



АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ. ЧАСТИНА 1 (ПО 7.1)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Обов'язкова (нормативна) (цикл професійної та практичної підготовки)</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>4 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 6 кред / 180 год Лекційних занять: 36 год Практичних занять: 36 год Лабораторні роботи (комп'ютерний практикум): 18 год Самостійна робота студентів: 90 год</i>
Семестровий контроль/ контрольні заходи	<i>Екзамен, МКР, індивідуальне семестрове завдання</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектори: доц. Яковлев Сергій Володимирович (yasv@rl.kiev.ua), ст. викл. Фесенко Андрій В'ячеславович Практичні: ас. Ядуха Дарія Вікторівна Комп'ютерний практикум: ас. Якимчук Олексій Петрович</i>

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Асиметрична криптографія, досить молода область криптографічної науки (рік її народження – 1976), в наш час займає чільне місце серед математичних методів захисту інформації, особливо у банківській та фінансовій сферах. Інша назва цієї гілки криптографії – криптографія з відкритим ключем. Знання математичних основ побудови асиметричних криптосистем, конкретних схем та протоколів з відкритим ключем є обов'язковим для фахівців усіх спеціальностей, пов'язаних з інформаційними технологіями.

Дисципліна “Асиметричні криптосистеми та протоколи” знайомить студентів з теоретичними основами криптографії з відкритим ключем, асиметричними системами шифрування, різноманітними криптографічними протоколами та їх застосуванням у системах захисту банківської та комерційної інформації, а також з новими перспективними напрямками розвитку криптології.

Курс “Асиметричні криптографічні системи та протоколи” має своєю *метою* дати студентам знання в галузі криптографії з відкритим ключем. Дисципліна знайомить з теорією складності функцій та алгоритмів, складнооборотними функціями та їх застосуванням для побудови асиметричних криптосистем, різноманітними криптографічними протоколами, зокрема з протоколами автентифікації, цифрового підпису тощо. У курсі розглядаються приклади застосування криптографічних протоколів у електронній комерції та електронному голосуванні. Значна увага приділена криптосистемам на еліптичних кривих.

Після засвоєння навчальної дисципліни студенти мають продемонструвати:

1) Знання:

- основних понять теорії складності алгоритмів;
- конкретних важкооборотних функцій, що застосовуються в асиметричній криптографії, їх класифікації;
- основних асиметричних схем шифрування;
- способів побудови та використання у криптографії геш-функцій, відомих стандартів гешування;
- різноманітних криптографічних протоколів, включаючи протоколи цифрового підпису, автентифікації, доведення без розголошення тощо;
- протоколів електронної комерції та електронного голосування.
- можливих криптоатак на асиметричні криптосистеми, оцінки їх складності;
- теорії імітостійкості Симмонса;
- основ криптографії на еліптичних кривих та стандартів цифрового підпису на еліптичних кривих, зокрема, стандарту ДСТУ 4145.

2) Уміння:

- оцінювати часову складність алгоритмів;
- генерувати параметри асиметричних криптосистем;
- використовувати важкооборотні функції для побудови асиметричних криптосистем;
- виконувати криптоаналіз деяких криптосистем з відкритим ключем;
- програмно реалізовувати асиметричні криптосистеми;
- оцінювати доцільність застосування тієї чи іншої асиметричної криптосистеми у складі комплексної системи захисту інформації.

3) Досвід:

- генерування параметрів асиметричних криптосистем, зокрема, застосування алгоритмів перевірки чисел на простоту;
- програмної реалізації схем шифрування з відкритим ключем, побудованих на задачах дискретного логарифмування та факторизації;
- програмної реалізації та дослідження властивостей найуживаніших алгоритмів цифрового підпису;
- криптоаналізу деяких криптографічних протоколів.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні компетентності та результати навчання за Стандартом вищої освіти:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями.

ЗК 3 – Здатність генерувати нові ідеї (креативність).

ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК 8 – Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 10 – Навички у використанні інформаційних і комунікаційних технологій.

ЗК 13 – Навички міжособистісної взаємодії.

Фахові компетентності

ФК 1 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі.

ФК 3 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

ФК 7 – Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.

ФК 9 – Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.

ФК 13 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

ФК 14 – Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.

