Силабус курсу

МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – бакалавр
Рік навчання: 2
Семестр: 3,4
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП к.т.н., доцент Ігор ЯКИМЕНКО jiz@wunu.edu.ua
Контактна інформація

Опис дисципліни

Курс «Математичні основи захисту інформації» орієнтований на формування глибоких теоретичних знань та практичних навичок застосування математичного апарату для забезпечення інформаційної та кібербезпеки. Дисципліна охоплює фундаментальні розділи теорії чисел, алгебраїчних структур, теорії еліптичних кривих та методів генерації псевдовипадкових послідовностей, які є основою сучасних криптографічних систем.

Вивчення курсу передбачає опанування математичних методів, що використовуються в алгоритмах шифрування, цифрового підпису, автентифікації та інших засобах захисту інформації. Особлива увага приділяється практичному застосуванню теоретичних знань для аналізу безпеки криптографічних систем та розробки нових методів захисту інформації.

Мета курсу: розвиток математичного мислення, набуття студентами глибоких математичних знань та вмінь, необхідних для професійної діяльності у сфері кібербезпеки та захисту інформації; оволодіння навичками розв'язання задач математичного захисту інформації та аналізу загроз інформаційній безпеці.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
Семестр 3			
2/2	Множини натуральних, цілих та раціональних чисел	Володіти основними поняттями теорії чисел, вміти застосовувати метод математичної індукції	Поточне опитування
2/2	Найбільший спільний дільник. Алгоритм Евкліда	Вміти знаходити НСД та НСК, застосовувати алгоритм Евкліда	Поточне опитування
2/2	Прості й складені числа	Розуміти властивості простих чисел, вміти здійснювати факторизацію	Поточне опитування
3/3	Числові функції	Знати основні числові функції (Ойлера, Мебіуса, Кармайкла) та їх властивості	Поточне опитування
2/2	Конгруенції	Володіти поняттям конгруенції, знати основні властивості та операції	Поточне опитування
2/2	Повна та зведена система лишків	Розуміти системи лишків, вміти застосовувати теореми Ойлера і Ферма	Поточне опитування

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Лінійні конгруенції з одним невідомим	Вміти розв'язувати лінійні конгруенції різними методами	Поточне опитування
2/2	Обернений елемент за множенням	Знати китайську теорему про лишки, вміти розв'язувати системи конгруенцій	Поточне опитування
3/3	Конгруенції вищих степенів	Вміти розв'язувати конгруенції вищих степенів за різними модулями	Поточне опитування
2/2	Конгруенції другого степеня	Розуміти теорію квадратичних лишків, знати символи Лежандра і Якобі	Поточне опитування
2/2	Первісні корені	Володіти теорією порядків та первісних коренів	Поточне опитування
2/2	Дискретні логарифми (індекси)	Розуміти поняття дискретного логарифма та його застосування	Поточне опитування
2/2	Арифметичні застосування теорії конгруенцій	Вміти застосовувати теорію конгруенцій для практичних задач	Поточне опитування
Семестр 4			
2/2	Алгебри. Бінарна алгебраїчні операція	Розуміти поняття бінарної операції, напівгрупи, групи	Поточне опитування
2/2	Група. Підгрупа	Володіти теорією груп, вміти працювати з циклічними групами	Поточне опитування
2/2	Група перестановок	Знати властивості групи перестановок, вміти обчислювати порядки	Поточне опитування
2/2	Многочлени, подільність многочленів	Володіти операціями над многочленами, знати алгоритм Евкліда для многочленів	Поточне опитування
3/3	Теорема Безу та схема Горнера	Вміти застосовувати теорему Безу, знаходити корені многочленів	Поточне опитування
2/2	Кільце. Підкільце	Розуміти теорію кілець, знати типи кілець та їх властивості	Поточне опитування
2/2	Фактор-кільця та ідеали	Володіти теорією ідеалів та фактор-кілець	Поточне опитування
2/2	Теорема Ейлера, мала теорема Ферма	Вміти застосовувати фундаментальні теореми теорії чисел	Поточне опитування
2/2	Поле. Підполе	Розуміти теорію полів, знати характеристики та розширення полів	Поточне опитування
2/2	Елементарні відомості про еліптичні криві	Володіти основами теорії еліптичних кривих	Поточне опитування
3/2	Умова несингулярності еліптичної кривої	Розуміти операції на еліптичних кривих, вміти знаходити точки	Поточне опитування
2/2	Число елементів групи точок еліптичної кривої	Знати параметри еліптичних кривих для криптографічних застосувань	Поточне опитування
2/2	Псевдовипадкова послідовність	Розуміти вимоги до псевдовипадкових послідовностей	Поточне опитування
2/2	Псевдовипадкова послідовність на базі багатомодульних перетворень	Знати методи перевірки на випадковість	Поточне опитування

