



СИМЕТРИЧНА КРИПТОГРАФІЯ (ПО 20)

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 підготовки)</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>3 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 6 кредитів ЕКТС / 180 годин Лекційних занять: 36 годин Практичних занять: 36 години Комп'ютерних практикумів: 18 годин Самостійна робота студентів: 90 годин</i>
Семестровий контроль/ контрольні заходи	<i>екзамен, МКР, РР</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектори: доц. Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua) Практичні: доц. Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua) Комп'ютерні практикуми: ас. Якимчук Олексій Петрович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Проблеми безпеки інформації за останні роки набули виключної актуальності, при цьому забезпечення захисту інформаційних технологій приймає комплексний характер. Серед різних методів захисту інформації (технічних, правових, організаційних та інших) найважливіше місце займають криптографічні методи. За останні десятиріччя криптологія сформувалася у самостійну наукову дисципліну, що має свою специфіку постановок задач та методів їхнього дослідження. Знання основних понять криптології, володіння криптографічними методами захисту інформації за сучасних умов вкрай необхідні будь-якому фахівцю, що займається створенням систем захисту інформації.

Дисципліна знайомить студентів з класичними шифрами, теорією Шеннона, криптографічними властивостями булевих функцій, сучасними блоковими та потоковими системами шифрування, принципами їх побудови та способами застосування.

При викладенні матеріалу дисципліни виділяються такі аспекти:

- основні теоретичні поняття;

- математичні моделі та обчислювальні алгоритми, що базуються на вивчених поняттях;
- застосування розглянутих моделей та алгоритмів у сучасних інформаційних технологіях.

Метою дисципліни є формування у студентів здатностей оперування основними сучасними поняттями симетричної криптографії, побудови математичних моделей криптосистем, криптографічних алгоритмів. Студент має бути здатним розібратися у наявних моделях, схемах криптографічних систем, описаних у спеціальній літературі.

У результаті вивчення курсу студент повинен продемонструвати такі результати навчання:

знання:

математичних основ, які складають фундамент модуля: алгоритми класичної криптографії, теорію Шеннона секретних систем, криптографічні властивості та апарат булевих функцій, теорію рекурентних послідовностей над скінченими полями;

основні схеми, конструкції та алгоритми сучасних криптографічних систем блокового та поточного шифрування;

основні методи та способи реалізації та правильного застосування криптографічних алгоритмів та схем симетричної криптографії;

основ криптографічної стійкості, методів частотного аналізу.;

уміння:

аналізувати криптографічні алгоритми, оцінювати їх криптографічні властивості;

проекувати системи криптографічного захисту інформаційних об'єктів, структур з обміном інформацією, телекомунікацій, що задовольняють задані вимоги;

досвід:

застосування теоретичних знань для розв'язання задач побудови криптографічних алгоритмів, систем криптографічного захисту інформації, аналізу їх стійкості;

обґрунтування вибору криптографічних засобів та методів для побудови систем захисту інформації.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знанням

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 спеціальності

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 форм

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)

Для засвоєння матеріалу курсу «Симетрична криптографія» студент повинен успішно опанувати курси «Алгебра та геометрія», «Дискретна математика», «Прикладна алгебра», «Теорія складності», «Комбінаторний аналіз» та «Спеціальні розділи обчислювальної математики». Успішне опанування курсу «Теорія імовірностей» сприяє поглибленню та закріпленню компетентностей та результатів навчання. Для виконання комп'ютерних практикумів необхідне успішне опанування дисциплін «Програмування» та «Алгоритми та структури даних».

Отримані практичні навички та засвоєнні знання необхідні для опанування дисципліни «Асиметричні криптосистеми та протоколи» та для виконання науково-дослідницької та прикладної діяльності у галузі криптології.