ФК 17 – Здатність проектувати, розробляти, реалізовувати та провадити первинний аналіз криптографічних алгоритмів різного профілю

ФК 18 – Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем

Програмні результати навчання

ПРН 1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.

ПРН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів.

ПРН 7 – Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач.

ПРН 11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символічних алгоритмів.

ПРН 13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.

ПРН 14 – Виявляти здатність до самонавчання та продовження професійного розвитку.

ПРН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

ПРН 16 – Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.

ПРН 19 – Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

ПРН 22 – Володіти основними принципами та методами побудови симетричних та асиметричних криптографічних систем у різних моделях обчислення, а також методами їх аналізу

ПРН 23 – Використовувати у професійній діяльності криптографічні примітиви та протоколи.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліну забезпечують освітні компоненти «Дискретна математика», «Алгебра та геометрія», «Програмування», «Теорія ймовірностей» «Математична статистика», «Прикладна алгебра», «Алгоритми та структури даних», «Матлогіка та теорія алгоритмів», «Теорія складності», «Спеціальні розділи обчислювальної математики», «Симетрична криптографія».

Одержані знання та навички будуть необхідними для проведення самостійних досліджень в галузі криптології (зокрема, при виконанні дипломної роботи бакалавра) та у практичній діяльності за фахом.

3. Зміст навчальної дисципліни

Розділ 1. Основи асиметричної криптографії. Криптосистеми на односторонніх функціях Діффі-Геллмана і RSA

Тема 1.1. Основні схеми асиметричної криптографії.

Тема 1.2. Криптосистеми, що базуються на односторонній функції дискретного піднесення до степеня. Складність алгоритмів.

Розділ 2. Геш-функції. Цифровий підпис з геш-функцією.

Тема 2.1. Властивості геш-функцій. Цифрові підписи з геш-функціями.

Розділ 3. Криптосистеми на односторонній функції Рабіна.

Тема 3.1. Криптосистеми шифрування та цифрового підпису Рабіна

Тема 3.2. Алгоритми доведення без розголошення.

Розділ 4. Криптографічні протоколи

Тема 4.1. Протоколи генерування випадкових біт та розділення секретів.

Тема 4.2. Спеціальні цифрові підписи. Протокол електронної готівки.

Тема 4.3. Електронні вибори.

Розділ 5. Імітостійкість та аутентифікація.

Тема 5.1. Теорія імітостійкості.

Розділ 6. Квантова криптографія. Криптосистеми на еліптичних кривих.

Тема 6.1. Квантова криптографія.

Тема 6.2. Криптосистеми на еліптичних кривих.

4. Навчальні матеріали та ресурси

1. *Анісімов А.В.* Алгоритмічна теорія великих чисел. К.: Академперіодика, 2001. – 218с.
2. *Вербіцький О.В.* Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
3. *Koblitz N.* A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – 312 p.
4. Математичні методи захисту інформації. Курс лекцій. Ч I. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
5. *Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я.* Математичні основи криптографії. – Дніпропетровськ: Національний гірничий університет, 2004. – Ч.1. – 391 с.
6. *Сушко С.О., Кузнецов В.Г., Фомичева Л.Я., Корабльов А.В.* Математичні основи криптоаналізу. – Д.: Національний гірничий університет, 2010. – 466 с.
7. *Задірака В.К., Олексюк О.С.* Комп'ютерна криптологія. – К.: 2002. – 504 с.
8. *Katz Jonathan, Lindell Yehuda.* Introduction to Modern Cryptography. – Boca Raton London New York: Chapman & Hall /CRC Taylor & Francis Group, 2008. – 534 p.

9. *Henk C.A. van Tilborg*. Fundamentals of Cryptology. – A Professional Reference and Interactive Tutorial. – Kluwer Academic Publishers, 1999, 2000. Second Printing 2001.
10. *Mao Wenbo*. Modern Cryptography. Theory and Practice. - Prentice Hall PTR, Upper Saddle River, New Jersey, 2004.
11. *Schneier B.* Applied Cryptography: protocols, algorithms and source code in C. John Wiley & Sons, New York, 1996.
12. Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography [електронний ресурс]. – 2008. – <https://cseweb.ucsd.edu/~mihir/papers/gb.pdf>
13. Oded Goldreich. Foundations of Cryptography [електронний ресурс]. – 1998-2003. – <https://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html>

