



# КВАНТОВІ ОБЧИСЛЕННЯ ТА КВАНТОВА КРИПТОГРАФІЯ (ПО 5)

## Робоча програма навчальної дисципліни (Силабус)

### Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</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>2 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 4 кредити ЄКТС / 120 год., з них Лекційних занять: 36 год. Практичних занять: 18 год. Самостійна робота студентів: 66 год.</i>
Семестровий контроль/ контрольні заходи	<i>екзамен, МКР, ДКР, поточний контроль</i>
Розклад занять	<i><a href="http://ipt.kpi.ua/navchalnij-protses">http://ipt.kpi.ua/navchalnij-protses</a></i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: к.ф.-м.н., Фесенко Андрій В'ячеславович (<a href="mailto:fesenko.andrii@lll.kpi.ua">fesenko.andrii@lll.kpi.ua</a>) Практичні: к.ф.-м.н., Фесенко Андрій В'ячеславович (<a href="mailto:fesenko.andrii@lll.kpi.ua">fesenko.andrii@lll.kpi.ua</a>)</i>
Розміщення курсу	<i>Google Classroom</i>

## Програма навчальної дисципліни

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

Навчальна дисципліна «Квантові обчислення та квантова криптографія» присвячена новітньому напрямку досліджень, який є важливим для студентів за спеціальністю 113 Прикладна математика, і охоплює сучасні результати, отримані в квантовій моделі обчислень, та їхній вплив на криптографічні механізми захисту інформації.

**Метою навчальної дисципліни** «Квантові обчислення та квантова криптографія» є ознайомлення студентів з основними поняттями, методами та результатами квантової моделі обчислень, побудовою формальної моделі квантових обчислень, наявних квантових алгоритмів та протоколів; формування у студентів навичок використання методів квантових обчислень, зокрема, при дослідженні криптографічних примітивів, тобто, ефективно застосовувати теоретичний математичний апарат для розв'язання практичних задач.

**Предметом навчальної дисципліни** є квантова модель обчислень та наявні квантові алгоритми і протоколи.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

1) *Знання:*

- основ квантової моделі обчислень;
- основних квантових алгоритмів;

- квантових протоколів та кодів корекції помилок;
- методів квантового криптоаналізу;
- особливостей реалізації квантових обчислювальних пристроїв.

*2) Уміння:*

- виконувати обчислення в квантовій моделі обчислень;
- застосовувати квантові алгоритми;
- використовувати методи квантового криптоаналізу;
- реалізовувати криптографічні шифри у квантовій моделі обчислень.

*3) Досвід:* вільно використовувати апарат теорії квантових обчислень, зокрема, для дослідження стійкості криптографічних примітивів.

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

**Загальні компетентності**

ЗК 1 – Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.

**Фахові компетентності**

ФК 1 – Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог.

ФК 5 – Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем.

ФК 6 – Здатність розроблювати новітні механізми криптографічного захисту.

**Програмні результати навчання**

РН 1 – Використовувати та адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач.

РН 2 – Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру.

РН 11 – Провадити аналіз криптографічних алгоритмів, протоколів та систем.

РН 12 – Орієнтуватись у останніх досягненнях криптології.

РН 15 – Розроблювати та аналізувати алгоритми у класичній та квантовій моделях обчислень.

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

Для засвоєння матеріалу курсу “Теорія складності” студент повинен успішно та вчасно опанувати курс “Сучасні алгебраїчні криптосистеми”.

Отримані практичні навички та засвоєні знання будуть корисними для проходження науково-дослідної практики.

### 3. Зміст навчальної дисципліни

#### Розділ 1. Квантові алгоритми.

Тема 1.1. Квантова модель обчислень.

Тема 1.2. Ефективні квантові алгоритми.

Тема 1.3. Конструктивні функції.

#### Розділ 2. Квантова криптографія.

Тема 2.1. Квантові протоколи.

Тема 2.2. Квантовий криптоаналіз.

Тема 2.3. Особливості квантової моделі обчислень.

### 4. Навчальні матеріали та ресурси

#### Базова рекомендована література

1. *Вакарчук І.О.* Квантова механіка. (4-е видання, доповнене). — Л.: ЛНУ ім. Івана Франка, 2012. — 872 с.
2. *Michael A. Nielsen, Isaac L. Chuang* Quantum Computation and Quantum Information (2 ed.). — Cambridge: Cambridge University Press, 2010. — pp. 702. — ISBN-13 978-1-107-00217-3. Режим доступу: <http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf>
3. *Colin P. Williams* Explorations in Quantum Computing (2 ed.). — Springer, London, 2011. — pp. 717. — ISBN-13 978-1-84628-886-9. — doi: 10.1007/978-1-84628-887-6.
4. *M. Nakahara, T. Ohmi* Quantum Computing: From Linear Algebra to Physical Realizations. — CRC Press, 2008. — pp. 438.

