



СИЛАБУС **НАВЧАЛЬНОЇ ДИСЦИПЛІНИ** **«ТЕХНОЛОГІЇ ЗАХИСТУ** **ІНФОРМАЦІЇ»**

Рівень вищої освіти: Перший (бакалаврський)
Спеціальність: 133 Галузеве машинобудування
Рік навчання: 3-й, семестр 6-й
Кількість кредитів ECTS: 5 кредитів
Назва кафедри: Комп'ютерних наук та
цифрової економіки
Мова викладання: українська

Лектор курсу

к.т.н., доц. Красиленко Володимир Григорович

Контактна інформація
лектора (e-mail)

krasvg@i.ua

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Технології захисту інформації» є вибірковою компонентою ОПП.

Загальний обсяг дисципліни 150 год.: лекції - 26 год.; практичні заняття - 24 год., самостійна робота - 100 год.

Формат проведення: лекції, практичні заняття, консультації. Підсумковий контроль – залік.

Основні положення навчальної дисципліни можуть застосовуватися при проходженні практики, подальшому навчанні на магістерському рівні вищої освіти та фаховій діяльності.

Призначення навчальної дисципліни

Навчальна дисципліна «Технології захисту інформації» призначена для формування у здобувачів вищої освіти знань, умінь і практичних навичок щодо забезпечення захисту інформації в комп'ютерних, автоматизованих та виробничо-інформаційних системах. Вона спрямована на опанування сучасних інформаційних технологій у сфері інформаційної безпеки, методів захисту даних, забезпечення їх конфіденційності, цілісності та доступності, а також засобів ідентифікації, автентифікації та контролю передавання інформації. Вивчення дисципліни забезпечує підготовку майбутніх фахівців до застосування технологій захисту інформації під час проєктування, експлуатації та супроводу цифрових систем у галузі машинобудування, автоматизації та комп'ютерно-інтегрованих технологій.

Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Технології захисту інформації» полягає у формуванні у здобувачів вищої освіти теоретичних знань про основні загрози, ризики та небезпеки втрати інформації, а також практичних умінь щодо забезпечення її захисту в комп'ютерних мережах, інформаційних системах і програмних засобах, що застосовуються у професійній діяльності.

Дисципліна спрямована на ознайомлення здобувачів із сучасними підходами, методами і технологіями захисту інформаційних ресурсів, зокрема із засобами криптографії, криптоаналізу, стеганографії, ідентифікації, автентифікації та реалізації політики безпеки. Її вивчення забезпечує підготовку майбутніх фахівців до використання технологій захисту інформації в умовах цифровізації, автоматизації та комп'ютеризації машинобудівного виробництва.

Завдання вивчення дисципліни

Ознайомити із сучасними підходами до проблем політики безпеки та захисту інформаційних ресурсів, збереження та захисту інформації, зі складом і змістом технологічних процедур, протоколів і операцій криптографії і поглибити на основі сучасних інформаційних технологій теоретичні знання та практичні навички у галузі інформаційної безпеки та криптографічних методів захисту інформації; підготувати фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності при передачі інформації, ідентифікації, автентифікації, криптографії, інтегрованих систем, політики безпеки машинобудівного виробництва.

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

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

Інтегральна компетентність (ІК):

Здатність особи розв'язувати складні спеціалізовані задачі та практичні проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів відповідних наук і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК):

ЗК1. Здатність до абстрактного мислення.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК6. Здатність проведення досліджень на певному рівні.

Спеціальні (фахові, предметні) компетентності (ФК):

ФК1. Здатність застосовувати типові аналітичні методи та комп'ютерні програмні засоби для розв'язування інженерних завдань галузевого машинобудування, ефективні кількісні методи математики, фізики, інженерних наук, а також відповідне комп'ютерне програмне забезпечення для розв'язування інженерних задач галузевого машинобудування.

ФК2. Здатність застосовувати фундаментальні наукові факти, концепції, теорії, принципи для розв'язування професійних задач і практичних проблем галузевого машинобудування.

ФК5. Здатність застосовувати комп'ютеризовані системи проектування та спеціалізоване прикладне програмне забезпечення для вирішення інженерних завдань в галузі машинобудування.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

Програмні результати навчання (ПРН):

ПРН3. Знати і розуміти системи автоматичного керування об'єктами та процесами галузевого машинобудування, мати навички їх практичного використання.

ПРН7. Готувати виробництво та експлуатувати вироби, застосовуючи автоматичні системи підтримування життєвого циклу.

ПРН4. Здійснювати інженерні розрахунки для вирішення складних задач і практичних проблем у галузевому машинобудуванні.

ПРН14. Розробляти деталі та вузли машин із застосуванням систем автоматизованого проектування.

