

	СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Захист інформації» Рівень вищої освіти: <u>Другий (магістерський)</u> Спеціальність: <u>ЕЗ Комп'ютерні науки</u> Рік навчання: <u>1-й, семестр 2-й</u> Кількість кредитів ECTS: <u>4 кредити</u> Назва кафедри: <u>Комп'ютерних наук та цифрової економіки</u> Мова викладання: <u>українська</u>
Лектор курсу	к.т.н, доцент Красиленко Володимир Григорович
Контактна інформація лектора (e-mail)	<u>krasvg@i.ua</u>

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Захист інформації» є вибірковою компонентою ОПП.

Загальний обсяг дисципліни 120 год.: лекції – 24 год.; практичні заняття – 22 год., самостійна робота – 74 год.

Формат проведення: лекції, практичні заняття, консультації.

Підсумковий контроль – залік.

Під час вивчення дисципліни можуть використовувати знання, отримані з таких дисциплін: «Дискретна математика», «Інформаційні технології», «Теорія ймовірностей та математична статистика».

Призначення навчальної дисципліни

Дисципліна «Захист інформації» спрямована надати здобувачам здатність аналізувати загрози інформаційній безпеці, застосовувати вимоги та стандарти захисту інформації, обирати криптографічні методи, організовувати керування ключами, використовувати засоби автентифікації, електронного підпису, стеганографії та оцінювати їхню надійність.

Мета вивчення навчальної дисципліни

Метою навчальної дисципліни «Захист інформації» є формування у здобувачів освіти системи теоретичних знань та практичних навичок, необхідних для забезпечення захисту інформації, а саме: ознайомлення з основними поняттями, принципами та проблемами інформаційної безпеки, вимогами до технічного захисту інформації та стандартами безпеки, методами

криптографічного захисту, електронного підпису, хешування, генерування псевдовипадкових послідовностей, узгодження й адміністрування ключів, автентифікації, авторизації, біометрії, криптоаналізу та стеганографії, а також розвиток здатності застосовувати набуті знання для розв'язання практичних завдань із захисту інформації.

Завдання вивчення дисципліни

Завданням дисципліни є ознайомлення з теоретичними засадами захисту інформації, його метою, предметом і основними поняттями; формування знань про проблеми інформаційної безпеки мереж та способи її забезпечення; вивчення вимог до технічного захисту інформації й основних стандартів інформаційної безпеки. Надати студентам теоретичні та практичні знання щодо принципів криптографічного захисту інформації, аналізу алгоритмів шифрування, електронного цифрового підпису, хешувальних функцій і генерування псевдовипадкових послідовностей. Курс охоплює вивчення протоколів узгодження ключів та їх адміністрування, технологій автентифікації й авторизації, біометричних методів і їх характеристик, а також основ криптоаналізу та стеганографії. Дисципліна спрямована на формування здатності оцінювати загрози інформаційній безпеці, обирати належні засоби захисту, аналізувати їхні властивості та обґрунтовувати рішення щодо забезпечення конфіденційності, цілісності й доступності інформації, а також на розвиток аналітичних навичок і вміння застосовувати набуті знання під час розв'язання практичних завдань у сфері захисту інформації.

ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ, ЯКИХ НАБУВАЄ ЗДОБУВАЧ ПРИ ВИВЧЕННІ ДИСЦИПЛІНИ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

У результаті вивчення навчальної дисципліни здобувач повинен сформувати такі програмні компетентності:

інтегральну компетентність (ІК):

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері комп'ютерних наук.

загальні компетентності (ЗК):

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність вчитися й оволодівати сучасними знаннями.

ЗК6. Здатність бути критичним і самокритичним.

спеціальні (фахові, предметні) компетентності (СК):

СК1. Усвідомлення теоретичних засад комп'ютерних наук.

СК3. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області.

СК5. Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

СК6. Здатність застосовувати існуючі і розробляти нові алгоритми розв'язування задач у галузі комп'ютерних наук.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

РН1. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань.

РН10. Проектувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

РН13. Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

РН18. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

Вивчення даної дисципліни формує у здобувачів освіти соціальні навички (soft skills): комунікативність (реалізується через: метод роботи в парах та групах, робота з інформаційними джерелами), робота в команді (реалізується через: метод проєктів), лідерські навички (реалізується через: робота в групах, метод проєктів, метод самопрезентації).

ПЛАН ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Назви теми	Форми організації навчання та кількість годин		Самостійна робота, кількість годин
		лекційні заняття	практичні заняття	
2-й семестр				
1	Тема 1. Загальні поняття захисту інформації, мета і предмет дисципліни	0	2	6
2	Тема 2. Проблеми інформаційної безпеки мереж та способи її забезпечення	4	2	12
3	Тема 3. Вимоги до ТЗІ, стандарти інформаційної безпеки	2	2	10
4	Тема 4. Принципи криптографічного захисту інформації	4	4	12
5	Тема 5. Огляд та аналіз алгоритмів криптографічного захисту інформації	4	4	6
6	Тема 6. Електронні цифрові підписи. Хешувальні функції, генерування псевдовипадкових послідовностей	2	2	12
7	Тема 7. Протоколи узгодження ключів та адміністрування ними	4	4	8
8	Тема 8. Технології автентифікації, авторизації, біометричні методи та характеристики. Криптоаналіз. Стеганографія	4	2	8
Разом		24	22	74

Самостійна робота здобувача вищої освіти

Самостійна робота здобувача організовується шляхом видачі індивідуального переліку питань і практичних завдань з кожної теми, які не виносяться на аудиторне опрацювання та виконання індивідуального творчого завдання.

