Національний технічний університет України «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»	НН Фізико-технічний інститут Кафедра математичних методів захисту інформації

МАТЕМАТИЧНІ ОСНОВИ ТЕОРІЇ КОДІВ АВТЕНТИФІКАЦІЇ

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	*4 курс, весняний семестр*
Обсяг дисципліни	*Загальна кількість: 4 кредитів ЄКТС / 120 годин* *Лекційних занять: 18 годин* *Практичних занять: 18 годин* *Самостійна робота студентів: 84 годин*
Семестровий контроль/ контрольні заходи	*Залік/ Поточний контроль, МКР.*
Розклад занять	*http://rozklad.kpi.ua* *http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Проф. Савчук Михайло Миколайович, д.ф.-м.н.*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

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

Навчальна дисципліна «Математичні основи теорії кодів автентифікації» продовжує тематику дисципліни «Симетрична криптографія», «Асиметричні криптосистеми та протоколи 1», та фокусується на напрямку сучасних досліджень в галузі обробки, передачі, захисту інформації та криптологічних дослідженнь, які суттєво враховують алгоритмічну і математичну частину процедур підтвердження цілісності та автентичності інформації.

У курсі розглядаються загальні підходи до автентифікації повідомлень, теоретичні поняття кодів автентифікації їх властивості, алгоритми побудови стійких кодів автентифікації, можливі атаки на автентичність і способи захисту від них, а також аспекти практичного застосування цих питань до проблем побудови, застосування і оцінювання стійкості кодів автентифікації.

Основною метою дисципліни є формування у студентів глибинного розуміння сучасних проблем та напрямків в сфері захисту інформаційних технологій і криптографічного захисту інформації, зокрема, підходів щодо створення методів автентифікації інформації, яка міститься у повідомленнях, а також підходів до оцінювання ризиків безпеки. Для досягнення мети

передбачається опрацювання розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал.

У результаті вивчення курсу студент повинен:

а) знати та розуміти сучасні підходи щодо алгоритмів автентифікації інформації, методів оцінювання стійкості кодів автентифікації;

б) вміти застосовувати теорію кодів автентифікації для побудови і дослідження систем передачі та захисту інформації з гарантованим забезпеченням цілісності та автентичності;

в) вміти будувати і використовувати коди автентифікації для забезпечення надійного захисту інформаційних технологій.

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

Дана дисципліна є доповненням до дисциплін «Симетрична криптографія», «Асиметричні криптосистеми та протоколи» та поширює і поглиблює відповідні компетентності та результати навчання. Однак матеріал курсу можна вивчати і без прив'язки до зазначених дисциплін; обов'язковим для опанування є базові знання з алгебри, дискретної математики, комбінаторики, теорії ймовірностей та математичної статистики, а також розуміння основних концепцій криптології.

Головний фокус дисципліни зосереджений на автентичності інформації, її впливу на побудову інформаційних систем та на теоретичних засадах криптології як наукової галузі та їх імплементації у методах криптоаналізу. Отримані навички та засвоєнні знання можуть використовуватись для проведення наукових та прикладних досліджень при побудові і оптимізації інформаційних систем, а також для розв'язання прикладних задач у галузі безпеки інформації та криптографічного захисту інформації.

3. Зміст навчальної дисципліни

Розділ 1. Поняття автентичності повідомлення. Загальні підходи до автентифікації повідомлень.

Тема 1.1. Поняття автентичності повідомлення. Імітостійкість за Сіммонсом.

Тема 1.2. Учасники систем автентифікації. Криптографія та коди автентифікації. Приклади кодів автентифікації.

Розділ 2. Математичне визначення коду автентифікації (А-коду). Характеристики А-кодів.

Тема 2.1. Загальне визначення коду автентифікації. А-коди з секретністю і без секретності. Параметри та характеристики А-кодів. Порівняння А-кодів та криптографічних систем шифрування.

Тема 2.2. Умови на параметри А-кодів. Матриці А-коду, інцидентності, табличного задання А-коду.

Тема 2.3. Перевірка обов'язкових умов. Можливі атаки на автентичність повідомлення при порушенні окремих умов. Приклади А-кодів та можливих атак.

Розділ 3. Декартові А-коди без секретності.

Тема 3.1. Декартові А-коди без секретності та А-коди з автентифікатором. Побудова А-коду з автентифікатором за матрицею А-коду. Матриця автентифікації А-коду з автентифікатором.

Тема 3.2. Приклади побудови А-коду з автентифікатором за матрицею А-коду та атак на автентичність повідомлення. Безумовно стійкі А-коди. Методи побудови безумовно стійких А-кодів без секретності.

Тема 3.3. Алгебраїчно-ймовірнісна модель А-коду. Мета і стратегії поведінки учасників системи автентичного кодування та передачі повідомлень.

