

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ



СИЛАБУС «МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Статус дисципліни	Обов'язкова
Код та назва спеціальності	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Безпека інформаційних і комунікаційних систем
Освітній ступінь	бакалавр
Обсяг дисципліни (кредитів ЄКТС)	150 год. (5 кр.)
Терміни вивчення дисципліни	2-й курс (IV семестр)
Назва кафедри, яка викладає дисципліну, аббревіатурне позначення	Електронні обчислювальні машини (ЕОМ)
Мова викладання	Українська
Лектор	Кандидат технічних наук, доцент ПАХОМОВА ВІКТОРІЯ МИКОЛАЇВНА v.m.pakhomova@ust.edu.ua https://diit.ust.edu.ua/faculty/tk/kafedra/evm/sostav/personal_page/346 https://lider.ust.edu.ua/course/view.php?id=348
	Український державний університет науки і технологій (УДУНТ), ННІ «Дніпровський інститут інфраструктури і транспорту (ДІІТ)», 49010, Україна, м. Дніпро, вул. Лазаряна, 2, ауд. 3202, +38 (056) 373-15-89
Передумови вивчення дисципліни	Дана дисципліна спирається на вивченні дисципліни «Вища математика» та дає основу для вивчення дисципліни «Прикладна криптологія»
Мета навчальної дисципліни	Вивчення математичних основ (визначення, леми, теореми, методи), що використовуються в моделях та системах інформаційної безпеки
Очікувані результати навчання	Визначення НСД та НСК за алгоритмом Евкліда, за розширеним алгоритмом Евкліда та з використанням канонічного розкладання на множники Застосування поліноміальних, експоненціальних (Мерсенна, Ферма) та прайморіальних формул Визначення відрахування за теоремами Ейлера та Ферма Розв'язання лінійного порівняння за модулем різними методами Розв'язання системи лінійних порівнянь за модулями китайською теоремою про остачі

Зміст дисципліни	Основні теми: Теорія подільності Теорія розкладності Теорія простих чисел Теорія відрахувань (лишків) Теорія алгебраїчних структур. Поля Галуа
Контрольні заходи та критерії оцінювання	КЗ1 (20 балів): виконання завдань; самотестування КЗ2 (20 балів): виконання завдань; самотестування Екзамен (60 балів): тести №1-2; практична частина
Політика викладання	Здобувач допускається до екзамену, якщо здав КЗ1 та КЗ2 Здобувачі несуть відповідальність, які під час будь-якого методу оцінювання порушують принципи академічної доброчесності (списують, обманюють, подають виконання чужого варіанту та ін.). Оскарження результатів оцінювання здійснюється при подачі заяви здобувача на ім'я декана.
Засоби навчання	Мова програмування для реалізації фундаментальних методів та тестів
Навчально-методичне забезпечення	Методичне забезпечення 1. Математичні основи інформаційної безпеки. Навчально-методичні рекомендації щодо виконання лабораторних робіт / Пахомова В. М. Дніпро: УДУНТ, 2024. – 34 с. 2. Математичні основи інформаційної безпеки. Навчально-методичні рекомендації щодо виконання курсового завдання / Пахомова В. М. Дніпро: УДУНТ, 2024. – 16 с. Основна література 3. <i>Pakhomova V.</i> Determination of network attacks using neural network technologies. Chapter 8. pp. 113-128. DOI: 10.30890/2709-2313.2021-07-08-003. Prospektive globale wissenschaftliche trends: Innovative Technik, Transport, Sicherheit. Monografische Reihe «Europäische Wissenschaft». Buch 7. Teil 8. Germany: Karlsruhe, 2021. 168 p. 4. <i>Pakhomova V.</i> Methodology for the formation of competences of first degree holders in the discipline «Mathematical foundation of information security». Modern engineering and innovative technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E». 2023. Issue 25. Part 2. pp. 29-33. DOI: 10.30890/2567-5273.2023-25-02-048. 5. <i>Pakhomova V.</i> Methods of forming competencies in applicants for the specialty «Cybersecurity» when performing a course assignment in the discipline «Mathematical foundation of information security». International scientific publication «Technique and technology of the future'2024». Germany, Karlsruhe. October 2024. pp. 41-47. DOI: 10.30890/2567-5273.2024-35-00-029. 6. <i>Pakhomova V.</i> Formation of competencies and soft skills when performing brigade discipline tasks «Mathematical foundation of information security». Modern engineering and innovative technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E». 2024. Issue 35. Part 1. pp. 66-72. DOI: 10.30890/2709-1783.2024-35-00-014 Інформаційні ресурси 7. Дистанційний курс в системі «Лідер» з дисципліни «Математичні основи інформаційної безпеки»; укладач: доц. Пахомова В.М. Сертифікат № ДК0304 від 03.07.2019. URL https://lider.ust.edu.ua/course/view.php?id=348