Самостійна робота здобувача є одним із способів активного, цілеспрямованого набуття нових для нього знань та умінь. Вона є основою його підготовки як фахівця, забезпечує набуття ним прийомів пізнавальної діяльності, інтерес до творчої роботи, здатність вирішувати наукові та практичні завдання.

Виконання здобувачем самостійної роботи передбачає, за необхідності, отримання консультацій або допомоги відповідного фахівця. Навчальний матеріал навчальної дисципліни, передбачений робочою програмою для засвоєння здобувачем у процесі самостійної роботи, виносяться на поточний і підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався під час аудиторних занять. Організація самостійної роботи здобувачів передбачає: планування обсягу, змісту, завдань, форм і методів контролю самостійної

роботи, розробку навчально-методичного забезпечення; виконання здобувачем запланованої самостійної роботи; контроль та оцінювання результатів, їх систематизацію, оцінювання ефективності виконання здобувачем самостійної роботи.

Індивідуальні завдання здобувач виконує самостійно під керівництвом викладача згідно з індивідуальним навчальним планом.

У випадку реалізації індивідуальної освітньої траєкторії здобувача заняття можуть проводитись за індивідуальним графіком.

Види самостійної роботи

№ п/п	Вид самостійної роботи	Години	Термін виконання	Форма та метод контролю
1	Підготовка самостійних питань з тематики дисципліни (опрацювання теоретичних основ прослуханого лекційного матеріалу)	44	щотижнево / під час заліково-екзаменаційної сесії	Усне та письмове опитування, тестування, оцінювання конспекту
2	Підготовка до лекційних та практичних занять (робота з інформаційними джерелами: опрацювання першоджерел)	10	щотижнево	Усне опитування, оцінювання конспекту
3	Індивідуальні творчі практичні завдання (вирішення і письмове оформлення завдань, інших робіт графічного характеру; презентації за заданою проблемною тематикою)	10	1 раз на 2 тижні / під час заліково-екзаменаційної сесії	Спостереження за виконанням, обговорення, виступ з презентацією
4	Підготовка до контрольних робіт та тестування, виконання завдань різних видів контролю під час практичних занять (самостійне опрацювання тестів відповідно до теми практичного заняття; самостійне розв'язання практичних задач, ситуаційних вправ)	10	щотижнево / під час заліково-екзаменаційної сесії	Тестування у системі Moodle
Разом		74		

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні

1. Остапов С. Е., Євсєєв С. П., Король О. Г. [та ін.]. Технології захисту інформації : навч. посіб. Львів : Новий Світ-2000, 2024.
2. Онацький О. В., Йона Л. Г., Белова Ю. В. Криптографічний захист інформації : навч. посіб. Одеса : Астропринт, 2023. 252 с.
3. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч.

посіб. Київ : Держ. торг.-екон. ун-т, 2023. DOI: <https://doi.org/10.31617/np.knute.2023-295>.

4. Ковальчук Л. В., Маслова Н. О. Математичні методи криптографії : електрон. навч. посіб. Дрогобич : ДВНЗ «ДонНТУ», 2024.

5. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. Boca Raton : CRC Press, 2021.

6. Paar C., Pelzl J., Güneysu T. Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms. 2nd ed. Berlin : Springer, 2024.

7. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. 2nd ed. San Francisco : No Starch Press, 2024.

8. Wong D. Real-World Cryptography. Shelter Island, NY : Manning, 2021.

9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022.

10. NIST FIPS 204. Module-Lattice-Based Digital Signature Standard. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: <https://doi.org/10.6028/NIST.FIPS.204>.

Додаткові

1. Красиленко В.Г., Нікітович Д.В. Моделювання покращених сліпих електронних цифрових підписів 2D типу для систем захисту інформації. Вісник Хмельницького національного університету. Технічні науки. 2022. №1 (305). С. 72-77.

2. Krasilenko V.G., Pidlubnyi V.F., Nikitovich D.V. Research and simulation of the method of generation of the flow of matrix keys of permutations and their characteristics for encryption-masking of video frames. Вісник Хмельницького національного університету. Серія «Технічні науки». 2023. № 3. С. 339-347. URL: [http://journals.khnu.km.ua/vestnik/pdf/technew/2023/VKNU-TS-2023N3\(321\).pdf](http://journals.khnu.km.ua/vestnik/pdf/technew/2023/VKNU-TS-2023N3(321).pdf)

3. Kychak V.M., Krasilenko V.G., Nikitovich D.V. Simulation of a cooperative cryptographic protocol for creating a joint secret key- permutation of a significant dimension. Вісник Хмельницького національного університету. Серія: технічні науки. 2025. №1 (347). С. 280-290. DOI: <https://doi.org/10.31891/2307-5732-2025-347-37> . URL: <https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/1325>

