Силабус курсу

ДОСЛІДЖЕННЯ І ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 1
Семестр: 1
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Ігор Якименко
Контактна інформація	jiz@wunu.edu.ua

Опис дисципліни

Метою курсу Мета вивчення дисципліни "Дослідження і проектування систем захисту інформації" полягає у формуванні у майбутніх фахівців умінь та навичок для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
4/-	Теоретичні засади дослідження та проєктування СЗІ. Концепції національної та інформаційної безпеки України	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/-	Структура та компоненти сучасних систем захисту інформації	Розуміти організаційні аспекти та взаємодії компонентів СЗІ Класифікувати загрози та ризики, застосовувати технічні та програмні засоби захисту інфрормації.	Поточне опитування
2/-	Міжнародні стандарти та практики у сфері інформаційної безпеки	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/-	Теоретико-числові основи криптографічних механізмів у СЗІ	Використовувати цілочисельну систему залишкових класів для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування

2/2	Симетричний метод шифрування у СЗК	Застосовувати методи метод шифрування у СЗК для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Асиметричний метод шифрування у СЗК	Використовувати асиметричний метод шифрування у СЗК для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Міжбазисні перетворення та ступінчаста СЗК	Застосовувати міжбазисні перетворення на основі розмежованої СЗК для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Методи пошуку оберненого поліному та відновлення поліномів за залишками	Використовувати метод пошуку оберненого поліному за модулем для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування, тестування
2/2	Дослідження стійкості методів шифрування та СЗІ	Оцінювати стійкість методу шифрування у поліноміальній системі залишкових класів для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Постквантові алгоритми шифрування	Розуміти принципові математичні засади постквантової криптографії, ідентифікувати та класифікувати ключові стандарти NIST FIPS для PQC	Поточне опитування
2/-	Проєктування комплексних систем захисту інформації з використанням криптографії	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/-	Аудит та оцінка ефективності СЗІ	Проводити аудит та оцінку ефективності СЗІ для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/-	Впровадження математично-криптографічних методів у практичні СЗІ	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/-	Науково-дослідна та інноваційна діяльність у сфері криптографії та СЗІ	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або	Поточне опитування

		кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	
2/-	Міждисциплінарний підхід та інтеграція сучасних технологій у проєктування СЗІ	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Kouther Fahad Alshammaria,* , Ayman Mostafaa , Shadi Nashwana Avalanche Analysis of Variant Polynomials for AES Turkish Journal of Computer and Mathematics Education Vol.12 No.14(2021), 2696- 2703
2. Tynymbayev, Sakhybay and Ibraimov, Margulan and Namazbayev, Timur and Gnatyuk, Sergiy, Development of Pipelined Polynomial Multiplier Modulo Irreducible Polynomials For Cryptosystems (February 25, 2022). Eastern-European Journal of Enterprise Technologies, 1 (4 (115)), 37–43, 2022.
3. Yakymenko I., Kasianchuk, M., Martyniuk, O., & Martyniuk, S. (2025). A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. *International Journal of Computing*, 24(1), pp. 92-101.
4. Yakymenko I., Kasianchuk M., Shylinska I. A Method for Polynomial Recovery from its Resudues Based on Addition in Z[x] Ring. *Informatics and Mathematical Methods in Simulation* Vol.14 (2024), No. 4, pp. 305-313.
5. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT., 2024, pp. 496–499.
6. Shevchuk R., Yakymenko I., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future Challenges. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT2024, 2024, pp. 552–559.
7. Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. *Journal of Applied Mathematics*., 2024, pp. 1-12.
8. Shevchuk R., Karpinski M., Kasianchuk Yakymenko I., Melnyk A., Tykhyi R. Software for Improve the Security of Kubernetes-based CI/CD Pipeline. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT2023, 2023, pp. 420–425.
9. Kasianchuk M., Yakymenko I., Yatskiv S., Gomotiuk O., Bilovus L.The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem. *CEUR Workshop Proceedings*, 2023, 3373, pp. 425–436.
10. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. *CEUR Workshop Proceedings*, 2022, 3156, pp. 365–377.
11. Nykolaychuk Ya., Yakymenko I., Vozna N., Kasianchuk M. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis*. 2022, Vol. 58, No. 4, P.611-618.
12. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. *12th International Conference on Advanced Computer Information Technologies*, ACIT 2022, 2022, pp. 345–350.
13. Yakymenko I., Kasianchuk M., Yatskiv V., Shevchuk R., Koval V., Yatskiv S. Sustainability and Time Complexity Estimation of Cryptographic Algorithms Main Operations on Elliptic Curves. *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*. Pp. 494-498.

