



Теоретико-числові алгоритми в криптології (ПО 19)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>11 Математика і 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>4 кредити, 120 годин Лекційних занять: 36 год Практичних занять (КП): 18 год Лабораторні роботи: 18 год Самостійна робота студентів: 48 год</i>
Семестровий контроль/ контрольні заходи	<i>Залік, РР, МКР</i>
Розклад занять	<i>http://rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лекції: асистент Ядуча Дарія Вікторівна (yadukhadv-ipt@lll.kpi.ua) Практичні: асистент Ядуча Дарія Вікторівна (yadukhadv-ipt@lll.kpi.ua) Лабораторні: асистент Якимчук Олексій Петрович (yakymchukop-ipt@lll.kpi.ua)</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

У дисципліні «Теоретико-числові алгоритми в криптології» вивчається низка методів, алгоритмів і понять, що лежать в основі роботи та аналізу як симетричних, так і асиметричних криптосистем.

Кредитний модуль знайомить студентів з алгоритмами факторизації цілих чисел; алгоритмами знаходження дискретних логарифмів; алгоритмами на решітках та деякими іншими алгоритмами, що використовуються при реалізації та аналізі криптографічних систем. При цьому робиться наголос на особливостях обчислювальної реалізації зазначених методів та алгоритмів.

Метою вивчення дисципліни є надання майбутнім фахівцям знань у галузі найуживаніших у криптології теоретико-числових, алгебраїчних та обчислювальних методів і алгоритмів, а також практичних навичок їх реалізації та застосування.

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

- **знання:**

- алгоритмів факторизації цілих чисел;
- алгоритмів знаходження дискретних логарифмів;
- основних понять та термінів для роботи з цілочисельними решітками у криптології;
- алгоритмів на решітках.

- **уміння:**

- реалізовувати алгоритми факторизації цілих чисел;
- реалізовувати алгоритми знаходження дискретних логарифмів;
- застосовувати алгоритми на решітках для криптоаналізу.

- **досвід:**

- застосування алгоритмів факторизації цілих чисел та алгоритмів знаходження дискретних логарифмів у криптоаналізі;
- комп'ютерної реалізації деяких алгоритмів факторизації цілих чисел та знаходження дискретних логарифмів.

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

- **Загальні компетентності:**

- ЗК 01 – Здатність учитися і оволодівати сучасними знаннями;
- ЗК 02 – Здатність застосовувати знання у практичних ситуаціях;
- ЗК 03 – Здатність генерувати нові ідеї (креативність);
- ЗК 05 – Здатність проведення досліджень на відповідному рівні;
- ЗК 07 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- ЗК 08 – Знання та розуміння предметної області та розуміння професійної діяльності;
- ЗК 10 – Навички у використанні інформаційних і комунікаційних технологій.

- **Фахові компетентності:**

- ФК 01 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем;
- ФК 02 – Здатність виконувати завдання, сформульовані у математичній формі;
- ФК 03 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень;
- ФК 06 – Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків;
- ФК 07 – Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення;
- ФК 09 – 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 18 – Навички розв’язування специфічних математичних та комп’ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем.

● **Програмні результати навчання:**

- ПРН 01 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці;
- ПРН 02 – Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами;
- ПРН 03 – Формалізувати задачі, сформульовані мовою певної предметної галузі, формувати їх математичну постановку та обирати раціональний метод вирішення, розв’язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів;
- ПРН 05 – Уміти розробляти та використовувати на практиці алгоритми, пов’язані з апроксимацією функціональних залежностей, чисельним диференціюванням та інтегруванням, розв’язанням систем алгебраїчних, диференціальних та інтегральних рівнянь, розв’язанням крайових задач, пошуком оптимальних рішень;
- ПРН 07 – Вміти проводити практичні дослідження та знаходити розв’язок некоректних задач;
- ПРН 09 – Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв’язання практичних 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 19 – Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми;
- ПРН 21 – Вміти формулювати та розв’язувати алгебраїчні та комбінаторні задачі, будувати та реалізовувати комбінаторні алгоритми та алгоритми прикладної алгебри, аналізувати теоретичну та практичну складність таких алгоритмів.

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

Кредитний модуль «Теоретико-числові алгоритми в криптографії» забезпечується такими курсами:

- ЗО 12.1 «Дискретна математика. Частина 1»;
- ЗО 12.2 «Дискретна математика. Частина 2»;

- ЗО 21.1 «Програмування. Частина 1»;
- ЗО 21.2 «Програмування. Частина 2»;
- ПО 1.1 «Прикладна алгебра. Частина 1»;
- ПО 1.2 «Прикладна алгебра. Частина 2»;
- ПО 3 «Спеціальні розділи обчислювальної математики».

3 Зміст навчальної дисципліни

Розділ 1. Алгоритми факторизації цілих чисел.