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Генератор псевдовипадкових чисел	Вміти реалізовувати та аналізувати різні типи генераторів	Поточне опитування

Рекомендовані джерела інформації

1. Авдєєва Т.В. Прикладна алгебра. Алгебраїчні структури. Морфізми. Основи теорії зображень груп. Навчальний посібник /Т.В. Авдєєва, В.М. Горбачук.- К.: НТУУ «КПІ», 2015. – 56 с.
2. Бобало Ю. Я. Інформаційна безпека : навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
3. Болдарєва О. М. Методичні рекомендації до самостійної роботи з дисципліни «Алгебра і теорія чисел» (курс лекцій) / О. М. Болдарєва, О. М. Яковлєва. - Одеса : ПНПУ імені К. Д. Ушинського, 2021. - 54 с. URL: http://dspace.pdpu.edu.ua/handle/123456789/11802?locale=uk
4. Гаврилків В.М. Елементи теорії груп та теорії кілець: навчальний посі бник / В.М. Гаврилків. — Івано-Франківськ: Голіней, 2018. — 148 с.
5. Головащук Н.С., Кочубінська Є.А., Овсієнко С.А.. Збірник задач з теорії кілець (базовий курс). – Навчальний посі бник для студентів механіко – математичного факультету. – К.: Видавничо–поліграфічний центр "Київський університет", 2013. – 86 с.
6. Дармосюк В. М. Алгебра та теорія чисел: конгруенції та їх застосування (завдання для самостійної роботи та методичні вказівки до їх виконання)/ В. М. Дармосюк, О. Ю. Пархоменко: посібник для самостійної та дистанційної роботи студентів. – Миколаїв: Миколаївський національний університет ім. В.О. Сухомлинського, 2021– 152 с.
7. Кулаковська І. В. Дискретна математика. Частина 1. Множини, відношення та математичні основи криптографії. Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз»: методичні вказівки / І. В. Кулаковська. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. – 100 с.
8. Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021 – 244 с.
9. Оглобліна О. І. Елементи теорії чисел: навч. посіб. / О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. – Суми: Сумський державний університет, 2015. – 186 с.
10. Стасюк М. Елементи математичних основ криптографії: навчальний посібник / Марта СТАСЮК – Львів: ЛДУ БЖД, 2021. – 216 с.
11. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем : навч. посіб. / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький: ХНУ, 2021. 174 с.
12. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 2018. – 816 p.
13. Washington L. Elliptic Curves: Number Theory and Cryptography / L. Washington. – 2nd Edition. – Chapman and Hall/CRC, 2018. – 513 p.
14. Hoffstein J. An Introduction to Mathematical Cryptography / J. Hoffstein, J. Pipher, J. Silverman. – 2nd Edition. – Springer, 2014. – 538 p.
16. Баняс Б. Методи формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем / Б. Баняс // Матеріали IX науково-технічної конференції „Інформаційні моделі, системи та технології", 08-09 грудня 2021 року. — Т. : ТНТУ, 2021. — С. 25–27.

