СИЛАБУС ВИБІРКОВОЇ КОМПОНЕНТИ

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

Факультет	Електроніки, автоматизація і метрології
Кафедра	Фізико-математичних наук
Статус навчальної дисципліни	**Вибіркова компонента освітніх програм першого (бакалаврський) рівня вищої освіти**
Рекомендовано для спеціальностей	053 Психологія; 051 Економіка; 061 Журналістика; 073 Менеджмент; 075 Маркетинг; 121 Інженерія програмного забезпечення; 122 Комп'ютерні науки; 125 Кібербезпека та захист інформації; 171 Електроніка; 172 Електронні комунікації та радіотехніка; 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 Інформаційно-вимірювальні технології; 176 Мікро- та наносистемна техніка; 275 Транспортні технології на автомобільному транспорті; 281 Публічне управління та адміністрування
Форма навчання	Денна, заочно-дистанційна

Викладачі

Козін Олександр Борисович
alexnazaret1@gmail.com

Доцент кафедри фізико-математичних наук, кандидат фіз.-мат. наук

Загальна інформація про дисципліну

Анотація до дисципліни

Дисципліна «Математичні основи криптографії» рекомендована для здобувачів першого (бакалаврського) рівня вищої освіти за всіма спеціальностями.

Предметом вивчення дисципліни «Математичні основи криптографії» є математичні методи криптографії наука про методи захисту конфіденційності, цілісності і автентичності інформації. Даний курс знайомить студентів із

- основними фундаментальними поняттями і законами криптографічного захисту інформації для їх використання

	в сучасних комп'ютерних системах; - основним математичним апаратом криптографії; - принципами побудови криптографічних протоколів та їх використання в задачах захисту інформації та даних; - програмними засобами, які реалізують основні криптографічні протоколи; - методами та засобами криптографічного захисту даних.
Мета дисципліни	Метою викладання навчального курсу «Математичні основи криптографії» є формування у студентів умінь та компетенцій для забезпечення реалізації ефективного криптографічного захисту інформації, а також застосування відповідних алгоритмів, методів і засобів криптографічного захисту при розробці сучасних інформаційних систем.
Компетентності, формуванню яких сприяє дисципліна	- Здатність застосовувати знання в практичних ситуаціях - Знання та розуміння предметної області та розуміння професійної діяльності. - Здатність до пошуку, оброблення та аналізу інформації. - Здатність до абстрактного мислення, аналізу та синтезу. - Здатність приймати обґрунтовані рішення - Здатність використовувати комп'ютерні технології та програмне забезпечення з обробки даних для вирішення практичних задач, аналізу інформації та підготовки аналітичних звітів.
Результати навчання	- Застосовувати ґрунтовні знання основних розділів вищої математики (лінійна та векторна алгебра, диференціальне числення, інтегральне числення, функції багатьох змінних, ряди диференціальні рівняння, теорія ймовірностей та математична статистика) в обсязі необхідному для користування математичним апаратом та методами за відповідною програмою підготовки. - Застосовувати основні фундаментальні та природничі знання, знання системного аналізу та технологій моделювання при проектування та розв'язання професійних задач.
Обсяг дисципліни	Загальний обсяг дисципліни: 6 кредити ЄКТС 180 годин). Для денної форми навчання: лекції – 22 годин, практичні заняття – 22 годин, лабораторні заняття – 22 годин, самостійна робота – 114 годин
Форма підсумкового контролю	залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркових компонент освітньої програми

Програма дисципліни

Тема 1.	***Класичні техніки шифрування.*** Криптографія: етапи історичного розвитку. Наївна криптографія. Формальна криптографія. Наукова криптографія. Комп'ютерна криптографія. Класичні техніки шифрування: шифри перестановок. Шифр частоколу. Матричний шифр. Класичні техніки шифрування:

	шифри підстановок. Шифр Цезаря. Шифр пар. Квадрат Полібія. Шифр Віженера. Багатоалфавітні системи. Роторні криптографічні машини. Криптосистема Ель-Гамаля.
Тема 2.	***Математичні питання криптографії.*** Елементи теорії зв'язку в секретних системах: основні положення Клода Шеннона. Класифікація сучасних криптосистем. Вимоги до сучасних криптосистем. Комбіновані криптосистеми. Основні принципи утворення криптографічних систем. Криптосистеми з відкритим розподілом ключів. Проблеми генерування псевдовипадкових послідовностей. Генератор RSA.
Тема 3.	***Сучасні криптографічні системи.*** Блокові шифри. Загальні відомості про блокові шифри. Криптографічний стандарт DES. Особливості стандарту DES. Опис алгоритму DES. Стійкість алгоритму DES. Модифікації алгоритму DES. Криптосистема RSA. Криптостійкість RSA.