Розділ 2. Алгоритми розв'язання задачі дискретного логарифмування.

Розділ 3. Алгоритми на решітках.

4 Навчальні матеріали та ресурси

Базова рекомендована література

1. *Т. Кормен, Ч. Лейзерсон, Р. Рівест, К. Стайн.* Вступ до алгоритмів (переклад з англ. Introduction to algorithms). – Київ: К. І. С., 2019. – 1288 с.
2. *Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.* Інформаційна безпека. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
3. *О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс.* Прикладна криптологія: системи шифрування. – Житомир: ДУТ, 2014. – 448 с.
4. *А. В. Анісімов* Алгоритмічна теорія великих чисел. К.: Академперіодика, 2001. – 218 с.
5. *В. Задірака, О. Олексюк* Комп'ютерна арифметика багаторозрядних чисел. – Київ, 2003. – 324 с.

Допоміжна рекомендована література

1. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography, 1996. – 780 с.
2. *Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman.* An Introduction to Mathematical Cryptography, 2008. – 523 с.
3. *Razvan Barbulescu.* Algorithms for discrete logarithm in finite fields. Université de Lorraine, 2013. – 181 с.
4. *Seong Oun Hwang, Intae Kim, Wai Kong Lee* Modern. Cryptography with Proof Techniques and Implementations, 2021. – 484 с.
5. *Daniele Micciancio, Shafi Goldwasser.* Complexity of Lattice Problems a Cryptographic Perspective, 2002. – 220 с.

Навчальний контент

5 Методика опанування навчальної дисципліни (освітнього компонента)

Для проведення занять застосовується практичний метод. Для лекційних занять використовуються пояснювально-ілюстративний та частково-пошуковий або евристичний методи, коли під час лекції викладач пропонує студентам визначити спосіб або підходи до розв'язання тієї чи іншої проблеми (задачі), і внаслідок керованої викладачем дискусії знаходиться правильний розв'язок проблеми.

На практичних заняттях використовуються метод проблемного викладу та репродуктивний метод: викладач попередньо задає студентам завдання, для виконання яких вони мають розібратися в певному теоретичному матеріалі і творчо застосувати ці знання до розв'язання поставлених задач. Після обговорення і осмислення матеріалу на практичних заняттях студенти шляхом відтворення і повторення певних дій на типових прикладах закріплюють свої знання та навички.

Для проведення лабораторних робіт використовується частково-пошуковий метод навчання. При цьому викладач ставить перед студентами задачі створення комп'ютерних програм для специфічних, доволі складних алгоритмів, що вимагає від студентів пошуку (з допомогою викладача) та опанування нових для них підходів програмування.

Лекційні заняття

1. Задача факторизації та задача пошуку канонічного розкладу числа, доведення їх поліноміальної еквівалентності. Задача факторизації у криптографії. Метод Ферма.
2. Метод Полларда (ρ -метод) для факторизації. Алгоритм Діксона.
3. Наближені та ланцюгові дроби. Алгоритм Брілхарта-Моррісона.
4. Алгоритм квадратичного сита (Померанця). Модифікації алгоритмів факторизації з використанням факторних баз.
5. Алгоритм Ленстри.
6. Задача дискретного логарифмування. Алгоритм узгодження.
7. Алгоритми Полларда для дискретного логарифмування (ρ -метод та λ -метод).
8. Алгоритм Сільвера-Поліга-Гелмана.
9. Алгоритм index-calculus та його модифікації (алгоритм Коперсмита).
10. Модифікації задачі дискретного логарифмування та алгоритми їх розв'язання.
11. Решітки: основні поняття та терміни (частина 1).
12. Решітки: основні поняття та терміни (частина 2). Теореми Блікфельда, Ерміта, Мінковського.
13. Алгоритмічні задачі на решітках: задача входження, задача рівності, задача SBR, задачі SVP, CVP та їх модифікації.
14. Алгоритм Бабая. Алгоритм ортогоналізації Грама-Шмідта.
15. Алгоритм LLL.
16. Використання алгоритму LLL для розв'язання задачі SVP. Оцінки для першого послідовного мінімуму решітки з використанням LLL-редукованого базису.

17. Узагальнення та модифікації алгоритму LLL.
18. Застосування алгоритму LLL для криптоаналізу.

Практичні заняття

1. Розв'язання задач на застосування алгоритмів Ферма та Полларда.
2. Побудова ланцюгових та наближених дробів. Алгоритм Діксона та Брілхарта-Моріссона.
3. Приклади застосування алгоритмів Ленстри та квадратичного сита (Померанця) для факторизації чисел.
4. Проведення частини №1 модульної контрольної роботи.
5. Приклади застосування алгоритму узгодження та ρ -методу Полларда.
6. Розв'язання задач на застосування алгоритмів Сільвера-Поліга-Гелмана та index-calculus.
7. Проведення частини №2 модульної контрольної роботи.
8. Приклади цілочисельних решіток та застосування алгоритму ортогоналізації Грама-Шмідта.
9. Проведення частини №3 модульної контрольної роботи.