4. Навчальні матеріали та ресурси

Базова література

1. Desmedt Y. Unconditionally secure authentication schemes and practical and theoretical consequences. Crypto'85. Lecture Notes in Computer Sciense, Vol. 218 (1996), pp.42-55.
2. Simmons Gustavus J. A Survey of Information Authentication. // Proceeding of the IEEE, volume 76, Number 5, May 1988.
3. Kabatianskii G., Johansson T. Smeets B. On the cardinality of systematic A-codes via error correcting codes. // IEEE Trans. On Information Theory, Vol. IT-42, #2 (1996), pp. 566-578.
4. Stallings William. Cryptography and Network Security: Principles and Practice. Second Edition. – Prentice Hall, Upper Saddle River, New Jersey, 1999.
5. Simmons Gustavus J. A cartesian product construction for unconditionally secure authentication codes that permit arbitration.//Journal of Cryptology, Vol. 2, #2 (1990), pp. 77-104.
6. Mao Wenbo. Modern Cryptography. Theory and Practice. - Prentice Hall PTR, Upper Saddle River, New Jersey, 2004.
7. Савчук М.М., Бурлака М.К. Кодування і класифікація перестановок за спеціальним перетворенням з оцінками потужності класів // Вісник Київського національного університету імені Тараса Шевченка. Серія фізико-математичні науки, 2019, №.2. – С. 35-42.

Додаткова література

1. Грайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.
2. Stinson D.R. Cryptography: theory and practice. - CRC Press, N.Y., 1995. – 434 p.
3. Schneier B. Applied Cryptography: protocols, algorithms and source code in C. John Wiley & Sons, New York, 1996.
4. Simmons Gustavus J. Message authentication with arbitration of transmitter / receiver disputes. // Eurocrypt'87. Lecture Note in Computer Sciense,Vol.304(1988), pp.151-164.
5. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. – К., 2003. – 472 с.
6. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. – К.: 2002. – 504 с.
7. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформациию. – К.: Вища щкола, 2002. - 457 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
Розділ 1. Поняття автентичності повідомлення. Загальні підходи до автентифікації повідомлень.	
1	Поняття автентичності і цілісності повідомлення. Теорія імітостійкості за Сіммонсом.
2	Учасники систем автентифікації. Можливі атаки на цілісність і автентичність. Принципи і загальні методи автентичності.
3	Криптографія та коди автентифікації. Приклади кодів автентифікації.
Розділ 2. Математичне визначення коду автентифікації. Характеристики А-кодів.	
4	Загальне визначення коду автентифікації. А-коди з секретністю і без секретності. Параметри та характеристики А-кодів.
5	Порівняння А-кодів та криптографічних систем шифрування.
6	Умови на параметри А-кодів. Матриці А-коду, інцидентності, табличного задання А-коду.
7	Перевірка обов'язкових умов. Можливі атаки на автентичність повідомлення при порушенні окремих умов. Приклади А-кодів та можливих атак.
Розділ 3. Декартові А-коди без секретності.	
8	Декартові А-коди без секретності та А-коди з автентифікатором. Побудова А-коду з автентифікатором за матрицею А-коду. Матриця автентифікації А-коду з автентифікатором.
9	Приклади побудови А-коду з автентифікатором за матрицею А-коду та приклади атак на автентичність повідомлення.
10	Безумовно стійкі А-коди. Методи побудови безумовно стійких А-кодів без секретності.
11	Алгебраїчно-ймовірнісна модель А-коду. Мета і стратегії поведінки учасників системи автентичного кодування та передачі повідомлень.
12	Залік

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Цілісність і автентичності повідомлення. Імітостійкість за Сіммонсом. Типи атак на цілісність і автентичність.
2	Учасники систем автентифікації. Загальні методи підтвердження цілісності та автентичності. Криптографічні методи автентифікації. Імітовставка, цифровий підпис. Приклади різних кодів автентифікації.
3	Загальне визначення коду автентифікації. Параметри та характеристики А-кодів. Порівняння А-кодів та криптографічних систем шифрування.
4	Умови на параметри А-кодів. Матриці А-коду, інцидентності, табличного задання А-коду. Перевірка обов'язкових умов. Можливі атаки на автентичність повідомлення при порушенні окремих умов.
5	Експрес-опитування 1**.**
6	Представлення декартового А-коду без секретності як А-коду з автентифікатором. Побудова А-коду з автентифікатором за матрицею А-коду.
7	Побудови А-коду з автентифікатором за матрицею А-коду та атаки на автентичність

	повідомлення.
8	Методи побудови безумовно стійких А-кодів без секретності.
9	Алгебраїчно-ймовірнісна модель А-коду. Мета і стратегії поведінки учасників системи автентичного кодування та передачі повідомлень.
10	Експрес-опитування 2.
11	МКР

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.

