Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий
фізико-технічний інститут
Кафедра математичних методів
захисту інформації

СПЕЦІАЛЬНІ РОЗДІЛИ ТЕОРІЇ СКЛАДНОСТІ

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	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*Загальна кількість: 4 кредити ЄКТС / 120 год., з них* *Лекційних занять: 36 год.* *Практичних занять: 18 год.* *Самостійна робота студентів: 66 год.*
Семестровий контроль/ контрольні заходи	*залік, МКР, поточний контроль*
Розклад занять	*http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: к.ф.-м.н., Фесенко Андрій В'ячеславович (fesenko.andrii@lll.kpi.ua)* *Практичні: к.ф.-м.н., Фесенко Андрій В'ячеславович (fesenko.andrii@lll.kpi.ua)*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

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

Навчальна дисципліна "Спеціальні розділи теорії складності" присвячена дослідженню спеціальних класів складності та застосуванню методів теорії складності в криптографії.

Метою навчальної дисципліни "Спеціальні розділи теорії складності" є ознайомлення студентів з формалізацією різних ресурсів обчислень, сучасними методами та результатами теорії складності обчислень, та їхнім використанням у криптографії; формування у студентів навичок використання зведень задач та використання наявної класифікації складності задач, тобто, ефективно застосовувати теоретичний математичний апарат для розв'язання практичних задач.

Предметом навчальної дисципліни є формальні моделі обчислень, методи визначення кількості необхідних ресурсів для обчислень, побудова класифікації обчислювальних задач у відповідності до кількості використовуваних ресурсів, створення методів класифікації задач та використання методів теорії складності у криптографії.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання: *1) Знання:*

- формальних моделей обчислень та їхніх властивостей;
- методів визначення кількості необхідних ресурсів для обчислень;
- сучасних методів та результатів теорії складності обчислень;

– формалізації криптографічних вимог в термінах складності задач.

2) Уміння:

– оцінювати кількість необхідних ресурсів для обчислень;
– аналізувати складність задач;
– використовувати сучасні методи теорії складності.

3) Досвід: вільно використовувати апарат теорії алгоритмів та теорії складності для дослідження складності задач довільної предметної області, зокрема криптографії.

Одержані знання та уміння посилюють компетентності, які надаються такими дисциплінами, як "Теорія складності" та "Математична логіка та теорія алгоритмів".

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

Для засвоєння матеріалу дисципліни "Спеціальні розділи теорії складності" студент повинен успішно та вчасно опановувати дисципліну "Теорія складності", засвоїти термінологію та поняття з дисциплін "Дискретна математика", "Математична логіка та теорія алгоритмів" та "Теорія імовірностей". Дисципліна "Спеціальні розділи теорії складності" є продовженням дисципліну "Теорія складності", однак за наявності необхідних навичок може опановуватись студентами незалежно.

Отримані практичні навички та засвоєні знання сприяють глибшому розумінню таких дисциплін як "Сучасні алгебраїчні криптосистеми" та "Квантові обчислення та квантова криптографія" тощо.

3. Зміст навчальної дисципліни

Розділ 1. Спеціальні класи складності.

Тема 1.1. Ієрархії в класах складності.
Тема 1.2. Імовірнісні класи складності.
Тема 1.3. Схемна складність.
Тема 1.4. Класи складності підрахунку.
Тема 1.5. Інтерактивні доведення.
Тема 1.6. Імовірнісно перевірні доведення.
Тема 1.7. Класи складності в середньому.

Розділ 2. Застосування методів теорії складності в криптографії.

Тема 2.1. Комунікаційна складність.
Тема 2.2. Псевдовипадковість.
Тема 2.3. Важкооборотні функції.
Тема 2.4. Перевірка лінійності.
Тема 2.5. Доведення без розголошення.
Тема 2.6. Дерандомізація.

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. *Клаковичъ Л.М., Левицька С.М., Костів О.В.* Теорія алгоритмів. Навчальний посібник. — Л.:Вид. центр ЛНУ ім. І. Франка, 2008. — 140 с.

2. *Кривий С.Л.* Дискретна математика: вибрані питання. — К.: Вид. дім "Києво-Могилянська академія", 2007. — 572 с.

Допоміжна рекомендована література

1. *S. Arora, B. Barak* Computational Complexity: A Modern Approach. [Електронний ресурс] — Cambridge University Press, 2009. — 594 pp. — ISBN13: 9780521424264. Режим доступу: http://theory.cs.princeton.edu/complexity/

2. *M. Sipser* Introduction to the Theory of Computation (3 ed.). — Cengage Learning, 2012. — 480 pp. — ISBN-13: 978-1-133-18779-0.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студентів для засвоєння студентами матеріалу та опанування практичних навичок. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного викладу, для проведення практичних занять — репродуктивний і частково-пошуковий метод, а також метод проблемного викладу. За джерелом передачі змісту для проведення лекційних занять застосовуються словесний метод, а для проведення практичних занять — практичний метод.

Дистанційна форма навчання: платформа дистанційного навчання «Сікорський» на основі системи Google Classroom та платформа для проведення онлайн-зустрічей Zoom, електронна пошта, канали Telegram.