Лабораторні роботи

1. Пошук канонічного розкладу великого числа, використовуючи відомі методи факторизації.
2. Реалізація алгоритму дискретного логарифмування Сільвера-Поліга-Геллмана.
3. Реалізація та застосування алгоритму дискретного логарифмування index-calculus.

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. Перед здачею лабораторної роботи на занятті студенту необхідно самостійно або в бригаді з двох людей виконати лабораторну роботу та повторити теоретичний матеріал за темою лабораторної.

Для кращого засвоєння матеріалу потрібно виконувати домашні завдання, які можна здавати до наступного практичного заняття. Для підготовки до виконання домашніх завдань та розрахункової роботи потрібно використовувати конспект лекцій та рекомендовану літературу.

Лабораторні роботи виконуються студентом самостійно, або в бригаді з двох студентів. При виконанні лабораторної роботи не дозволяється використовувати готові реалізації та програмний код, створений іншими особами. Захист практичної частини лабораторної роботи відбувається студентом самостійно або в бригаді з двох студентів (залежно від обраного типу виконання завдання). Теоретичний захист лабораторної роботи відбувається студентом самостійно. При захисті практичної частини лабораторної роботи студенти зобов'язані продемонструвати процес та результати застосування створеної програмної реалізації, а також відповісти на питання стосовно створеного програмного коду. При теоретичному захисті лабораторної роботи студенти мають відповісти на теоретичні контрольні питання, що наведені у завданні до лабораторної.

При підготовці до складання теоретичних тестів та модульної контрольної роботи студенту необхідно повторити теоретичний та практичний матеріал за відповідною темою. При написанні роботи не дозволяється користуватись жодними допоміжними засобами, конспектом тощо. За вимогою викладача студент має пройти захист письмової частини модульної контрольної роботи. При захисті студенту потрібно описати свій спосіб виконання завдань задля обґрунтування самостійності виконання цього завдання. У випадку якщо студент не відповідає на запитання щодо своїх розв'язків, завдання не зараховується.

Розподіл годин самостійної роботи за семестр

<i>Тип роботи</i>	<i>Кількість годин самостійної роботи</i>
Підготовка до лекцій	10
Підготовка до практичних занять	6
Виконання лабораторних робіт	14
Підготовка до модульної контрольної роботи	2
Виконання індивідуального завдання (РР)	10
Підготовка до заліку	6
<i>Загальна кількість</i>	<i>48</i>

Політика та контроль

7 Політика навчальної дисципліни (освітнього компонента)

- **Відвідування занять**

Студенту рекомендується відвідувати лекції та практичні заняття. Під час дії воєнного стану матеріал лекцій та практичних занять дублюється в асинхронному режимі, щоб студенти мали можливість опрацювати матеріал самостійно, якщо не мали можливості бути присутніми на заняттях.

Система оцінювання орієнтована на виконання занять, які здатні розвинути практичні уміння та навички.

- **Пропущені контрольні заходи**

Результат частини модульної контрольної роботи для студента, який не виконав контрольний захід в зазначені терміни, є нульовим. Повторне написання частини модульної контрольної роботи не допускається.

- **Оголошення результатів контрольних заходів**

Захист виконаного домашнього завдання (за вимогою) та модульної контрольної 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 виконання домашніх, лабораторних робіт, розрахункової роботи, теоретичних тестів та модульної контрольної роботи вказуються на роботах з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Результати письмової частини заліку вказуються на бланках (завданнях, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Усна частина заліку проводиться у форматі співбесіди зі студентом. Студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач.

- **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 випадку, якщо в результаті перевірки лабораторної, розрахункової або домашньої роботи студента виявлено плагіат більше 10%, студент зобов'язаний виконати завдання повторно та не матиме можливість складати залік на основній сесії. У випадку, коли плагіат програмного коду студента становить менше 10%, студент отримує –10 балів до рейтингу.

- **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 оцінювального листа та/або зауважень.