3. Зміст навчальної дисципліни

Розділ 1. Основи класичної криптографії

Тема 1.1. Класичні схеми шифрування

Тема 1.2. Теорія Шеннона

Розділ 2. Булеві функції та їх криптографічні властивості

Тема 2.1. Булеві функції та їх криптографічні властивості

Розділ 3. Симетричні криптографічні системи

Тема 3.1. Системи блокового шифрування

Тема 3.2. Системи потокового шифрування

4. Навчальні матеріали та ресурси

Рекомендована література

1. Математичні методи захисту інформації : курс лекцій для студ. напр. 0802 "Прикладна математика", 0804 "Комп'ютерні науки", 1601 "Інформаційна безпека" / Укл. Л. О. Завадська, М. М. Савчук; Міністерство освіти і науки України, НТУУ "КПІ". - Київ : НТУУ "КПІ", 2008. – 128 с.
2. Корченко, Олександр Григорович. Прикладна криптологія: системи шифрування : підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс ; Міністерство освіти і науки України, Житомирський військовий інститут імені С.П. Корольова Державного університету телекомунікацій. – Житомир : [б. в.] ; 2014. - 447 с.
3. Фаль, Олексій Михайлович. Криптографія: основні ідеї та застосування : Препринт / О.М. Фаль. - К. : Політехніка, 2003. - 28 с.
4. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
5. Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography [електронний ресурс]. – 2008. – <https://cseweb.ucsd.edu/~mihir/papers/gb.pdf>
6. Oded Goldreich. Foundations of Cryptography [електронний ресурс]. – 1998-2003. – <https://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html>

Відеозаписи лекцій викладено на Youtube-каналі кафедри ММЗІ та доступні за такими посиланнями: <https://www.youtube.com/playlist?list=PLhCN8H4P5Lv6lB15aY8GUSpMb8IHn0i->

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 – пояснювально-ілюстративний метод, репродуктивний метод та метод проблемного викладу. Захист розрахункової роботи та комп'ютерних практикумів передбачає використання дискусійного методу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Цілі, напрямки, методи і аспекти захисту інформації. Криптологія. Задачі криптографії та криптоаналізу. Початкові поняття криптології та етапи розвитку. Класифікація криптосистем. Класична криптографія: терміни, поняття, позначення, типи шифрів. Визначення шифру підстановки (заміни). Моноалфавітні підстановки: визначення, загальний шифр простої підстановки.
2	Моноалфавітні шифри класичної криптографії: Цезаря, афінної заміни, шифр Полібія, книжковий шифр. Частотний аналіз шифру Цезаря, афінної підстановки.
3	Блокові (табличні) підстановки: шифр Плейфера, афінна біграмна заміна, шифр Хілла, шифр біграмної підстановки та його частотний аналіз.
4	Визначення поліалфавітної підстановки. Модульне шифрування. Класичні поліалфавітні шифри: Віженера, шифр з автоключем, аперіодичні поліалфавітні шифри, книжковий шифр з бігучим рядком, шифр Вернама (одноразовий блокнот). Частотний аналіз шифру Віженера.
5	Визначення шифру загальної перестановки. Класичні шифри перестановки: скітала, частоколу, табличні перестановки, маршрути Гамільтона, ґрати Кардано, магічні квадрати. Класифікація класичних шифрів.
6	Поняття ентропії, властивості ентропії імовірнісних ансамблів, сумісна та умовна ентропія, взаємна інформація. Джерела дискретних сигналів, ентропія на символ джерела, надлишковість. Моделі джерел відкритого тексту.
7	Поняття стійкості, теоретична і практична стійкість. Правило Керкгоффа. Ієрархія типів атак на криптосистему за рівнем доступної криптоаналітиці інформації. Підходи до криптоаналізу класичних шифрів на основі шифрованих текстів та на основі відкритих текстів.
8	Загальна схема секретного зв'язку. Поняття криптосистеми. Математична модель Шеннона симетричного шифру. Припущення Шеннона. Формули для розрахунку сумісних і умовних розподілів в математичній моделі шифру. Цілковито таємна криптосистема. Необхідні і достатні умови цілковитої таємності. Межа Шеннона. Цілковита таємність шифру Вернама.
9	Ненадійність ключа і відкритого тексту. Теореми про ентропію ключів за умовою криптограми та про середнє число хибних ключів (із доведенням). Функція ненадійності ключа. Відстань однозначності: визначення, доведення формули, інтерпретація, застосування. Принципи Шеннона: розсіювання і перемішування. Підхід до побудови стійких криптосистем, запропонований Шенноном. Класифікація сучасних криптосистем

