Силабус освітнього компонента
Програма навчальної дисципліни

Математичні основи криптології

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Математичні основи криптології" є обов'язковою навчальною дисципліною. Вивчення дисципліни дає уявлення про основні математичні методи та підходи, що застосовуються для забезпечення криптографічного захисту інформації в процесі зберігання та передачі інформації, представленої в двійкових кодах. Дисципліна присвячена вивченню математичних основ криптології та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах. Дисципліна розкриває поняття шифрів, симетричної та асиметричної криптографії, електронного підпису, гешування та інші математичні об'єкти криптографії. Вивчаються відповідні криптографічні стандарти, що застосовуються сьогодні в захисті інформації в Україні та за кордоном.

Мета та цілі дисципліни

Ознайомлення з математичними основами криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Математичний аналіз, Лінійна алгебра, Теорія ймовірностей і математична статистика, Дискретна математика, Інформатика, Програмування, Правове регулювання кібербезпеки.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основні поняття теорії захисту та полів Галуа. Основні поняття. Моделі, основні показники та основні визначення секретних систем. Поля Галуа.	2
Тема 2. Математичні основи. Алгоритм Евкліда. Фунеція Ейлера. Теорема Ейлера. Теорема Ферма. Кітайська теорема про залишки. Квадратичні лишки. Тести на простоту.	2
Тема 3. Компоненти криптосистем. Примітивний елемент. Прості шифри. Історія розвитку криптографії. Перестановчі та підстановчі шифри.	2
Тема 4. Сучасні блокові шифри. Структура блокових шифрів. DES та 3DES. ГОСТ 28147-89 («Магма»). AES. «Калина-256».	2
Тема 5. Теорія чисел у криптографії. Прості числа і тести простоти. Теорема Ферма, Ейлера, китайська теорема про залишки. Квадратичні порівняння з модулем.	2

Тема 6. Асиметричні криптосистеми. RSA. Криптосистеми Рабіна та Ель-Гамаля. Ключовий обмін Діффі-Хеллмана. Системи на основі еліптичних кривих.	2
Тема 7. Криптографічні геш-функції та цифровий підпис. Геш-функції (MD, SHA, Whirlpool, «Купина»). Призначення та властивості гешування. Цифровий підпис (RSA, DSA, ЕЦП на еліптичних кривих).	2
Тема 8. Псевдовипадкові числа та криптоаналіз. Генератори псевдовипадкових чисел. Методи перевірки випадковості. Основні методи криптоаналізу: груба сила, лінійний, диференціальний аналіз.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лекцій	Кількість годин	Вагові коефіцієнти a
Тема 1. Знайомство з оболонкою виконання лабораторних робіт з криптології. Інструменти підготовки інформації. Огляд середовищ та програм для криптографічних досліджень. Встановлення та налаштування програмного забезпечення. Робота з тестовими файлами та текстами для шифрування. Правила ведення лабораторного звіту.	4	0,1
Тема 2. Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Поняття блочного шифру. Основні режими шифрування.	4	0,1
Тема 3. Шифрування та дешифрування у класичних шифрах. Шифри підстановки (Цезаря, Віженера, Полібія). Шифри перестановки (простий та подвійний). Практична реалізація методів класичного шифрування.	4	0,1
Тема 4. Дослідження сучасних симетричних та асиметричних криптосистем. Блочні симетричні шифри: DES, AES, ГОСТ 28147-89. Сильні та слабкі сторони симетричного шифрування.	4	0,1
Тема 5. Виконання криптографічних перетворювань у DES. Генерація ключів у DES. Структура алгоритму DES. Практична реалізація DES у ПЗ.	4	0,1
Тема 6. Виконання криптографічних перетворювань у AES. Генерація ключів у AES. Архітектура AES. Виконання шифрування та дешифрування. Порівняння реалізацій AES із DES.	4	0,1
Тема 7. Генерування та дослідження геш-функцій. Призначення геш-функцій у криптології. Властивості криптографічних геш-функцій.	4	0,1
Тема 8. Асиметричні криптосистеми: RSA, Рабін, Ель-Гамаль, Діффі-Хеллман. Генерація ключів у RSA. Реалізація процесів шифрування та дешифрування. Криптосистема Рабіна. Криптосистема Ель-	4	0,1