Список рекомендованих джерел

Базови

1. Фільштінський В. А., Бережний А. В. Математичні основи криптографії : конспект лекцій. Суми : Сумський державний університет, 2011. 138 с.
2. Остапов С. Е., Валь Л. О. Основи криптографії : навч. посіб. Чернівці : Книги-XXI, 2008. 188 с
3. Вербіцький О. В. Вступ до криптології. – Львів: Видавництво НТЛ., 2008. –248 с.
4. Глинчук Л.Я. Криптологія: навч.-метод. посіб. – Луцьк: Вежа-Друк, 2014. – 163 с.
5. Остапов С.Е., Валь Л.О. Основи криптографії. Навчальний посібник. – Чернівці: Книги – XXI, 2008. – 188 с.
6. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с. Технології захисту інформації : навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.
7. Жураковский Ю.П., Полторак В.П. Теорія інформації кодування: Підручник. - Київ : Вища школа, 2001. - 255 с.
8. Теорія інформації та кодування : навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Дніпродзержинськ : Національний гірничий університет, 2012. – 108 с.
9. Захист інформації в автоматизованих системах управління : навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с
10. Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с.
11. Основи криптографічного захисту інформації : підручник / авт.: Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2011. – 94 с.
12. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
13. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
14. Фаль О. М. Криптографія : основні ідеї та застосування / О. М. Фаль. – К. : ІВЦ Видавництво «Політехніка», 2003. – 28 с.

Допоміжні
1. Козіна Г. Л., Молдов'ян М. А., Неласа Г. В. Криптопротоколи: схеми цифрового підпису : навч. посіб. Запоріжжя : ЗНТУ, 2014. 170 с.
2. Michael Braun and Anton Kargl. A Note on Signature Standards, 2007. URL: http://eprint.iacr.org/2007/357.
3. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. Харків : Вид. «Форт», 2010. 608 с.
4. Горбенко І. Д., Горбенко І. Д. Прикладна криптологія. Харків : Вид. «Форт», 2012. 878 с.
5. Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л.Я. Математичні основи криптографії. Дніпропетровськ : НГУ, 2006. 391 с.
6. Русин Б. П., Варецький Я. Ю. Біометрична аутентифікація та криптографічний захист : монографія. Львів : Коло, 2007. 287 с.
7. Блінцов В. С. Захист програмних продуктів : навчальний посібник / В. С. Блінцов, С. С. Козирев. – Миколаїв : НУК, 2010. – 146 с.
8. Гулак Г. Н. Основы криптографической защиты информации / Г. Н. Гулак. – К. : Вид. ГУІКТ, 2009. – 228 с.
9. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – К. : ДМК Пресс, 2008. – 544 с.
10. Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник / Г. Ф. Конахович. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
11. Криптографія [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/Криптографія.

Інформація про консультації

Очні консультації щопонеділка у 2023-2024 н/р, з 14-15 до 15-15 год., ауд. 104/а за попередньою домовленістю.
Онлайн консультації: Telegram (+38097-59-86-586) в робочі дні з 15.00 до 19.00 за попередньою домовленістю.

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		

0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять: Здача індивідуальних домашніх завдань.

Інші умови: Навчально-методичні матеріали дисципліни розміщені за посиланням:

1. Державна служба спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua/dsszzi/control/uk/index
2. Захист інформації http://jrnl.nau.edu.ua/index.php/ZI
3. Бізнес і безпека www.bsm.com.ua
4. Офіційний веб портал парламенту Українихttp://www.rada.gov.ua