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються такі методи навчання: для лекційних занять – пояснювально-ілюстративний метод та метод проблемного викладу; для практичних занять – репродуктивний метод та метод проблемного викладу. Виконання комп'ютерних практикумів передбачає використання частково-пошукового методу, а виконання та захист розрахункової роботи – використання частково-пошукового та дискусійного методів.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Односторонні функції. Функція дискретного піднесення до степеня. Схема Діффі-Геллмана розповсюдження ключів відкритими каналами.
2	Односторонні функції з секретом. Одностороння функція RSA. Криптосистема RSA. Поняття цифрового підпису. Шифрування та підпис в RSA.
3	Системи шифрування, що базуються на односторонній функції Діффі-Хелмана: криптосистеми Мессі-Омури, шифрування та цифрового підпису Ель-Гамала.
4	Складність алгоритмів та односторонні функції.
5	Можливі атаки на цифровий підпис без геш-функції. Геш-функції. Методи побудови криптографічних геш-функцій. Характеристики відомих геш-функцій.
6	Цифрові підписи з геш-функціями. Атаки на цифровий підпис з побудовою колізій.
7	Одностороння нкція з секретом Рабіна. Добуток квадратних коренів за модулем.
8	Система шифрування та цифровий підпис Рабіна.
9	Протоколи доведення з нульовим розголошенням.
10	Протоколи генерування випадкових біт (схема Блюма-Мікалі). Протоколи розділення секретів.
11	Спеціальні цифрові підписи. Сліпий цифровий підпис. Протокол електронної готівки. Невидимий цифровий підпис.
12	Протоколи електронного голосування.
13	Теорія імітостійкості Сіммонса.
14	Ідентифікація та автентифікація. Криптографічні протоколи автентифікації.
15	Квантова криптографія. Квантовий протокол передачі ключа.
16	Еліптичні криві.
17	Криптосистеми на еліптичних кривих.
18	Стандарти цифрового підпису на еліптичних кривих.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Математичні основи криптографії. Властивості циклічних груп та генераторів
2	Квадратичні лишки та псевдоквадрати
3	Розв'язування квадратних рівнянь за модулем
4	Властивості простих чисел, тестування простоти
5	Оцінювання складності алгоритмів
6	МКР частина 1
7	Властивості криптосистем, побудованих на задачі дискретного логарифмування: схеми відкритого розподілу ключів Діффі-Хеллмана, системи шифрування Мессі-Омури.
8	Властивості схеми шифрування Ельгамалю
9	Властивості схеми цифрового підпису Ельгамалю та схем типу Ельгамалю (DSA, Шнорра тощо)
10	Властивості схем шифрування та цифрового підпису RSA
11	Атаки на схему RSA
12	Властивості криптосистеми Рабіна
13	Криптографічні властивості геш-функцій
14	Аналіз властивостей криптографічних протоколів (протоколу вироблення спільних бітів, протоколів розподілу секрету тощо)
15	Криптографічно стійкі генератори псевдовипадкових бітів. Імовірнісне шифрування
16	Застосування еліптичних кривих у криптографії
17	МКР частина 2
18	Захист розрахункових робіт

Комп'ютерний практикум

Для закріплення теоретичних знань та формування необхідних практичних навичок студенти повинні виконати три комп'ютерних практикуми:

- 1) побудова тестів для перевірки якості випадкових та псевдовипадкових послідовностей;
- 2) вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем;
- 3) криптосистема Рабіна; атака на протокол доведення знання без розголошення.

Комп'ютерні практикуми можуть виконуватись самостійно або у парі. У другому випадку виконання задач практикумів розподіляється між учасниками на власний розсуд, а оцінка за виконання ставиться обом учасникам однакова, за фактичне виконання задач практикумів.

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до модульної контрольної роботи.