10	Одновимірні та багатовимірні булеві функції. Способи представлення булевих функцій: таблиці істинності, формули, ДДНФ, розклад Шеннона. Поліном Жегалкіна (АНФ), алгебраїчний степінь булевої функції. Швидке перетворення Мебіуса. Спектральні представлення булевих функцій. Ряд та коефіцієнти Фур'є, перетворення та коефіцієнти Уолша. Швидке перетворення Фур'є. Властивості коефіцієнтів Фур'є та Уолша, рівність Парсеваля.
11	Криптографічні властивості булевих функцій. Невиродженість, відсутність заборон, збалансованість, згладжування. Статистичні аналоги булевих функцій. Нелінійність як відстань до класу афінних функцій, вивід формули, оцінка. Поняття бент-функції.
12	Кореляційний імунітет булевих функцій: різні визначення, зв'язок із коефіцієнтами Уолша Лавинні ефекти булевих функцій. Строгі лавинні критерії та критерії поширення. Похідні булевих функцій, функція автокореляції та її зв'язок із критеріями поширення.
13	Потокові шифри: визначення, загальна модель. Типи генераторів гама. Внесення нелінійності у схеми на основі реєстрів зсуву із лінійним зворотним зв'язком.
14	Типи атак на потокові шифри. Кореляційна атака на схему нелінійної комбінації (на прикладі генератору Геффа). Сучасні потокові шифри
15	Симетричні блокові шифри: визначення, загальні властивості. Принципи побудови сучасних блокових шифрів. Схеми блокового шифрування: SP-мережа, схема Фейстеля, їх властивості.
16	Стандарт шифрування DES: схема роботи, характеристики, недоліки. Модифікації алгоритму DES. Шифри, побудовані на основі схеми Фейстеля. Стандарт шифрування ДСТУ ГОСТ 28147:2009: схема роботи, характеристики.
17	Стандарт шифрування AES: схема роботи, структура, характеристики. Швидка реалізація AES. Стандарти шифрування ДСТУ 7624:2014 «Калина» та ГОСТ Р 34.12-2015 «Кузнечік»: схема роботи, основні характеристики.
18	Режими роботи блокових шифрів, основні характеристики. Вплив спотворень у шифротекстах на відкриті тексти у різних режимах роботи.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Шифри перестановки та їх властивості
2	Шифри підстановки: шифр Цезаря, шифр Віженера, диск Альберті, їх властивості
3	Афінні шифри та шифри Хілла. Групові властивості шифрів.
4	Криптоаналіз шифру Віженера. МКР, частина 1.
5	Ентропія імовірнісного ансамблю та її властивості
6	Сукупна та умовна ентропії, взаємна інформація, їх властивості.
7	Джерела дискретних сигналів. Моделі відкритого тексту.
8	Теорія Шеннона, цілком таємні шифри.
9	Відстань однозначності та її оцінювання. МКР, частина 2.
10	Булеві функції та їх представлення. Класи булевих функцій.
11	Коефіцієнти Фур'є та Уолша булевих функцій, їх властивості. Нелінійність булевих функцій, бент-функції.
12	Кореляційний імунітет булевих функцій.
13	Похідна булевої функції та її властивості. Лавинні ефекти, строгі лавинні критерії.

14	Лінійні структури булевих функцій. МКР, частина 3.
15	Блокові шифри, схеми побудови. Властивості SP-мереж та схем Фейстеля.
16	Режими роботи блокових шифрів та їх властивості.
17	Потокові шифри, схеми побудови та властивості.
18	МКР, частина 4.

Комп'ютерні практикуми

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

1) обчислення статистичних властивостей мови, розподілів символів та біграм, оцінювання ентропії на символ мови;

2) криптоаналіз шифру Віженера;

3) криптоаналіз шифру афінної біграмної заміни;

4) побудова кореляційної атаки на генератор Геффа.

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

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 самостійних та модульних контрольних робіт.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу за темою «Булеві функції та їх криптографічні властивості». Для підготовки до виконання розрахункової роботи слід скористатися рекомендованою літературою, конспектом та/або відеозаписами лекцій. Студенту надається не менше двох тижнів на виконання розрахункової роботи, після чого в узгоджений із викладачем час студент повинен захистити виконану роботу.

Виконання комп'ютерного практикуму сприяє формуванню навичок самостійної та творчої роботи (пошуку додаткових матеріалів, формалізація поставлених задач, реалізація алгоритмів їх розв'язування); також, при виконанні практикуму в бригаді, формуються навички колективної роботи над розробницькими проектами.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу	12
2.	Підготовка до практичних занять	18
3.	Підготовка до 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 необхідні навички. 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 розрахункової роботи, 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 домашніх завдань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження.