Завданням самостійної роботи студентів є навчити студентів самостійно працювати з літературою, творчо сприймати навчальний матеріал і осмислювати його та формування навичок до щоденної роботи з метою одержання та узагальнення знань, умінь і навичок. На самостійну роботу відводяться наступні види завдань:

- обробка і осмислення інформації, отриманої безпосередньо на заняттях;
- робота з відповідними підручниками та особистим конспектом лекцій;
- самостійне розв’язання лекційних запитань;
- підготовка до модульної контрольної роботи;
- підготовка до складання семестрового контролю.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять.

Відвідування лекцій та практичних занять є рекомендованим згідно Положення про організацію освітнього процесу КПІ ім. Ігоря Сікорського. Втім, через особисті обставини студент може пропустити те чи інше заняття. У разі хвороби студент може представити довідку про термін проходження лікування з установи, де проходило лікування. У інших випадках (наприклад, через сімейні обставини) питання вирішується в індивідуальному порядку з викладачем. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

У будь-якому випадку студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для засвоєння матеріалу курсу та для виконання контрольних робіт і семестрового контролю. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути теоретичне розуміння положень курсу, практичні уміння та навички.

Пропущені контрольні заходи.

Студент, який без поважних причин пропустив модульну контрольну роботу, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), підтверджених відповідними документами, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Пропущений залік не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен складати залік на додатковій сесії.

Оголошення результатів контрольних заходів.

Результати виконання експрес-опитувань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями.

Результати модульної контрольної роботи оголошуються кожному студенту окремо у присутності або у дистанційній формі, 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 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. 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 курсу.

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 та/або зауважень.

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

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Експрес-опитування	15	1	2	30
2.	Модульна контрольна робота	70	1	1	70
	Усього				100

Поточний контроль: експрес-опитування, опитування за темою заняття, МКР.

Календарний контроль. Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться один раз за семестр, на 8-му навчальному тижні семестру. Для одержання першої атестації поточний рейтинг студента повинен бути не менше 10 балів.

Семестровий контроль. Рейтингова оцінка складається з результатів роботи в семестрі. Якщо семестровий рейтинг складає не менше 60 балів, студенту виставляється відповідна оцінка, окрім випадку, коли студент не погоджується із нею.

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням замість складання заліку можуть пройти усну співбесіду із викладачем за матеріалами курсу. На співбесіді, відповідаючи на теоретичні питання (до десяти питань), студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їх семестровий рейтинг складає не менше 10 балів), та студенти, які не погоджуються із такою оцінкою, на останньому практичному занятті виконують залікову роботу. При цьому їх семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової роботи. Залікова робота включає в себе теоретичну частину, яка складається усно, та практичну частину, яка виконується письмово.

Студенти, які не одержали позитивної оцінки за результатами заліку, йдуть на перескладання дисципліни. Перескладання проводиться у такій само формі, як і залікова робота. На перескладанні семестровий рейтинг та результати виконання залікової роботи анулюються, а рейтингова оцінка виставляється за результатами виконання роботи на перескладанні.

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 допускаються до складання семестрової атестації та рекомендуються кафедрі на відрахування або повторне проходження дисципліни. Критерії оцінювання контрольних заходів, форми проведення іспиту/заліку та інші деталі рейтингової системи наведено у Положеннях про рейтингову систему, які є додатками до даного силабусу.

Критерії оцінювання контрольних заходів, форми проведення іспиту/заліку та інші деталі рейтингової системи наведено у Положеннях про рейтингову систему, які є додатками до даного силабусу.

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

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль

1. Поняття автентичності повідомлення. Імітостійкість за Сіммонсом.
2. Учасники систем автентифікації. Криптографія та коди автентифікації. Приклади кодів автентифікації.
3. Загальне визначення коду автентифікації. Параметри та характеристики А-кодів. Порівняння А-кодів та криптографічних систем шифрування.

4. Умови на параметри А-кодів. Матриці А-коду, інцидентності, табличного задання А-коду. Перевірка обов'язкових умов.
5. Можливі атаки на автентичність повідомлення при порушенні окремих умов. Приклади А-кодів та можливих атак.
6. Декартові А-коди без секретності. А-коди з автентифікатором. Побудова А-коду з автентифікатором за матрицею А-коду. Матриця автентифікації А-коду з автентифікатором.
7. Приклади побудови А-коду з автентифікатором за матрицею А-коду та атак на автентичність повідомлення.
8. Безумовно стійкі А-коди. Методи побудови безумовно стійких А-кодів без секретності.
9. Алгебраїчно-ймовірнісна модель А-коду. Мета і стратегії поведінки учасників системи автентичного кодування та передачі повідомлень.

Робочу програму навчальної дисципліни (силабус):
Склав: професор, д. ф.-м. н. Савчук Михайло Миколайович.
Ухвалено кафедрою математичних методів захисту інформації (протокол № 6 від 22.06.2022).

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