При виконанні комп'ютерного практикуму студент має розібратися у відповідному теоретичному матеріалі за допомогою наданої літератури включно з методичними вказівками до даного практикуму, написати відповідну комп'ютерну програму та зробити за її допомогою вказані у методичних вказівках обчислення. Викладач, що проводить практикум, консультує студентів з питань його виконання, перевіряє правильність роботи програми та приймає усний звіт

студента з питань створення комп'ютерної програми та відповідного теоретичного матеріалу. Крім того, викладачем проводиться перевірка програми на плагіат.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати індивідуальне семестрове завдання. Завдання включає в себе розкриття певної теми з теоретичного матеріалу у вигляді аналітичного звіту та захист цього звіту на семінарському занятті. Завдання на роботу надає викладач, який також встановлює граничні строки для її здачі; студенту надається не менше двох місяців на виконання.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу, підготовка до тестів з теорії	12
2.	Підготовка до практичних занять	18
3.	Виконання комп'ютерних практикумів	18
4.	Підготовка до виконання модульної контрольної роботи	2
5.	Виконання індивідуального завдання	10
6.	Підготовка та складання іспиту	30
	Усього	90

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Відвідування занять з комп'ютерних практикумів є обов'язковим тільки для захисту поставлених на практикумі завдань, а також для одержання консультацій викладачів щодо виконання завдань.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Студент, який без поважних причин пропустив захист індивідуального завдання, не допускається до складання іспиту. Якщо пропуск стався з поважної причини, захист розрахункової роботи дозволяється в інший узгоджений із викладачем час.

Пропущений іспит не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен скласти іспит на додатковій сесії.

Оголошення результатів контрольних заходів

Результати виконання контрольних заходів оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються оціночними листами, в яких студенти можуть побачити свою оцінку за певними критеріями, а також позначення основних помилок та коментарі до них.

Результати модульної контрольної роботи вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Захист виконаного індивідуального семестрового завдання проводиться у формі публічного презентаційного захисту. Результати захисту оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок.

На усному екзамені студенту оголошується оцінка після закінчення відповіді на кожне теоретичне питання або задачу із зазначенням усіх помилок, коментарями, зауваженнями тощо, після чого оголошується загальна оцінка за екзамен, що є сумою оцінок за теоретичні питання та задачі.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

У разі виявлення порушень норм академічної доброчесності під час виконання контрольного заходу студент одержує за цей захід нуль балів без можливості повторного виконання.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

№	Контрольний захід	Макс бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	0,8	10	8
2.	Модульна контрольна робота	20	1	20
3.	Теоретичне опитування	3	2	6
3.	Комп'ютерні практикуми	6	3	18
4.	Індивідуальне семестрове завдання	8	1	8
4.	Іспит	40	1	40
	Усього			100

Критерії оцінювання контрольних заходів

1) Виконання домашніх завдань

Усі домашні завдання перевіряються у кожного студента протягом семестру. Одне домашнє завдання оцінюється у 0,8 рейтингових бали.

Критерії оцінювання одного домашнього завдання:

- Правильне повне виконання усіх завдань 100% оцінки
- Виконання з деякими неточностями 75-99% оцінки
- Виконання не менш ніж 50% усіх завдань 50-74% оцінки
- Наявність окремих правильно виконаних завдань 25-49% оцінки
- Усі завдання повністю неправильні 0 балів
- Домашнє завдання не здано 0 балів

Домашнє завдання, яке не було здано або було здано після дедлайну, вважається невиконаним і автоматично оцінюється у 0 балів.

Максимальна кількість балів, яку можна одержати за домашні завдання, дорівнює 8. Загальна кількість балів, яку студент одержує за домашні завдання, дорівнює сумі балів за кожне перевірене домашнє завдання.

2) Модульна контрольна робота

Модульна контрольна робота (МКР) складається з декількох частин, які проводяться протягом семестру по мірі опанування теоретичного та практичного матеріалу. Кількість задач та їх вартість у балах визначається викладачами в залежності від складності самої задачі та об'єму винесеного на дану частину МКР матеріалу.

Критерії оцінювання однієї задачі МКР:

- Правильне повне розв'язання без помилок 100% оцінки
- Розв'язання з несуттєвими помилками та/або описками 90-99% оцінки
- Розв'язання з деякими неточностями 70-89% оцінки
- Розв'язання із правильною ідеєю, але грубими помилками 50-69% оцінки
- Наявність правильної ідеї розв'язку з неправильним її застосуванням або незакінченим розв'язком 30-49% оцінки
- Розв'язок повністю неправильний або відсутній 0% оцінки

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Виконання частини МКР, пропущеної з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за модульну контрольну роботу, дорівнює 20. Загальна кількість балів, яку студент одержує за одну частину модульної контрольної, дорівнює сумі балів за кожне завдання у відповідності до їх вартості та наведених

критеріїв оцінювання. Загальна кількість балів, яку студент одержує за модульну контрольну роботу, дорівнює сумі балів за виконання усіх її частин.