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

№	Контрольний захід	Макс. бал	Ваговий бал	Кількість	Всього
1.	Домашні роботи	2	1	7	14
2.	Лабораторні роботи (практична частина)	8	1	3	24
3.	Лабораторні роботи (теоретичний захист)	3	1	3	9
4.	Теоретичні тести	8	1	1	8
5.	Розрахункова робота	5	1	1	5
6.	Модульна контрольна робота	40	1	1	40
<i>Загальна кількість</i>					100

Згідно з календарним планом курсу, контрольні заходи проводяться:

- задача лабораторних робіт (практичної та теоретичної частин):
 - лабораторна робота №1 – на 3-му занятті з лабораторних робіт (5-6 тиждень навчання);
 - лабораторна робота №2 – на 5-му занятті з лабораторних робіт (9-10 тиждень навчання);
 - лабораторна робота №3 – на 7-му занятті з лабораторних робіт (13-14 тиждень навчання);
- модульна контрольна робота:
 - частина №1 МКР – на 3-му практичному занятті (5-6 тиждень навчання);
 - частина №2 МКР – на 6-му практичному занятті (11-12 тиждень навчання);
 - частина №3 МКР – на 7-му практичному занятті (13-14 тиждень навчання);

У випадку, якщо лабораторні роботи здаються невчасно згідно з календарним планом, застосовується зменшення оцінки у розмірі –1 бал за кожен тиждень пропуску (–0.5 за практичну

частину лабораторної роботи та -0.5 за теоретичну частину лабораторної роботи), але не більше ніж 20% від максимальної оцінки за лабораторну роботу. Якщо студент здав вчасно лише одну з частин лабораторної (практичну або теоретичну), то зменшення оцінки буде відбуватись лише за однією частиною (тобто -0.5 за кожний тиждень пропуску).

У випадку, якщо домашні роботи здаються невчасно згідно з календарним планом, застосовується зменшення оцінки у розмірі -0.5 бала за затримку здачі до 7 днів; у випадку здачі з затримкою більше ніж 7 днів робота оцінюється в 0 балів.

У випадку, якщо розрахункова робота здається невчасно згідно з календарним планом, застосовується зменшення оцінки у розмірі -0.5 бала за затримку здачі до 7 днів; -1 бал за затримку здачі 7 – 14 днів; у випадку здачі з затримкою більше ніж 14 днів робота оцінюється в 0 балів.

Теоретичні тести проводяться на лекційних заняттях та направлені на перевірку знання та розуміння матеріалу, який було розглянуто на лекційних заняттях (попередніх або поточного).

Оцінювання виконання лабораторних робіт та розрахункової роботи відбувається за такими критеріями: знання та розуміння теорії, повнота виконання всіх завдань, правильність виконання програми та дотримання інструкцій, точність обробки даних і розрахунків, якість аналізу та висновків, оформлення звіту та програмних файлів.

Оцінювання виконання домашніх робіт та модульної контрольної роботи відбувається за такими критеріями: повнота виконання всіх завдань, правильність обчислень, логіка та обґрунтування рішень, глибина аналізу та висновки.

Заохочувальні бали (до 10 балів за семестр) можуть бути отримані студентом за виконання додаткових завдань (у лабораторних, домашніх чи розрахункових роботах) та за активність на лекційних та практичних заняттях.

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях кожного семестру. Для отримання атестації поточний рейтинг студента повинен бути щонайменше 50% від максимальної кількості балів, які студент може отримати за всі контрольні заходи, що відбулися на час атестації.

Зауважимо, що оцінювання виконаних домашніх та додаткових завдань відбувається наприкінці семестру, а, отже, на проміжну атестацію студентів впливають виключно результати всіх частин модульної контрольної роботи, теоретичних тестів та лабораторних робіт, проведених до моменту виставлення проміжної атестації.

Набрані рейтингові бали студента за семестр є його фінальною оцінкою за таких умов:

1. сума рейтингових балів ≥ 60 ;
2. зараховані усі домашні роботи;
3. зарахована розрахункова робота;
4. зараховані усі лабораторні роботи;
5. перевірка програмного коду на плагіат не виявила значного рівня плагіату (більше 10 %).

У випадку, якщо студент набрав менше за 60 балів (але більше 30) протягом семестру або якщо студент хоче спробувати підвищити отриманий результат, студент складає залікову роботу. При складанні залікової роботи усі набрані за семестр бали анулюються. Кількість балів, які можна набрати за залікову роботу, дорівнює 100 балів.

Для допуску до перескладання студенту необхідно здати усі домашні та лабораторні роботи, здати розрахункову роботу та набрати більше 10 балів за семестр.

Залікова робота (перескладання) складається з трьох частин – теоретичної письмової, практичної письмової та усної. Теоретична письмова частина складається з переліку коротких питань за матеріалом лекцій, практична письмова містить розв'язання трьох обчислювальних задач, усна частина проводиться індивідуально з кожним студентом та містить 5 теоретичних питань.

У випадку, якщо студент набрав більше 10 балів за семестр, він може перенести здачу предмету (повторне складання) на наступний семестр. Зауважимо, що повторне вивчення предмету не передбачено. При повторному складанні предмету студенту необхідно відповідно до узгодженого з викладачем календарного плану виконати усі контрольні заходи.

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: асистент кафедри ММЗІ, Ядуха Дарія Вікторівна.

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

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