



СПЕЦІАЛЬНІ РОЗДІЛИ ТЕОРІЇ АЛГОРИТМІВ ТА ДИСКРЕТНИХ АВТОМАТІВ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Третій (PhD)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Прикладна математика</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна, вечірня)</i>
Рік підготовки, семестр	<i>2 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 6 кредитів ЄКТС / 180 годин Лекційних занять: 10 годин Практичних занять: 8 годин Самостійна робота здобувачів: 162 години</i>
Семестровий контроль/ контрольні заходи	<i>Іспит</i>
Розклад занять	http://rozklad.kpi.ua http://ipt.kpi.ua/navchalnij-protses
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: проф. Савчук Михайло Миколайович, д.ф.-м.н. (mikhail.savchuk@gmail.com) Практичні: доц. Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua)</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Навчальна дисципліна «Спеціальні розділи теорії алгоритмів та дискретних автоматів» присвячена дослідженню фундаментальних понять, які використовуються у криптології, але мають велике значення для різних галузей математики; зокрема, розглядаються формалізації понять важкооборотності (one-wayness), псевдовипадковості (pseudorandomness), незначущості (negligibility), переваги (advantage) тощо.

У курсі досліджуються існуючі формальні моделі для визначення наведених понять, їх можливі реалізації у математичних примітивах, проблеми практичного застосування та вплив на складність інших математичних задач. Більш детально розглядаються застосування у галузі криптології, зокрема, теоретичні моделі стійкості криптографічних систем в залежності від рівня інформації, доступної аналітику (ССА, СРА тощо).

Основною метою дисципліни є формування у здобувачів глибинного розуміння формальних дискретних та імовірнісних моделей, їх властивостей, внутрішніх зв'язків та

інтерпретацій у термінах різних наукових галузей. У результаті вивчення курсу здобувач повинен вільно володіти концепціями та підходами до визначення фундаментальних понять, які лежать в основі математичних теорій сучасних прикладних наук (складність, важкооборотність, псевдовипадковість, незначущість тощо) та вміти застосовувати їх у прикладних задачах та для формалізації власних наукових досліджень.

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

Для засвоєння матеріалу курсу необхідні базові знання з дискретної математики, математичної логіки, теорії алгоритмів, теорії імовірності, математичного моделювання, криптографії та криптоаналізу.

Отримані практичні навички та засвоєнні знання можуть використовуватись для проведення власних наукових досліджень і подальшої наукової та професійної діяльності.

3. Зміст навчальної дисципліни

- Тема 1. Аналітичні комбінаторні моделі та їх застосування
- Тема 2. Теоретико-складнісні моделі та підходи до їх побудови
- Тема 3. Важкооборотні функції та псевдовипадкові генератори
- Тема 4. Псевдовипадкові відображення
- Тема 5. Криптографічні застосування

4. Навчальні матеріали та ресурси

1. Philippe Flajolet, Robert Sedgewick. Analytic Combinatorics. – Cambridge University Press, 2009. – 829 pages. – <https://algo.inria.fr/flajolet/Publications/book.pdf>
2. S. Arora, B. Barak Computational Complexity: A Modern Approach. [Електронний ресурс] — Cambridge University Press, 2009. — 594 pp. — Режим доступу: <http://theory.cs.princeton.edu/complexity/>
3. Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography [електронний ресурс]. – 2008. – <https://cseweb.ucsd.edu/~mihir/papers/gb.pdf>
4. Oded Goldreich. Foundations of Cryptography [електронний ресурс]. – 1998-2003. – <https://www.wisdom.weizmann.ac.il/~oded/foc-drafts.html>
5. Dan Boneh, Victor Shoup A Graduate Course in Applied Cryptography [Електронний ресурс] // Режим доступу: <https://toc.cryptobook.us/book.pdf>
6. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. – Boca Raton London New York: Chapman & Hall /CRC Taylor & Francis Group, 2008. – 534 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для лекційних та практичних занять використовуються дискусійний метод, дослідницький метод та метод проблемного виконання. На лекціях здобувачі заохочуються до висловлювання власних думок та ведення дискусії із викладачем. На практичних заняттях та при виконанні аналітичного звіту здобувачі заохочуються до ініціативності, самостійності, творчого пошуку та креативності.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Аналітичні комбінаторні моделі та їх застосування. Підходи на основі генератрис, алгебр інцидентності та некомутативних алгебр
2	Теоретико-складнісні моделі та підходи до їх побудови. Моделі обчислень, протоколи доведень.
3	Поняття важкооборотної функції та важкооборотної функції із секретом. Поняття псевдовипадковості. Псевдовипадкові генератори бітів та їх зв'язок із важкооборотними функціями.
4	Псевдовипадкові відображення, псевдовипадкові перестановки: різні підходи до визначення та зв'язок між ними.
5	Криптографічні застосування: моделювання криптографічних перетворень (блокові шифри, потокові шифри, геш-функції, протоколи) за допомогою комбінаторних, імовірнісних та складнісних підходів у різних системах обмежень.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Алгебраїчні властивості важкооборотних функцій, побудова генераторів псевдовипадкових бітів на основі важкооборотних функцій.
2	Побудова псевдовипадкових відображень; моделі Лабі-Ракова, Н-коефіцієнти Патаріна.
3	Оцінки стійкості криптографічних перетворень у різних моделях. Письмове опитування.
4	Семінарське заняття