3) Тести з теоретичного матеріалу

Протягом семестру по мірі опанування теоретичного матеріалу студенти пишуть два тести. Тести складаються із відкритих питань та питань із мультिवибором відповіді. Кількість питань та їх вартість у балах визначається викладачами.

Критерії оцінювання одного тестового питання:

- | | |
|---|-------------|
| • Правильна відповідь | 100% оцінки |
| • Обрано не усі правильні відповіді | 50% оцінки |
| • Відкрита відповідь містить суттєві неточності | 50% оцінки |
| • Обрана хоча б одна неправильна відповідь | 0% оцінки |
| • Відкрита відповідь є неправильною | 0% оцінки |

Студент, який без поважних причин пропустив тест, одержує за нього нуль балів без можливості перескладання. Виконання тесту, пропущеного з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за один тест, дорівнює 3 бали. Загальна кількість балів, яку студент одержує за один тест, дорівнює сумі балів за кожне тестове питання у відповідності до їх вартості та наведених критеріїв оцінювання.

4) Комп'ютерні практикуми

Комп'ютерні практикуми виконуються самостійно, бригадами по два студенти або одноосібно. Кожен комп'ютерний практикум оцінюється в 6 балів. Оцінка за комп'ютерний практикум формується з таких складових:

- | | |
|---------------------------------------|-----------------|
| – практична частина (програмний код): | 50% від оцінки; |
| – протокол виконання практикуму: | 25% від оцінки; |
| – захист (теоретична частина): | 25% від оцінки. |

Зданий протокол та захист практикуму є необхідними умовами його зарахування.

Здача комп'ютерного практикуму після призначеного терміну виконання без поважної причини приводить до зниження оцінки за нього на 0,5 балу за кожен тиждень запізнення; максимальне зниження оцінки за пропуск дедлайну – 1,5 балу.

Через чотири тижні після призначеного терміну виконання комп'ютерні практикуми перестають прийматись. Можливість здати та захистити такі комп'ютерні практикуми буде надана один раз перед перескладанням дисципліни.

5) Індивідуальне семестрове завдання

Індивідуальне семестрове завдання (ІСЗ) виконується у формі наукового звіту об'ємом 10-15 сторінок за наданою формою. Оцінювання ІСЗ складається з двох етапів: безпосереднього виконання студентом індивідуального завдання та його презентаційний захист; кожна частина дає до 50% від оцінки.

Критерії оцінювання індивідуального завдання:

- | | |
|--|---------------|
| • Змістовна частина | 50% оцінки |
| ○ Тема завдання глибоко та детально розкрита | 50% оцінки |
| ○ Тема завдання розкрита поверхнево | 25-49% оцінки |
| ○ Тема завдання розкрита фрагментарно | 10-24% оцінки |
| ○ Тема завдання не розкрита | 0% оцінки |

- Представлення результатів 50% оцінки
 - Робота оформлена охайно, структуровано, матеріал логічно пов'язаний 50% оцінки
 - Робота оформлена неохайно, із порушенням логіки викладення матеріалу 25-49% оцінки
 - Робота оформлена хаотично і не відображує жодної авторської думки 10-24% оцінки
 - Робота не виконана 0 балів за роботу

Максимальна кількість балів, яку можна одержати за індивідуальне завдання, дорівнює 8.

У випадку виявлення використання великих мовних моделей для генерування тексту звіту завдання автоматично вважатиметься невиконаним із оцінкою 0 балів.

Здача індивідуального завдання після призначеного терміну виконання без поважної причини приводить до зниження оцінки за неї на 0,25 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 2 бали. Індивідуальне завдання, здане через вісім днів після призначеного терміну, автоматично вважається невиконаним та оцінюється у 0 балів.

У такому випадку можливість виконати та захистити ІСЗ буде надана один раз

Виконання та захист РР є обов'язковою умовою допуску до іспиту.