Гамаля. Алгоритм Диффі-Хеллмана.		
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Класичні методи шифрування та математичні основи криптології. Основні поняття криптології. Модульна арифметика, прості числа та їх властивості. Класичні методи шифрування: підстановка, перестановка, шифр Віженера. Принцип роботи шифрувальної машини «Енігма». Завдання: виконати приклади шифрування та дешифрування різними методами.	0,1
Тема 2. Сучасні криптографічні алгоритми та криптосистеми. Сучасні блочні шифри: DES, AES, ГОСТ 28147-89. Криптографічні геш-функції: SHA, MD5, «Купина». Основи асиметричних криптосистем: RSA, Рабін, Ель-Гамаль, Диффі-Хеллман. Цифровий підпис та його значення. Завдання: реалізувати приклади роботи алгоритмів шифрування та хешування.	0,1
Тема 3. Теорія чисел та її застосування в криптології. Основні властивості простих чисел. Теорема Евкліда та алгоритм знаходження НСД. Мала теорема Ферма та теорема Ейлера. Взаємозв'язок з криптографічними алгоритмами (RSA, Diffie–Hellman). Використання модульної арифметики у криптографії.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,3

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Історія та еволюція комп'ютерних мереж. Розвиток мереж ARPANET, Internet. Стандартизація мережевих технологій (IETF, IEEE, ISO). Перехід від IPv4 до IPv6: причини та перспективи.	8
Тема 2. Фізичні середовища передачі даних. Кабельні технології: коаксіал, «виті пари», оптоволокно. Безпровідні канали: Wi-Fi, Bluetooth, LTE/5G. Характеристики та обмеження середовищ передачі.	8
Тема 3. Топології комп'ютерних мереж. Шина, зірка, кільце, дерево, гібридна топологія. Переваги та недоліки різних топологій. Використання в локальних та глобальних мережах.	7
Тема 4. Служби Інтернету. DNS: структура, принцип роботи. DHCP: автоматичне надання IP-адрес. WWW, FTP, SMTP, POP3, IMAP – принципи роботи сервісів.	7
Тема 5. Основи маршрутизації. Таблиці маршрутизації та їх структура. Статична та динамічна маршрутизація. Приклади налаштування статичних маршрутів.	7
Тема 6. Технології комутації. Комутація каналів vs комутація пакетів. Принцип роботи комутаторів 2-го рівня (L2). VLAN та їх застосування в корпоративних мережах.	7

Тема 7. Протоколи доступу до середовища. CSMA/CD та CSMA/CA. Розподіл каналів у безпровідних мережах. Проблеми колізій та їх уникнення.	7
Тема 8. Хмарні та віртуальні технології в мережах. Хмарні сервіси (IaaS, PaaS, SaaS). Віртуалізація серверів і мереж. SDN (Software Defined Networking) та його роль у сучасних мережах.	7
Тема 9. Безпека комп'ютерних мереж. Класифікація мережевих атак. Основні засоби захисту (фаєрволи, IDS/IPS, VPN). Безпека бездротових мереж (WPA2/WPA3).	7
Тема 10. Моніторинг та адміністрування мереж. SNMP: моніторинг мережевого обладнання. NetFlow та аналіз мережевого трафіку. Інструменти Wireshark, Nmap.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Introduction to Cyber Security»
https://www.netacad.com/courses/introduction-to-cybersecurity?course=&courseLang=en-US

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Євсеєв С. П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів "Новий світ-2000", 2021. – 120 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
2. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Євсеєв С. П. Кібербезпека: сучасні технології захисту. / Євсеєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678 с.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. http://kist.ntu.edu.ua/textPhD/tzi.pdf.
5. Євсєев С. П. Кібербезпека: основи кодування та криптографії/ С. П. Євсеєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
6. Система стандартів з організації навчального процесу. ТЕКСТОВІ ДОКУМЕНТИ У СФЕРІ НАВЧАЛЬНОГО ПРОЦЕСУ. Загальні вимоги до виконання. СТЗВО-ХПІ-3.01-2025. https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2025/06/STZVO-HPI-3.01-2025-2.pdf

Додаткова література

7. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020. – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Бобало Ю. Я., Горбатий І. В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с. – ISBN 978-966-941-339-0
http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,3	0,3		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з

Шкала оцінювання

Сума	Національна оцінка	ECTS

положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

балів		
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