#### Допоміжна рекомендована література

1. *F. Wojcieszyn* Introduction to Quantum Computing with Q# and QDK. — Springer, 2022. — 296 pp.

# Навчальний контент

## 5. Методика опанування навчальної дисципліни (освітнього компонента)

Для проведення занять застосовується практичний метод. Для лекційних та практичних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання, для індивідуальних занять використовується частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами проблему, і ті вирішують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, підбираючи для цього необхідні джерела інформації, методи, підходи тощо. Для виконання розрахунково-графічної роботи застосовується метод проблемного виконання.

### Лекційні заняття

Перелік лекційних занять наводиться у послідовності їхнього викладання та опанування. Кожне заняття займає дві академічні години аудиторного часу та вимагає в середньому дві години самостійної роботи.

№ з/п	Назва теми лекції та перелік основних питань
	<b>Розділ 1. Квантові алгоритми.</b>
1	<i>Квантова модель обчислень.</i> Обчислюваність та теза Черча-Тюрінга-Дойча. Бра-кет нотація Дірака. Основні постулати квантової моделі обчислень. Кубіт та багатокубітні системи. Принцип квантової суперпозиції та оператори проектування.
2	Клонування станів. Розрізнення станів та переплутані стани. Квантовий паралелізм та модель стандартного оракула. Однокубітні та багатокубітні квантові вентиля.
3	<i>Ефективні квантові алгоритми.</i> Алгоритми Дойча, Дойча-Йожи, Саймона та порівняння їх ефективності в класичній та квантовій моделі обчислень.
4	Властивості та ефективна реалізація квантового перетворення Фур'є.
5	Зведення задачі факторизації цілих чисел до пошуку періоду функції. Ефективний в квантовій моделі обчислення алгоритм Шора для факторизації цілих чисел та задачі дискретного логарифмування.
6	Задача про приховану підгрупу та наявні результати її ефективного розв'язку в квантовій моделі обчислень. Зведення задач Дойча, Дойча-Йожи, Саймона, факторизації цілих чисел та задачі дискретного логарифмування до задач про приховану підгрупу.
7	Задача про прихований зсув. Алгоритм Куперберга. Ефективний розв'язок -узагальненої задачі про прихований зсув. Узагальнення задач про приховану підгрупу та прихований зсув, їхній взаємозв'язок та властивості.
8	Алгоритм Гровера, його оцінки складності та узагальнення.
	<b>Розділ 2. Квантова криптографія.</b>
9	<i>Квантові протоколи.</i> Квантова телепортація та протокол надщільного кодування.
10	Квантові протоколи узгодження ключів.
11	Квантові коди виправлення помилок.
12	<i>Квантовий криптоаналіз.</i> Вентилі групи Кліффорда та квантова реалізація шифрів.
13	Узагальнений алгоритм Саймона.
14	Квантовий аналіз криптопримітивів.
15	Використання алгебраїчних задач для криптоаналізу симетричних шифрів.
16	<i>Особливості квантової моделі обчислень.</i> Особливості фізичної реалізації квантових обчислювальних пристроїв.
17	Квантова машина Тюрінга та відповідні класи складності.
18	Огляд сучасних результатів квантової моделі обчислень.

## Практичні заняття

---

№ з/п Назва теми заняття та перелік основних питань

---

- 1 Квантова модель обчислень.
  - 2 Алгоритми Дойча, Дойча-Йожи та Саймона.
  - 3 Квантове перетворення Фур'є та алгоритм Шора.
  - 4 МКР частина №1. Задачі про приховану підгрупу та прихований зсув.
  - 5 Алгоритм Гровера. Квантова телепортація та протокол надщільного кодування.
  - 6 Квантові протоколи узгодження ключів. Квантові коди виправлення помилок.
  - 7 Узагальнений алгоритм Саймона.
  - 8 МКР частина №2. Квантовий аналіз криптопримітивів.
  - 9 Квантова машина Тюрінга. Теор. тест. МКР частина №3.
- 

## 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 вказаного терміну. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до модульної контрольної роботи.