4. Krasilenko V.G., Nikitovich D.V., Tytarchuk Y.O. Multi-party protocol for agreement of shared secret permutations-keys of significant dimension with their isomorphic representations. Наука і техніка сьогодні. 2024. № 6 (34). С. 689-703. URL: <http://perspectives.pp.ua/index.php/nts/article/view/12701/12763> DOI:

[https://doi.org/10.52058/2786-6025-2024-6\(34\)-689-703](https://doi.org/10.52058/2786-6025-2024-6(34)-689-703)

5. Красиленко В.Г., Нікітович Д.В. Імітаційне моделювання методів для генерування потоку великорозмірних перестановок при їх ізоморфних представленнях матрицями. Наука і техніка сьогодні. 2025. № 13 (41). С.1089-1109. URL: <http://perspectives.pp.ua/index.php/nts/article/view/18208/18262>. DOI: [https://doi.org/10.52058/2786-6025-2024-13\(41\)-1089-1009](https://doi.org/10.52058/2786-6025-2024-13(41)-1089-1009)

6. Saiko V., Krasilenko V., Kiporenko S., Chikov I., Nikitovych D. Modeling of a cryptographic protocol for matching a shared secret key-permutation of significant dimension with its isomorphic representations. CEUR Workshop Proceedings, 2023. Vol. 3646. P. 196-205. (Scopus). URL: https://ceur-ws.org/Vol-3646/Paper_19.pdf

7. Красиленко В. Г., Юрчук Н. П., Нікітович Д. В. Застосування ізоморфних матричних представлень для моделювання протоколу узгодження секретних ключів-перестановок значної розмірності. Вісник Хмельницького національного університету. Серія: Техн. науки. 2021. № 2 (295). С. 78-88

8. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: <https://doi.org/10.6028/NIST.FIPS.203>.

9. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: <https://doi.org/10.6028/NIST.CSWP.29>.

Інформаційні ресурси.

1. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. – Режим доступу: www.dstszi.gov.ua/dstszi/control/uk/index.

2. Захист інформації. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації.

3. Комплексні системи захисту інформації / [Електронний ресурс]. [Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Синюгін]–Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi.

4. <http://kist.ntu.edu.ua/textPhD/tzi.pdf>.

5. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf.

6. <http://repository.hneu.edu.ua/handle/123456789/22547>.

7. <http://dspace.wunu.edu.ua/retrieve/52646/lekzii.pdf>.

8. https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf.

9. <https://dspace.nuft.edu.ua/jspui/handle/123456789/13418>.

СИСТЕМА ОЦІНЮВАННЯ ТА ВИМОГИ ДО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

У кінці семестру, здобувач вищої освіти може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру, до 10% за показники наукової, інноваційної, навчальної, виховної роботи та студентської активності і до 30% підсумкової оцінки – за результатами підсумкового контролю.

Розподіл балів за видами навчальної діяльності

№ п.п.	Вид навчальної діяльності	Бали
Атестація 1.		
1	Участь у дискусіях на лекційних заняттях	5
2	Участь у роботі на практичних заняттях	10
3	Виконання контрольних робіт, тестування	5
4	Підготовка самостійних питань з тематики дисципліни	10
	Всього за атестацію 1	30
Атестація 2.		
1	Участь у дискусіях на лекційних заняттях	7
2	Участь у роботі на практичних заняттях	12
3	Виконання контрольних робіт, тестування	5
4	Підготовка самостійних питань з тематики дисципліни	6
	Всього за атестацію 2	30
	Показники наукової, інноваційної, навчальної, виховної роботи та студентської активності	10
	Підсумкове тестування	30
Разом		100

У кінці семестру, здобувач вищої освіти може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру, до 10% за показники наукової, інноваційної, навчальної, виховної роботи та студентської активності і до 30% підсумкової оцінки – за результатами підсумкового контролю.

Якщо здобувач упродовж семестру за підсумками контрольних заходів набрав (отримав) менше половини максимальної оцінки з навчальної дисципліни (менше 35 балів), то він не допускається до заліку. Крім того, обов'язковим при мінімальній кількості балів за підсумками контрольних заходів є виконання індивідуальної творчої роботи (презентації).

Під час виконання навчальних завдань, а також завдань поточних та підсумкових контрольних заходів не допустимо порушення академічної доброчесності. Презентації та виступи мають бути авторськими та оригінальними, інформація про результати власної навчальної (наукової, творчої) діяльності – достовірною; у разі використання ідей, розробок,

тверджень, відомостей мають бути посилення на джерела інформації з дотриманням норм законодавства про авторське право і суміжні права.

Програма навчальної дисципліни передбачає врахування результатів неформальної та інформальної освіти при наявності підтверджуючих документів як окремі кредити вивчення навчальних дисциплін.

Переведення балів внутрішньої 100-бальної шкали в національну здійснюється у відповідності до шкали.

Відповідність шкал оцінок якості засвоєння навчального матеріалу

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
75-81	C		
66-74	D	задовільно	
60-65	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