ОНП: «Комп'ютерні науки»** **Рівень вищої освіти - третій** (освітньо-науковий) **Семестр: 5, рік:** 2022-2023 н.р. **Дні занять, час занять, аудиторія:** Згідно розкладу. Перейдіть за посиланням http://www.ntu.edu.ua/studentam/rozklad/
Лекції веде ПІП	Доцент кафедри інформаційних систем і технологій, к. ф.-м. н. Сисак Катерина Ярославівна
Контактна інформація	електронна пошта – kist.ntu.edu.ua@gmail.com телефон кафедри – 044-280-70-66
Аудиторія	
Час консультацій	
Семінарські / практичні / лабораторні заняття веде	
ПІП	Доцент кафедри інформаційних систем і технологій, к. ф.-м. н. Сисак Катерина Ярославівна
Контактна інформація	електронна пошта – kist.ntu.edu.ua@gmail.com, sysakkya@gmail.com телефон кафедри – 044-280-70-66
Аудиторія	
Час консультацій	

Анотація курсу

Предметом вивчення навчальної дисципліни є теоретичні основи криптографічних методів захисту інформації і практична реалізація, вдосконалення та розробка криптографічних протоколів. **Міждисциплінарні зв'язки:** «Теорія алгоритмів», «Технології захисту інформації», «Теорія ймовірностей».

Програма навчальної дисципліни складається з таких модулів:

Модуль 1. Алгоритми теорії чисел та криптографія.

Тема 1. Арифметичні операції в скінченних полях. Функція Ойлера. Квадратичні лишки.

Тема 2. Алгоритми тестування простоти. Факторизація натуральних чисел. Первісні корені за простим модулем.

Тема 3. Ймовірнісні алгоритми. Порівняння складності задач. Ймовірнісне криптування.

Тема 4. Важкооборотні функції. Генератори псевдовипадкових бітів.

Модуль 2. Просунуті криптосистеми з відкритим ключем.

Тема 5. Еліптичні криві та криптосистеми на еліптичних кривих.

Тема 6. Протоколи на основі ймовірнісного криптування.

Тема 7. Криптосистема Рабина.

Тема 8. Криптосистема Голдвассера-Мікалі.

Методи контролю:

- експрес-контроль;
- усна співбесіда за матеріалами розглянутої теми;

- фронтальне, індивідуальне та комбіноване усне опитування;
- тестовий модульний контроль;
- завдання до самостійної роботи.

Підсумковою формою контролю знань є екзамен у формі письмової контрольної робити.

Джерела для вивчення курсу –

1. **Електронний ресурс бібліотеки НТУ http://lib.ntu.edu.ua/catalog/login.html.**
2. **Віртуальне середовище навчання Zoom, GoogleClass/Meet.**
3. **Робоча програма та конспект лекцій з дисципліни.**

Оцінювання

Підсумкова оцінка вивчення курсу розраховується з використанням наступних категорій

Поточне, підсумкове тестування та самостійна робота (максимальна кількість балів)						Екзамен / залік	Підсумковий контроль (максимальна кількість балів разом)
Модуль 1			Модуль 2				
Відвідування	Активність	Модульний контроль	Відвідування	Активність	Модульний контроль		
5	15	10	5	15	10	40	100

Критерії оцінювання http://vstup.ntu.edu.ua/pro_orhanizatsiyu_osvitnoho_protsesu.pdf.

Політика несвоєчасної здачі роботи. поточні та підсумкові контролі проводяться відповідно до встановлених відділом аспірантури графіків. У випадку неявки здобувача вищої освіти на контроль за поважних причин є можливість індивідуального проведення в узгоджений з викладачем термін за наявністю **дозволу відділу аспірантури**.

Повторне складання екзамену у випадку отримання незадовільної оцінки допускається не більше двох разів: один раз – викладачу, другий – комісії, яка створюється відділом аспірантури.

Запізнені завдання. При здачі роботи без поважної причини пізніше встановленого терміну оцінка буде знижена на 10 %. Технічні проблеми (поломка обладнання, проблеми з друком) не є поважною причиною для несвоєчасної здачі роботи.

Політика переоцінки. Упродовж тижня після оголошення результатів поточного контролю здобувач освіти може звернутися до оцінювача за роз'ясненням і/або з незгодою щодо отриманої оцінки. У випадку незгоди з рішенням оцінювача щодо результатів семестрового контролю здобувач освіти може звернутися до оцінювача з незгодою щодо отриманої оцінки у день її оголошення. Перескладання семестрового контролю з метою підвищення позитивної оцінки не допускається.

Політика відвідування та / або активності. Відвідування навчальних занять є обов'язковим для здобувача освіти. Вільне відвідування лекційних занять можливе лише за дозволом відділу аспірантури. Невиконання здобувачем освіти завдань, що визначені індивідуальним навчальним планом практичних, семінарських і лабораторних занять, через відсутність на заняттях є підставою для прийняття рішення про недопущення до семестрового контролю. За рішенням відділу аспірантури буде надана можливість виконати пропущені завдання за індивідуальним графіком (але не пізніше, ніж до завершення семестрового контролю).

Плагіат, академічна доброчесність http://vstup.ntu.edu.ua/polozhennyantu_dobroch.pdf. Порушенням академічної доброчесності є: – академічний плагіат; – фальсифікація; – списування; – обман; – хабарництво. При проходженні контролю (поточного або підсумкового) особа, яка проходить контроль, не має права використовувати будь яку зовнішню (сторонню) допомогу. Якщо оцінювач підозрює особу, що проходить контроль, у використанні недозволених допоміжних

засобів, він має право запропонувати їй учинити дії, які б спростували підозру. У разі відмови, списування, використання недозволені допоміжних засобів чи зовнішньої допомоги (обману) результат оцінюється як «0» балів («незадовільно»).

Поведінка в аудиторії. Ноутбуки та портативні пристрої можна використовувати ВИКЛЮЧНО з навчальною метою за вказівкою викладача. Неправильне використання ноутбуків чи кишенькових пристроїв вважатиметься порушенням дисципліни, викладач має право ініціювати відповідні дії. В аудиторії забороняється вживання їжі, напоїв (за винятком води). Студенти та викладачі повинні дотримуватися етичних норм поведінки.

Для студентів з обмеженими можливостями або особливими потребами слід звернутися до деканату та обговорити з викладачем питання організації навчання якомога раніше.

При виникненні у студента проблем зі здоров'ям, які можуть заважати навчанню (напружені стосунки, посилене занепокоєння, вживання заборонених речовин, почуття слабкості, труднощі з концентрацією уваги та/або відсутність мотивації) слід звернутися до медичного пункту, що розташований в будівлі гуртожитку №3 за адресою вул. Бойчука, 36.

Свої скарги, пропозиції, зауваження та повідомлення про наявність конфліктних ситуацій в рамках освітніх програм здобувачі можуть надсилати електронною поштою за адресою: general@ntu.edu.ua, або скористатися скринькою довіри, яка розміщена при вході в університет. E-mail звернень до психологічної служби: philosophy@ntu.edu.ua.

Зв'язок з викладачем: e-mail викладача: sysakkya@gmail.com.

Рекомендована література:

1. J. Katz, Ye. Lindell. Introduction to Modern Cryptography (2-nd ed.). — CRC Press, 2015.
2. N. Koblitz. Algebraic Aspects of Cryptography. — Vol. 3 — Springer, 1999.
3. N. Koblitz. A Course in Number Theory and Cryptography. — NY, Springer, 1994.
4. Вербіцький О. В. Вступ до криптографії. — Львів, ВНТЛ, 1998.