6. Самостійна робота здобувача

Здобувач 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.

Опанування дисципліни передбачає виконання аналітичного звіту та його презентація у вигляді семінарської доповіді. Здобувач самостійно обирає та узгоджує із викладачем теоретичну тему, по якій необхідно провести огляд останніх опублікованих наукових результатів, які оформлюються як звіт. Одержані результати необхідно презентувати на семінарській доповіді у форматі міні-лекції, на яку можуть запрошуватись зацікавлені бакалаври, магістри та аспіранти.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Здобувачам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх та контрольних завдань. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички.

Пропущені контрольні заходи

Здобувач, який пропустив письмове опитування, одержує за нього нуль балів без можливості перескладання. Повторне написання письмового опитування не допускається.

Дата та час семінарської доповіді узгоджується здобувачами та викладачами заздалегідь із урахуванням можливого залучення інших зацікавлених слухачів.

Оголошення результатів контрольних заходів

Результати письмового опитування вказуються на бланках із розв'язками здобувачів з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Результати виконання аналітичного звіту та його захисту у вигляді семінарської доповіді оголошуються кожному здобувачу окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких здобувачі можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження. Здобувачі заохочуються до попереднього обговорення із викладачами як звіту, так і доповіді для усунення можливих недоліків перед здачею.

Результати іспиту оголошуються наприкінці його проходження з позначенням усіх помилок, коректної або некоректної відповіді, а також з необхідними коментарями та зауваженнями.

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 здобувачів 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

Здобувачі 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.

Здобувачі мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

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

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Письмове опитування	20	1	1	20
2.	Аналітичний звіт	20	1	1	20
3.	Семінарська доповідь	20	1	1	20
4.	Іспит	40	1	1	40
	Усього				100

Рейтингова оцінка складається з результатів роботи в семестрі та результату складання іспиту.

Письмове опитування складається з декількох завдань, кожне з яких оцінюється окремо; вартість кожного завдання у балах зазначається в умові. Для одержання балів кожне завдання повинне бути розв'язане не менш ніж на 60%.

Складання аналітичного звіту з обраної теми оцінюється до 20 балів; враховується відповідність змісту звіту обраній темі, новизна та кількість опрацьованих джерел, якість оформлення тексту звіту.

Семінарська доповідь проводиться у вигляді презентаційного виступу за результатами аналітичного звіту; за неї також можна одержати до 20 балів; в оцінці враховуються презентаційні навички здобувача, якість виконаної презентації, взаємодія із слухачами.

Семестрова атестація (іспит) проводиться усно зі здобувачами, які були допущені за результатами роботи протягом семестру. Необхідною умовою допуску є семестровий рейтинг не менше 30 балів. Іспит складається з двох теоретичних питань по 20 балів кожне, на які необхідно дати розгорнуту усну відповідь.

Перескладання дисципліни проходить у такій само формі, як і іспит. На перескладанні результати основного іспиту анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів перескладання.

Здобувачі, які після першого перескладання 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:

<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):

Склали:

професор кафедри ММЗІ, д.ф.-м.н. Савчук Михайло Миколайович,

доцент кафедри ММЗІ, к.т.н. Яковлев Сергій Володимирович,

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2024 від 19.06.2024).

Погоджено Методичною комісією НН ФТІ (протокол №6/2024 від 27.06.2024)