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 виконаної та оформленої розрахункової роботи проводиться у формі співбесіди з викладачем. Під час захисту студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач. Результати виконаної та повністю оформленої РР у встановлений викладачем термін кожен студент захищає індивідуально. Результати захисту оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок.

Результати письмової частини іспиту вказуються на бланках для письмової екзаменаційної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини іспиту/заліку оголошуються наприкінці її проходження.

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, рейтингової системи оцінювання та/або зауважень.

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

№	Контрольний захід	Макс бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	2	≥ 3	6
3.	Модульна контрольна робота	28	1	28
4.	Розрахункова робота	8	1	8
5.	Комп'ютерні практикуми	4 / 6	4	18
6.	Іспит	40	1	40
	Усього			100

Критерії оцінювання контрольних заходів

1) Виконання домашніх завдань

Домашні завдання перевіряються вибірково та випадковим чином, однак у кожного студента буде не менше трьох перевірянь домашніх завдань протягом семестру. Одне домашнє завдання оцінюється у 2 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

Здача домашнього завдання після назначеного терміну виконання без поважної причини приводить до зниження оцінки за нього на 0,05 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 0,4 бали. Домашнє завдання, яке не було здано або було здано більш ніж через вісім днів після дедлайну, вважається невиконаним і автоматично оцінюється у 0 балів.

Максимальна кількість балів, яку можна одержати за домашні завдання, дорівнює 6. Загальна кількість балів, яку студент одержує за домашні завдання, дорівнює сумі балів за кожне перевірене домашнє завдання. Якщо одержана сума перевищує 6 балів, вона встановлюється у 6 балів.

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 28. 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) Розрахункова робота

Розрахункова робота (РР) складається з декількох завдань. Кожен студент одержує своє індивідуальне завдання для виконання. Кількість задач та їх вартість у балах визначається викладачами та наводиться у завданні на РР. Оцінювання РР складається з двох етапів: безпосереднього виконання студентом індивідуального завдання та його захист у викладача; кожна частина дає до 50% від оцінки за кожну задачу РР.

Критерії оцінювання одного завдання РР:

- | | |
|--|---------------|
| • Повне розв'язання без помилок, правильна відповідь | 50% оцінки |
| • Правильне розв'язання із неправильною відповіддю через неточності та арифметичні помилки | 25-49% оцінки |
| • Розв'язання із правильною ідеєю, але грубими помилками | 10-24% оцінки |
| • Розв'язок повністю неправильний або відсутній | 0% оцінки |

Критерії оцінювання захисту одного завдання РР:

- | | |
|---|---------------------|
| • Студент демонструє вичерпне розуміння наведеного розв'язку та відповідного теоретичного матеріалу | 50% оцінки |
| • Студент відповідає з неточностями та помилками | 30-49% оцінки |
| • Відповідь студента містить окремі вірні положення | 10-29% оцінки |
| • Студент демонструє повне нерозуміння теоретичного матеріалу та наведеного розв'язку | 0 балів за завдання |

Максимальна кількість балів, яку можна одержати за виконання та захист РР, дорівнює 8.

Задача РР 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. АЛЕ: якщо РР була здана через вісім днів після призначеного терміну, вона автоматично оцінюється у 0 балів.

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

4) Комп'ютерні практикуми

Комп'ютерні практикуми виконуються самостійно, бригадами по два студенти або одноосібно. Перші три комп'ютерні практикуми оцінюються в 4 бали, четвертий 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 0,25 балу за кожен тиждень запізнення; максимальне зниження оцінки за пропуск дедлайну – 1 бал.

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) 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. Теоретичний тест складається із відкритих питань та питань із мультिवибором відповіді. Кожне питання оцінюється у 1 бал. 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

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 нерозуміння 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.

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 “Cryptography” Дана Боне на платформі Coursera). 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;
- виконана та здана розрахункова робота.

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 розрахункову роботу та/або комп'ютерні практикуми, не допускаються до складання іспиту. Таким студентам буде надана можливість здати та захистити розрахункову роботу 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. Яковлєв 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)