З метою кращого засвоєння матеріалу дисципліни, а також формування навичок самостійної роботи студентам пропонується виконати домашню контрольну роботу за індивідуально обраними темами, погодженими з викладачем. Для підготовки до виконання домашньої контрольної роботи слід скористатися рекомендованою літературою та записами лекцій. Кінцевий термін виконання домашньої контрольної роботи оголошується викладачем.

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

Форми організації освітнього процесу, види навчальних занять і оцінювання результатів навчання регламентуються *Положенням про організацію освітнього процесу в Національному технічному університеті України "Київському політехнічному інституті імені Ігоря Сікорського"*.

#### Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань та модульної контрольної роботи. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички.

Матеріал занять, які були з тих чи інших причин пропущені, необхідно опанувати самостійно.

#### Пропущені контрольні заходи

Результат модульної контрольної роботи або теоретичного тесту для студента, який не з'явився на контрольний захід, є нульовим. У такому разі, студент має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання будь-якої частини модульної контрольної роботи або теоретичного тесту не допускається.

Результат невчасно виконаної домашньої контрольної роботи є нульовим. Повторне виконання домашньої контрольної роботи не допускається.

Невчасно виконана домашня робота оцінюється згідно з політикою кінцевого термінів виконання та політикою виконання домашніх завдань.

Пропущений екзамен не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості "не з'явився" та повинен скласти екзамен вже 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.

Результати теоретичного тесту вказуються на бланках для теоретичних тестів (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

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

Результати письмової частини екзамену 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 екзамену оголошуються наприкінці її проходження.

## Політика академічної поведінки та доброчесності

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>.

Конфліктні ситуації мають відкрито обговорюватись в академічних групах з викладачем, необхідно бути взаємно толерантним, поважати думку іншого. Плагіат та інші форми нечесної роботи є неприпустимими.

Всі індивідуальні завдання студент має виконати самостійно із використанням рекомендованої літератури й отриманих знань та навичок. Цитування в письмових роботах допускається тільки із відповідним посиланням на авторський текст. Недопустимими є підказки і списування у ході теоретичних опитувань, на контрольних роботах і тестах, та на екзамені.

У разі порушення принципів академічної доброчесності студентом він може бути не допущеним до основного складання екзамену. Бали семестрового рейтингу, набрані з порушенням принципів академічної доброчесності, будуть анульовані.

## 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>.

Зокрема, необхідно дотримуватися моральних норм, правил етичної поведінки, принципів та правил академічної доброчесності. Повага один до одного дає можливість ефективніше досягати поставлених командних результатів. Тому необхідно дотримуватись таких норм академічної етики як дисциплінованість, дотримання субординації, чесність, відповідальність, робота в аудиторії з вимкненими мобільними телефонами. При використанні свого ноутбука або телефону (чи інших пристроїв) для аудіо- чи відеозапису під час лекційних або практичних занять, необхідно заздалегідь отримати дозвіл викладача.

## 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 наведених зауважень.

## Правила призначення заохочувальних та штрафних балів

Передбачено заохочувальні бали за

- вчасне розв'язання додаткових задач домашніх робіт (до 5 заохочувальних балів);
- активність на практичних заняттях та інших видах спілкування при вивченні курсу (до 5 заохочувальних балів).

Загальна кількість зароблених заохочувальних балів для одного студента за семестр не може перевищувати 6 балів. Заохочувальні бали виставляються виключно наприкінці курсу і не впливають на проміжні атестації.

## Політика виконання домашніх завдань

Виконані завдання домашніх робіт надсилаються студентами через сервіс Google Classroom (відповідне посилання надається викладачем на першому занятті) у форматах .png, .jpg, .pdf (інші формати необхідно завчасно узгодити з викладачем). Орієнтація всіх сторінок має бути такою, що дозволяє читати текст без додаткових поворотів. Заборонено надсилати домашні роботи у вигляді архівів та посилань на зовнішні ресурси.

При порушеннях оформлення виконана домашня робота може бути повернена на доопрацювання без збереження дати початкового надсилання.

Виконана домашня робота вважається зарахованою, якщо:

- правильно виконано більше 30% обов'язкових задач;
- не виявлено плагіату у роботі;
- отримано відповідне підтвердження від викладача через сервіс Google Classroom.

Роботи, які надіслані пізніше ніж за добу до дня екзамену/перескладання, не будуть враховані на цьому контрольному заході.