5) Семестрова атестація (іспит)

Семестрова атестація (іспит) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Іспит включає в себе

- практичну частину (3 задачі, 18 балів);
- теоретичний тест (10 питань, 10 балів);
- теоретичну частину (1 теоретичне питання із розгорнутою відповіддю, 12 балів);

Критерії оцінювання задач практичної частини співпадають з критеріями оцінювання задач МКР. Критерії оцінювання тестових питань співпадають із критеріями для тестів з теоретичного матеріалу.

Критерії оцінювання теоретичного питання із розгорнутою відповіддю:

- Студент демонструє вичерпне розуміння теоретичного матеріалу 100% оцінки
- Студент відповідає з незначними неточностями 90-99% оцінки
- Студент відповідає з суттєвими неточностями 60-89% оцінки
- Відповіді студента лише частково вірні 30-59% оцінки
- Відповіді студента містять лише окремі вірні положення 10-29% оцінки
- Студент демонструє повне незрозуміння теоретичного матеріалу 0 балів

Під час іспиту забороняється використання будь-яких додаткових довідкових матеріалів.

Заохочувальні бали

Модульна контрольна робота може включати в себе додаткові задачі, правильне розв'язання яких оцінюється бонусними (заохочувальними) балами поза шкалою семестрового рейтингу. Окрім цього, на практичних заняттях можуть бути сформульовані додаткові аудиторні чи домашні завдання, виконання яких у встановлені терміни також оцінюється заохочувальними балами.

Студенти, які склали іспит не менш ніж на 36 балів, мають право одержати бонусне завдання, розв'язання якого також надасть до 6 заохочувальних балів.

Студенти можуть одержати заохочувальні бали за опанування тематичних онлайн-курсів (наприклад, курс “Cryptology” Дана Боне на платформі Coursera), які не були зараховані у дисципліні «Симетрична криптографія». Для цього студент повинен заздалегідь перевірити у

викладача відповідність онлайн-курсу дисципліні та узгодити граничний термін опанування онлайн-курсу. Кількість заохочувальних балів у такому випадку буде визначатись результатами проходження такого курсу.

Загальна кількість заохочувальних балів, які можна одержати за дисципліну: 10 балів.

Умови одержання проміжної атестації

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях семестру. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Умови допуску до семестрової атестації

Необхідною умовою допуску до семестрової атестації є

- семестровий рейтинг не менше 25 балів;
- виконані та здані усі комп'ютерні практикуми;
- виконане та захищене індивідуальне семестрове завдання.

Студенти, які протягом семестру отримали від 10 до 25 балів, але виконали інші умови допуску, не допускаються до складання іспиту. Замість іспиту такі студенти виконують письмову допускну роботу (10 задач, 20 балів), результати якої додають до семестрового рейтингу; якщо після виконання допускну роботи семестровий рейтинг стає більшим 30 балів, студент допускається до семестрової атестації на перескладанні, а його семестровий рейтинг вважається таким, що дорівнює 30 балів; в іншому випадку результати допускну роботи анулюються, а на перескладанні студент повторно виконує допускну роботу.

Студенти, які не виконали індивідуальне семестрове завдання та/або комп'ютерні практикуми, не допускаються до складання іспиту. Таким студентам буде надана можливість здати та захистити ІСЗ та/або комп'ютерні практикуми перед додатковою сесією, щоб одержати допуск до перескладання дисципліни.

Студенти, які протягом семестру одержали менше 10 балів, не допускаються до складання чи перескладання семестрової атестації та рекомендуються кафедрі на відрахування або повторне переслуховування дисципліни.

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і іспит. Для допуску до перескладання студент повинен одержати не менше 30 рейтингових балів (з урахуванням першої спроби складання іспиту або допускну роботи), виконати і захистити розрахункову роботу, виконати і захистити усі комп'ютерні практикуми. На перескладанні результати основного іспиту анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів перескладання.

Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізований атестаційній комісії. Формат повторного перескладання визначається комісією.

Підсумкова оцінка з дисципліни

Рейтингова оцінка складається з результатів виконання семестрових контрольних заходів (включно з заохочувальними) та результатів усного іспиту або його перескладання. Оцінка за стобальною шкалою переводиться до університетської шкали оцінок за наведеною таблицею відповідності.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Склав: доцент кафедри ММЗІ, к.т.н. Яковлев Сергій Володимирович

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2 від 25.06.2025 р.).

Затверджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2025 року)