17. Бедратюк Л.П. Дискретні струкутри. Навч.посібник для студентів вищих навч.закладів.- Хмельницький: ХНУ, 2014. – 106 с.
18. Мілінчук Ю.А. Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи забезпечення безпеки інформації» для бакалаврів напряму підготовки 12 Інформаційні технології/ Ю.А. Мілінчук, І.А. Сєчкін –Дніпро: НТУ «ДП», 2020. – 9 с.
19. Петрушак, В.С. Аналіз методів та засобів формування псевдовипадкової послідовності чисел/ В. С. Петрушак, І. В. Столярчук // Вісник Хмельницького національного університету. Технічні науки. – 2016. – №1. – С. 49-51.
20. Баришев Ю. В. Методи формування псевдовипадкових чисел для псевдонедетермінованих геш-функцій [Текст] / Ю. В.Баришев, Т. А. Кравчук // Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації», м. Вінниця, 19-21 квітня 2016 р. – Вінниця: ВНТУ, 2016. – С. 58-60.
21. Жовмір О. А. Застосування ланцюгових дробів до розв'язування діофантових рівнянь [Електронний ресурс] / О. А. Жовмір, Н. В. Сачанюк-Кавецька // Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2023)», Вінниця, 22 червня 2023 р. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2023/paper/view/17290.
22. Федоренко Н.Д. Дискретна математика: навчальний посібник у двох частинах / Н.Д. Федоренко та ін. – Ч. 1. – К.: КНУБА, 2014 – 104 с.
23. Silverman J. The Arithmetic of Elliptic Curves / J. Silverman. – 2nd Edition. – Springer, 2009. – 513 p.
24. Shoup V. A Computational Introduction to Number Theory and Algebra / V. Shoup. – 2nd Edition. – Cambridge University Press, 2009. – 580 p.
25. Ferguson N. Cryptography Engineering: Design Principles and Practical Applications / N. Ferguson, B. Schneier, T. Kohno. – Wiley, 2010. – 384 p.
26. Cryptology ePrint Archive [Електронний ресурс]. – Режим доступу: https://eprint.iacr.org/
27. NIST Post-Quantum Cryptography Standardization [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography
28. Number Theory Web [Електронний ресурс]. – Режим доступу: http://www.numbertheory.org/
29. The On-Line Encyclopedia of Integer Sequences (OEIS) [Електронний ресурс]. – Режим доступу: https://oeis.org/
30. Sage Mathematical Software System [Електронний ресурс]. – Режим доступу: https://www.sagemath.org/
OpenSSL Cryptography and SSL/TLS Toolkit [Електронний ресурс]. – Режим доступу: https://www.openssl.org/

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Семестр 3 – залік

Модуль 1		Модуль 2		Модуль 3	Модуль 4
20%	20%	20%	20%	5%	15%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за оцінювання практичних робіт №1-6.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів, за темами 1-6	Оцінка за даний модуль визначається як середнє арифметичне оцінювання практичних робіт №7-13.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів, за темами 7-13	Визначається як середнє арифметичне за виконання завдань за темами №1-2 тренінгу	Оцінка за виконаний і представлений реферат на вибрану тему.

Семестр 4 – екзамен

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінг	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за оцінювання практичних робіт №14-22.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів, за темами 14-22	Оцінка за даний модуль визначаєтьс я як середнє арифметичн е за оцінювання практичних робіт №23-28	1.Теорети чні питання: 2 питання по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів, за темами №23-28	Визначається як середнє арифметичне за виконання завдань за темами №3-4 тренінгу	Оцінка за виконаний і представле-ний реферат на вибрану тему.	1. Теорети-чні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

СЕМЕСТР 3 (ЗАЛІК)

Поточне оцінювання під час практичних робіт:

90–100 балів – у повному обсязі володіє навчальним матеріалом з математичних основ захисту інформації, вільно, самостійно та аргументовано його викладає під час відповідей на практичних заняттях, глибоко та всебічно розкриває зміст теоретичних питань з подільності цілих чисел, конгруенцій, алгебраїчних структур; демонструє розуміння криптографічних застосувань математичних методів.

75–89 балів – достатньо повно володіє навчальним матеріалом з теорії чисел та основних алгебраїчних структур, але при викладанні деяких питань з конгруенцій вищих степенів, первісних коренів або дискретних логарифмів не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки в обчисленнях.

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст з математичних методів захисту інформації, але без глибокого всебічного аналізу властивостей числових функцій, конгруенцій або групових структур, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки в застосуванні алгоритму Евкліда, розв'язуванні конгруенцій.

60–64 бали – не в повному обсязі володіє навчальним матеріалом з основних розділів курсу, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст

теоретичних питань з подільності чисел, числових функцій, основ теорії груп та кілець, допускаючи при цьому суттєві неточності.
1–59 балів – не володіє навчальним матеріалом з математичних методів захисту інформації, не розкриває зміст теоретичних питань з базових розділів теорії чисел та алгебраїчних структур.

СЕМЕСТР 4 (ЕКЗАМЕН)

Поточне оцінювання

Аналогічні критерії як для семестру 3, але з фокусом на:

- Розділ 3: Теорія еліптичних кривих
- Розділ 4: Генератори псевдовипадкових чисел