## Політика кінцевих термінів виконання

За порушення кінцевого терміну виконання кожної домашньої роботи (який вказано у кожній домашній роботі) максимальний бал за цю домашню роботу стає меншим на 0.5 бали за кожен тиждень пропуску, причому:

- одним тижнем пропуску вважається затримка надсилання виконаної домашньої роботи на 1-6 днів від вказаного кінцевого терміну;
- двома тижнями пропуску вважається затримка надсилання виконаної домашньої роботи на більше ніж на 7 днів.

При порушенні вказаного кінцевого терміну домашньої контрольної роботи така робота зараховуватись не буде.

При порушенні кінцевого терміну написання частин модульної контрольної роботи, письмової частини екзамену, першого та другого перескладання такі роботи зараховуватись не будуть.

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

№ з/п	Контрольний захід	Макс. бал	Ваговий бал	Кіл-ть	Усього
1.	Модульна контрольна робота	26	1	1	26
2.	Виконання домашніх завдань	1	1	9	9
3.	Теоретичний тест	10	1	1	10
4.	Домашня контрольна робота	15	1	1	15
5.	Екзамен	40	1	1	40
	Усього				100

### Поточний контроль

Поточний контроль здійснюється шляхом перевірки домашніх робіт. За активну роботу на практичних заняттях передбачені заохочувальні бали.

### Календарний контроль

Проміжна атестація студентів (далі — атестація) є календарним рубіжним контролем поточного стану виконання вимог силабусу та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестру. Для одержання першої атестації (на 8-му навчальному тижні) та другої атестації (на 14-му навчальному тижні) поточний рейтинг студента повинен бути щонайменше 60% від максимуму балів, які студент може отримати за всі контрольні заходи, що відбулися на час атестації.

Зауважимо, що оцінювання виконання домашніх завдань та домашньої контрольної роботи відбувається наприкінці семестру, як і виставлення загальної кількості заохочувальних балів, а, отже, на проміжну атестацію студентів впливають виключно результати всіх частин модульної контрольної роботи, оцінених до моменту виставлення проміжної атестації.

Таким чином на результат першої атестації впливають тільки оцінки за першу частину модульної контрольної роботи (максимальна кількість балів за яку дорівнює 12). На результат другої атестації впливають додатково оцінки за другу частину модульної контрольної роботи (максимальна кількість балів за яку дорівнює 10).

## Таблиця необхідної кількості балів для отримання проміжних атестацій

<i>Проміжна атестація</i>	<i>Максимально можлива кількість балів</i>	<i>Необхідна кількість балів</i>
перша атестація	12	7
друга атестація	22	13

### Семестровий контроль

Оцінка результатів роботи студента в семестрі є сумою всіх балів, які він отримує:

- за виконання модульної контрольної роботи;
- за виконання домашніх робіт;
- за написання теоретичного тесту;
- за домашню контрольну роботу;
- як заохочувальні бали.

Семестрова атестація (екзамен) проводиться зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску до складання екзамену на основній сесії є:

- семестровий рейтинг є не меншим ніж 25 балів;
- зараховані всі домашні роботи;

Рейтингова оцінка складається з результатів роботи в семестрі та результатів екзамену. Екзамен включає в себе практичну частину (3 задачі, 24 бали) та теоретичну частину (2 питання з різних змістовних частин дисципліни, 16 балів). Під час екзамену забороняється використання будь-яких додаткових довідкових матеріалів.

Рейтингова оцінка з урахуванням заохочувальних балів не може перевищувати 100 балів.

Студенти, які не одержали позитивної оцінки за результатами екзамену на основній сесії, йдуть на складання екзамену на додатковій сесії.

Студенти, які протягом семестру отримали від 10 до 24 балів включно, не допускаються до складання екзамену на основній сесії. Замість екзамену такі студенти виконують додаткову письмову роботу (5 задач, 20 балів), результати якої додають до семестрового рейтингу; якщо після виконання додаткової роботи семестровий рейтинг стає більшим за 25 балів, студент допускається до семестрової атестації на перескладанні; в іншому випадку результати додаткової роботи анулюються, а на перескладанні студент повторно виконує додаткову письмову роботу.

Необхідні умови допуску до складання екзамену на додатковій сесії є такими ж як і на основній сесії. Робота при складанні екзамену на додатковій сесії має той самий вигляд, як і на основній сесії. На перескладанні результати основного екзамену анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів складання екзамену на додатковій сесії.

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

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

### 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:** ст. викладач кафедри ММЗІ, к.ф.-м.н. Фесенко Андрій В'ячеславович.

**Ухвалено** кафедрою математичних методів захисту інформації (протокол №6 від 22.06.2022).

**Погоджено** Методичною комісією НН ФТІ (протокол №6 від 30.06.2022).