УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ

СИЛАБУС
«Математичні основи інформаційної безпеки»

Статус дисципліни	Обов'язкова
Код та назва спеціальності	125 «Кібербезпека»
Назва освітньої програми	Кібербезпека
Освітній ступінь	бакалавр
Обсяг дисципліни (кредитів ЄКТС)	120 год. (4 кр.)
Терміни вивчення дисципліни	2-й курс (IV семестр)
Назва кафедри, яка викладає дисципліну, абревіатурне позначення	Електронні обчислювальні машини (ЕОМ)
Мова викладання	Українська
Лектор (викладач(і))	к.т.н., доцент Пахомова Вікторія Миколаївна v.m.pakhomova@ust.edu.ua https://diit.edu.ua/faculty/tk/kafedra/evm/sostav/personal_page/346 https://lider.diit.edu.ua/course/view.php?id=348 УДУНТ, 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 та на основі канонічного розкладання на множники Застосування поліноміальних, експоненціальних (Мерсенна, Ферма) та прайморіальних формул Визначення відрахування за теоремами (Ейлера, Ферма) Розв'язання лінійного порівняння за різними методами Розв'язання системи порівнянь за китайською теоремою про остачі
Зміст дисципліни	**Основні теми:** Теорія подільності Теорія розкладності Теорія чисел Теорія відрахувань (лишків) Теорія алгебраїчних структур
Контрольні заходи та критерії оцінювання	**ПК1** (20 балів): виконання завдань; самотестування **МК1** (25 балів): тестування; практична частина **ПК2** (25 балів): виконання завдань; самотестування **МК2** (30 балів): тестування; практична частина

Політика викладання	Здобувач допускається до МК1, якщо здав ПК1. Здобувач допускається до МК2, якщо здав М1 (ПК1; МК1) та ПК2. 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. *Пахомова В. М.* Методичні вказівки до лабораторних робіт з дисципліни «Математичні методи захисту інформації». Дніпропетровськ: ДНУЗТ, 2010. – 22 с. 2. *Пахомова В. М* Методичні вказівки до виконання курсового завдання з дисципліни «Математичні методи захисту інформації». Дніпропетровськ: ДНУЗТ, 2010. – 11 с. **Основна література** 3. *Завадська Л. О.* Спеціальні розділи математики. Елементи теорії скінченних полів. Київ: Політехніка, 2006. – 54 с. 4. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посібник / *М. С. Вертузаєв, О. М. Юрченко*. Київ: Вид-во Європ. ун-ту, 2001.– 321 с. 5. Інформаційна безпека: навч. посібник / *Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник* [та ін.]. Львів : Вид-во Львівської політехніки, 2019. – 580 с. 6. *Ковальчук Л. В., Яремчук Ю. Є.* Прикладна алгебра. Основи абстрактної алгебри. Вінниця: ВНТУ, 2015. – 98 с. 7. *Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л. Я.* Математичні основи криптографії. Дніпропетровськ: НГУ, 2004. – 392 с. 8. Основи інформаційної безпеки : навч. посібник / *В. В. Дудикевич, В. О. Хорошко, Ю. Є. Яремчук*. Вінниця : ВНТУ, 2018. – 316 с. **Додаткова література** 9. Основи криптографічного захисту інформації: підручник / *Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук*. Вінниця : ВНТУ, 2011. – 199 с. 10. *Харченко Л. С., Ліпкан В. А., Логінов О. В.* Інформаційна безпека України: глосарій / заг. ред. Р.А. Калюжний. Київ: «Текст», 2004. – 134 с. 11. *Hansen F., Oleshchuk V. A.* Conformance Checking of RBAC Policy and its Implementation. The First Information Security Practice and Experience Conference, ISPEC 2005, Singapore, LNCS, Volume 3439, pp. 144-155, 2005. 12. *Pakhomova V.* 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 «Europaische Wissenschaft». Buch 7. Teil 8. Germany: Karlsruhe, 2021. 168 p. **Інформаційні ресурси** 13. 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.diit.edu.ua/course/view.php?id=348