Тренінг

90–100 балів – у повному обсязі володіє навчальним матеріалом з математичних методів захисту інформації, вільно самостійно та аргументовано його використовує під час розв'язування практичних криптографічних задач тренінгу; демонструє глибоке розуміння взаємозв'язку між теоретичними математичними концепціями та їх практичним застосуванням у криптографії.
75–89 балів – достатньо повно володіє навчальним матеріалом з математичних основ криптографії, але при розв'язуванні окремих задач тренінгу з реалізації криптографічних алгоритмів або аналізу їх безпеки не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки в математичних обчисленнях.
65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при розв'язування задач тренінгу з математичних методів криптографії, але без глибокого всебічного аналізу математичних властивостей алгоритмів, обґрунтування та аргументації вибору параметрів, допускаючи при цьому суттєві неточності та помилки в реалізації алгоритмів.
60–64 бали – не в повному обсязі володіє навчальним матеріалом з математичних основ захисту інформації, фрагментарно (без аргументації та обґрунтування) його використовує, частково розв'язуючи задачі тренінгу з базових криптографічних перетворень, допускаючи при цьому суттєві неточності.
1–59 балів – не володіє навчальним матеріалом з математичних методів криптографії, не розв'язує задачі тренінгу з реалізації криптографічних алгоритмів, не бере участі у колективних завданнях під час проведення тренінгу.

Самостійна робота

90–100 балів – зміст та захист реферату з математичних методів захисту інформації свідчить про високий рівень опанування навчального матеріалу, реферат містить елементи самостійного дослідження сучасних тенденцій у застосуванні математичних методів в криптографії, аналіз новітніх криптографічних алгоритмів або математичних підходів до забезпечення інформаційної безпеки, студент на високому рівні виявляє творчий підхід до аналізу математичних аспектів кібербезпеки.
75–89 балів – зміст та захист реферату загалом свідчить про належний рівень опанування навчального матеріалу з математичних основ криптографії, можуть бути несуттєві не доопрацювання в частині глибокого математичного аналізу або недостатньо повного розкриття криптографічних застосувань, студент належно виявляє творчий підхід до дослідження обраної теми.
60–74 балів – поставлені завдання з дослідження математичних аспектів захисту інформації виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими з математичної точки зору, свідчать про недостатній рівень опанування теоретичного матеріалу з теорії чисел, алгебраїчних структур або їх криптографічних застосувань; студент припускається значних помилок у викладенні математичних концепцій, в окремих моментах виявляє творчий підхід до виконання завдань.
1–59 балів – завдання з дослідження математичних методів захисту інформації практично не виконані; відсутні авторські напрацювання в галузі математичних основ криптографії; грубі помилки у викладенні базових математичних понять та їх застосування в криптографії, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до дослідження математичних проблем інформаційної безпеки.

Модульний контроль, Екзамен

(Модульний), Екзаменаційний білет складається з двох теоретичних питань, за кожне з яких можна отримати від 0 до 30 балів (максимум 60 балів), та однієї практичної задачі, за яку можна отримати від 0 до 40 балів.

Теоретичні питання (по 30 балів кожне):

15–30 балів – студент отримує цю кількість балів, якщо у повному обсязі володіє навчальним матеріалом з математичних методів захисту інформації, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання з теорії чисел, конгруенцій, алгебраїчних структур, еліптичних кривих або генераторів псевдовипадкових чисел, демонструє розуміння їх криптографічних застосувань.

1–14 балів – студент отримує цю кількість балів, якщо в цілому володіє навчальним матеріалом з основних розділів математичних методів захисту інформації, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання з базових математичних структур, допускаючи при цьому суттєві неточності в математичних викладках, відповіді на запитання щодо криптографічних застосувань нечіткі.

Практичне завдання (40 балів):

25–40 балів – студент отримує цю кількість балів, якщо у повному обсязі володіє навчальним матеріалом з математичних методів, правильно розв'язує практичну задачу з обчислення числових функцій, розв'язування конгруенцій, операцій на алгебраїчних структурах, роботи з еліптичними кривими або аналізу псевдовипадкових послідовностей і правильно інтерпретує отримані результати з точки зору їх застосування в криптографії, демонструє самостійність виконання математичних обчислень.

10–24 балів – у достатньому обсязі володіє навчальним матеріалом з основних математичних методів захисту інформації, правильно розв'язує практичну задачу, але на додаткові контрольні запитання про криптографічні застосування результатів відсутня повна відповідь, допускає несуттєві неточності в проміжних обчисленнях та фрагментарно (без повної аргументації) інтерпретує отримані результати, демонструє самостійність виконання основних етапів розв'язання.

1–9 балів – не в повному обсязі володіє матеріалом з математичних основ захисту інформації, фрагментарно розв'язує практичне завдання з елементарних розділів теорії чисел або алгебраїчних структур, допускає суттєві неточності в базових математичних обчисленнях, поверхнево його викладає, недостатньо розкриває зміст поставлених питань щодо практичного застосування математичних методів у криптографії.

Шкала оцінювання:

ECTS	Бали	Зміст
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов’язковим повторним курсом