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
	Розділ 1. Спеціальні класи складності.
1	*Ієрархії в класах складності.* Альтернаційна машина Тюрінга та її властивості.
2	Класи складності поліноміальної та булевої ієрархій.
. 3	*Імовірнісні класи складності.* Ймовірнісна машина Тюрінга та її види. Класи складності $RP/coRP$. Метод імовірнісної ампліфікації.
4	Класи складності BPP, PP, ZPP та їхні властивості.
5	*Схемна складність.* Класи складності $P/poly$, AC та NC. Теорема Карпа-Ліптона.
6	*Класи складності підрахунку.* Особливості класів складності $\#P$ та $\oplus P$. Теорема Тода.
7	*Інтерактивні доведення.* Клас складності IP. Теорема Шаміра.
8	*Імовірнісно перевірні доведення.* PCP теорема.
9	*Класи складності в середньому.* Класи складності $distP$ та $distNP$.
	Розділ 2. Застосування методів теорії складності в криптографії.
10	*Комунікаційна складність.* Теорема Н'юмана.
11	*Псевдовипадковість.* Псевдовипадкові генератори.
12	*Важкооборотні функції.*
13	*Перевірка лінійності.* Тест Блума-Лубі-Рубінфельда.
14	*Доведення без розголошення.*
15	*Дерандомізація.*
16	Генератор Нісан-Вігдерсона.
17	Обчислення нижніх оцінок.
18	Сучасні результати теорії складності та їхні застосування.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Ієрархії в класах складності.
2	Імовірнісні класи складності.
3	Імовірнісні класи складності. Схемна складність.
4	МКР частина №1. Класи складності підрахунку. Інтерактивні доведення.
5	Імовірнісно перевірні доведення. Класи складності в середньому.
6	Комунікаційна складність. Псевдовипадковість.
7	Важкооборотні функції. Перевірка лінійності.
8	МКР частина №2. Доведення без розголошення. Дерандомізація.
9	Дерандомізація. 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.

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 опановувати самостійно.

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.

Результати письмової частини заліку вказуються на бланках для письмової залікової 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.

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 заліку.

У разі порушення принципів академічної доброчесності студентом він може бути не допущеним до основного складання заліку. 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 10 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 10 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 форматі Portable Document Format (.pdf) у вигляді одного файлу, але дозволяється завантажувати додаткові розв'язки у форматі Portable Document Format (.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 у вигляді оцінки від викладача через сервіс Google Classroom.

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

№ з/п	Контрольний захід	Макс. бал	Ваговий бал	Кіл-ть	Усього
1.	Модульна контрольна робота	53	1	1	53
2.	Виконання домашніх завдань	3	1	9	27
3.	Теоретичний тест	20	1	1	20
	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 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 20). На результат другої атестації впливають додатково оцінки за другу частину модульної контрольної роботи (максимальна кількість балів за яку дорівнює 20).

Таблиця необхідної кількості балів для отримання проміжних атестацій

Проміжна атестація	*Максимально можлива кількість балів*	*Необхідна кількість балів*
перша атестація	20	12
друга атестація	40	24

Семестровий контроль

Рейтингова оцінка студента складається з результатів роботи в семестрі і є сумою всіх балів, які він отримує:

– за виконання модульної контрольної роботи;
– за виконання домашніх робіт;
– за написання теоретичного тесту;
– як заохочувальні бали.

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

Якщо семестровий рейтинг складає не менше 60 балів і зараховані всі домашні роботи, студенту виставляється відповідна оцінка, окрім випадку, коли студент не погоджується із нею.

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

Студенти, які набрали від 50 до 60 балів за семестр, і в яких є зарахованими всі домашні роботи, за бажанням замість складання заліку можуть пройти усну співбесіду із викладачем за матеріалом дисципліни. На співбесіді, ставиться до 10 теоретичних питань, кожне з яких оцінюється в 1 бал. Студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки. Якщо кількості правильних відповідей не вистачило для отримання мінімальної позитивної оцінки, то студент йде на перескладання заліку.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їхній семестровий рейтинг складає не менше 30 балів і зараховані всі домашні роботи), та студенти, які не погоджуються із такою оцінкою, на останньому практичному занятті виконують залікову роботу. При цьому їхній семестровий рейтинг анулюється, включно із заохочувальними балами, а рейтингова оцінка виставляється за результатом виконання залікової роботи. Залікова робота містить тест з теоретичного матеріалу та практичну частину. Максимальна кількість балів за залікову роботу складає 100 балів.

Студенти, які не одержали позитивної оцінки за результатами заліку, йдуть на складання заліку на додатковій сесії. До складання заліку на додатковій сесії допускаються тільки студенти, усі домашні роботи яких є зарахованими до дати складання заліку на додатковій сесії, і семестровий рейтинг був не меншим за 10 балів. Робота на перескладанні має той самий вигляд, як і залікова робота. На перескладанні семестровий рейтинг та результати виконання залікової роботи анулюються, а рейтингова оцінка виставляється за результатами виконання роботи на перескладанні. Максимальна кількість балів за залікову роботу на додатковій сесії також складає 100 балів.

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

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

Кількість балів	*Оцінка*
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 №2 від 16.02.2022).
Погоджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2022).