Національний технічний університет України «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»	Навчально-науковий фізико-технічний інститут Кафедра математичних методів захисту інформації

СИМЕТРИЧНА КРИПТОГРАФІЯ (ПО 6)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Обов'язкова (нормативна) (цикл професійної підготовки)*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*Загальна кількість: 5.5 кредитів ЄКТС / 165 годин* *Лекційних занять: 36 годин* *Практичних занять: 36 години* *Комп'ютерних практикумів: 18 годин* *Самостійна робота студентів: 75 годин*
Семестровий контроль/ контрольні заходи	*екзамен, МКР, РР*
Розклад занять	*http://rozklad.kpi.ua* *http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектори: професор Савчук Михайло Миколайович, д.ф.-м.н. (mikhail.savchuk@gmail.com), доцент Яковлєв Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua)* *Практичні: доцент Яковлєв Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua)* *Комп'ютерні практикуми: ас. Чорний Олег Миколайович*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання 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 кредитного модуля 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 кредитного модуля 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;

проектувати 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

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

РН 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.

РН 7 – Вміти проводити практичні дослідження та знаходити розв’язок некоректних задач.

РН 11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів

РН 13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп’ютерної математики

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

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

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

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

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

РН 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 опановувати 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. Основні поняття криптології. 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 потокового шифрування

Тема 3.2. Системи блокового шифрування

4. Навчальні матеріали та ресурси

Базова 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

Допоміжна рекомендована література

1. Завадська Л.О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006 – 54с.
2. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 2. Теорія чисел. – Вінниця: ВНТУ, 2017 – 129 с.
3. Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я. Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.
4. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія. – К.: 2002. – 504 с.
5. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації. – К.: Вища школа, 2002. – 457 с.
6. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. – Boca Raton London New York: Chapman & Hall /CRC Taylor & Francis Group, 2008. – 534 p.
7. Henk C.A. van Tilborg. Fundamentals of Cryptology. – A Professional Reference and Interactive Tutorial. – Kluwer Academic Publishers, 1999, 2000. Second Printing 2001.
8. Mao Wenbo. Modern Cryptography. Theory and Practice. - Prentice Hall PTR, Upper Saddle River, New Jersey, 2004.
9. Schneier B. Applied Cryptography: protocols, algorithms and source code in C. John Wiley & Sons, New York, 1996.

Відеозаписи лекцій викладено на Youtube-каналі кафедри ММЗІ та доступні за такими посиланнями: https://www.youtube.com/playlist?list=PLhCN8H4P5Lvg6lBl5aY8GUSpMb8IHN0i-

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
	Тема 1.1. Основні поняття криптології. Класичні схеми шифрування
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 шифра 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, грати Кардано, магічні квадрати. Класифікафікація класичних шифрів.
	Тема 1.2. Теорія Шеннона
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 Керкгоффса. Ієрархія типів атак на криптосистему за рівнем доступної криптоаналітику 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. Цілком таємна криптосистема. Необхідні і достатні умови цілковита таємності. Межа Шеннона. Цілковита таємність шифру Вернама.
9	Ненадійність ключа і відкритого тексту. Теореми про ентропією 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

	Тема 2.1. Булеві функції та їх криптографічні властивості
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.
	Тема 3.1. Системи потокового шифрування
13	Потокові шифри: визначення, загальна модель. Типи генераторів гами. Внесення нелінійності у схеми на основі регістрів зсуву із лінійним зворотним зв'язком.
14	Типи атак на потокові шифри. Кореляційна атака на схему нелінійної комбінації (на прикладі генератору Джиффі). Сучасні потокові шифри
	Тема 3.2. Системи блокового шифрування
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 «Кузнєчік»: 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'ютерний практикум

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 Джиффі.

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.

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.

Календарний рубіжний контроль

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Календарний контроль базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

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 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.

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 (РСО)

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	2	1	≥ 3	6
3.	Модульна контрольна робота	30	1	1	32
4.	Розрахункова робота	10	1	1	10
5.	Комп'ютерні практикуми	3	1	4	12
6.	Іспит	40	1	1	40
	Усього				100

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестра. 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.

Семестрова атестація (іспит) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску є:

- семестровий рейтинг ≥ 25;
- виконання та складання усіх комп'ютерних практикумів;
- виконання та захист розрахункової роботи.

Рейтингова оцінка складається з результатів роботи в семестрі та результатів усного іспиту. Іспит включає в себе практичну частину та теоретичну частину. Під час іспиту забороняється використання будь-яких додаткових довідкових матеріалів.

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

Перескладання дисципліни проходить у такій само формі, як і іспит. На перескладанні результати основого 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 спеціалізованій атестаційній комісії. Формат повторного перескладання визначається комісією.

Студенти, які протягом семестру одержали менше 10 балів, не здали без поважних причин колоквіум та/або не захистили без поважних причин домашню контрольну роботу, не допускаються до складання семестрової атестації та рекомендуються кафедрі на відрахування.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
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):
Склали: професор кафедри ММЗІ, д.ф.-м.н. Савчук Михайло Миколайович;
доцент кафедри ММЗІ, к.т.н. Яковлєв Сергій Володимирович
Ухвалено кафедрою математичних методів захисту інформації (протокол №6 від 19.06.2024 р.).
Затверджено Методичною комісією НН ФТІ (протокол № 6 від 27.06.2024 року)