14. Касянчук М.М., Якименко І.З., Николайчук Я.М. Симетричні криптоалгоритми у системі залишкових класів. *Cybernetics and Systems Analysis*, 2021, Vol 57, Issue 2, p.184-189.

15. Mykhailo Kasianchuk, Ihor Yakymenko, Vasyl Yatskiv, Stepan Ivasiev, Andriy Sverstiuk. Same Bit-Size Moduli Formation of Residue Number System for Application in Asymmetric Cryptography. *IntelITSIS 2021*. pp. 301-308.

16. Shevchuk R., Yakymenko I., Karpinski M., Shylinska I., Kasianchuk M. Finding the inverse of a polynomial modulo in the ring Z[x] based on the method of undetermined coefficients. *Computer Science*. vol. 25. no. 2. 2024. pp.1-14.

17. Adebayo, A., Adeniyi, A. E., Ajao, J., Isiaka, R., Gbolagade, K., & Abdulsalam, S. (2024). Development of a Multi-Level Data Encryption Standard with Residue Number System for Data Security. Conference Organising Committee, 14. https://www.researchgate.net/profile/Bolaji-Oladokun/publication/382947230_Bridging_the_Digital_Divide_Empowering_Nigerian_Universities_through_Technological_Advancements_in_Academic_Libraries/links/66b4749c8f7e1236bc43f5e7/Bridging-the-Digital-Divide-Empowering-Nigerian-Universities-through-Technological-Advancements-in-Academic-Libraries.pdf#page=20

18. Hati, I. N. K. (2023). A brief summary of the full RNS variant of some homomorphic encryptions. Journal of Modern Technology and Engineering, 8(2), 112–118

19. Krasnobayev, V., Koshman, S., & Kovalchuk, D. (2022). The concept of using the number system in the residual classes for building artificial intelligence system. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(67), 65–70

20. Mousavi, S., Rahmati, D., Gorgin, S., & Lee, J.-A. (2024). Enhancing Computational Efficiency in Intensive Domains via Redundant Residue Number Systems (arXiv:2408.05639). arXiv. https://doi.org/10.48550/arXiv.2408.05639

21. Oke, A. A., Nathaniel, B. A., Bukola, B. F., & Ayopo, O. A. (2021). Residue number system based applications: A literature review. Annals. Computer Science Series, 19(1). https://anale-informatica.tibiscus.ro/download/lucrari/Vol19/19-1-20-Babatunde.pdf

22. Bouziani, M. M., Merbah, M. M., Tiskar, M. M., ET-Tahir, M. A., & Chaouch, M. A. (2022). When can we talk about implementing an Information Security Management System, according to ISO 27001. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(2), 394-401

23. M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," Symmetry, vol. 15, no. 11, p. 1981, 2023. https://doi.org/10.3390/sym15111981.

24. R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," Comput. Secur., vol. 108, p. 102376, 2021

25. C. Ubochi, B. Olaniyi, K. Ukagwu, and S. Nnamchi, "A comparative analysis of symmetric cryptographic algorithm as a data security tool: A survey," J. Sci. Technol. Res., vol. 5, no. 3, pp. 144–168, 2023.

26. Ahmad, M., Doja, M. N., & Beg, M. M. S. (2021). Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. Journal of King Saud University-Computer and Information Sciences, 33(1), 77–85. https://www.sciencedirect.com/science/article/pii/S1319157817304202

27. Certauri.com. (2023). RSA vs ECC: A comprehensive performance analysis. https://www.certauri.com/rsa-vs-ecc-a-comprehensive-performance-analysis/

28. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications, 209. https://www.sciencedirect.com/science/article/pii/S1084804522001813

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Підсумковий бал (за 100 – бальною шкалою) з дисципліни "Дослідження і проектування систем захисту інформації" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 1-6.	Підсумкове модульне тестування за темами № 1-15.	Оцінка визначається як середнє арифметичне за виконання та презентацію одного завдання.	Оцінка визначається як середнє арифметичне за виконання та презентацію одного завдання.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2.Практичне завдання - max 40 балів.

Шкала оцінювання

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	**A** (відмінно)
85–89	добре	**B** (дуже добре)
75–84		**C** (добре)
65–74	задовільно	**D** (задовільно)
60–64		**E** (достатньо)
35–59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1–34		**F** (незадовільно з обов'язковим повторним курсом)