Вивчення даної дисципліни формує у здобувачів освіти соціальні навички (softskills): комунікативність (реалізується через: метод колективного планування, узгодження та виконання технологічних етапів, алгоритмів криптографічних перетворень, протоколів узгодження секретних ключів, моделювання), лідерські навички (реалізується через: керування роботою в групах, оцінювання проміжних результатів та взаємодій).

ПЛАН ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Назви теми	Форми організації навчання та кількість годин		Самостійна робота, кількість годин
		лекційні заняття	практичні заняття	
1	Загальні поняття захисту інформації, мета і предмет дисципліни. Класифікація ТЗІ.	4	2	10
2	Проблеми інформаційної безпеки та способи її забезпечення. Історичні аспекти. Політики безпеки.	2	2	10
3	Вимоги до ТЗІ, стандарти інформаційної безпеки. Математичні основи криптографії.	4	2	14
4	Принципи криптографічного захисту інформації.	2	4	10
5	Огляд та аналіз алгоритмів криптографічного захисту інформації. Симетричні та асиметричні системи. DES, AES, афінні шифри, RSA.	4	4	14
6	Електронні цифрові підписи. Хешувальні функції, генерування псевдовипадкових послідовностей.	4	4	12
7	Протоколи узгодження ключів та адміністрування ними.	4	4	14
8	Технології автентифікації, авторизації, біометричні методи та характеристики. Стеганографія.	2	2	16
Разом		26	24	100

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.

Види самостійної роботи

№з/п	Вид самостійної роботи	Години	Терміни виконання	Форма та метод контролю
1	Опрацювання питань, що виносяться на самостійне вивчення	20	Протягом семестру	Усне та письмове опитування, обговорення проблемних питань
2	Підготовка до лекційних та практичних занять (робота з інформаційними джерелами: опрацювання першоджерел)	36	Протягом семестру	Усне та письмове опитування, тестовий контроль, вирішення ситуаційних задач, обговорення проблемних питань
3	Індивідуальне завдання	24	1 раз на семестр	Захист індивідуального завдання, обговорення, виступ з презентацією
4	Підготовка до контрольних робіт заходів	20	2 рази на семестр	Тестування
Разом		100		

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні

1. Засоби та системи технічного захисту інформації : навч. посіб. / [І.Є. Антіпов та ін.]; Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2021. 215 с.
2. Захист інформації в комп'ютерних системах та мережах: навч. посіб., С.Г. Семенов, А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко. Х.: НТУ «ХПІ», 2021. 251 с.
3. Кузнецов О.О., Євсєєв С.П., Король О.Г. Захист інформації в інформаційних системах: навч. посіб. Харків: ХНЕУ, 2019. 510 с.
4. Математичні основи криптографії: конспект лекцій / В.А. Фільштінський, А.В. Бережний. Суми: Сумський державний університет, 2019. 138 с.
5. Тарнавський Ю.А. Технології захисту інформації: підручник, Київ: КПІ ім. Ігоря Сікорського, 2021. 162 с.

6. Технології комплексного захисту інформації в кіберпросторі : навч. посіб. / [Л. Ф. Політанський та ін. ; за заг. ред. Л. Ф. Політанського] ; Чернів. нац. ун-т ім. Юрія Федьковича. Чернівці : ЧНУ імені Юрія Федьковича, 2022. 203 с.

7. Євсєєв С. П. Кібербезпека: основи кодування та криптографії/ С. П. Євсєєв, О. В. Мілов, С. Е. Остапов, О. В. Северінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с. – Режим доступу: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdB13xCaUju>

8. Євсєєв С.П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів “Новий світ2000”, 2021. – 120 с. – Режим доступу: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdB13xCaUju>

9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdB13xCaUju>

10. . Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

Додаткові

1. Гетьман І.А., Алтухов О.В. Технології захисту інформації : посіб.; Донбас. держ. машинобуд. акад. (ДДМА). Краматорськ : ДДМА, 2018. 119 с.

2. Saiko V., Krasilenko V., Kiporenko S., Chikov I., Nikitovich 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

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

4. 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 (321). С. 339-347. DOI: 10.31891/2307-5732-2023-321-3-339-347
Режим доступу: [http://journals.khnu.km.ua/vestnik/pdf/technew/2023/VKNU-TS-2023-N3\(321\).pdf](http://journals.khnu.km.ua/vestnik/pdf/technew/2023/VKNU-TS-2023-N3(321).pdf)

5. Krasilenko V.G., Lazarev A.A, Nikitovich D.V. Multi-functional parametric (MFP) matrix-algebraic models (MAM) of cryptographic

transformations (CTs) with operations by modulo and their modeling. *Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та статей*. 2020. С. 306–313

6. Технології захисту інформації: навч. посібник С. Е. Остапов, С.П. Євсєєв, О. Г. Король. Харків: Вид. ХНЕУ, 2018. 476 с.

7. Krasilenko V.G., Lazarev A.A., Nikitovich D.V. Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In *Control and Signal Processing Applications for Mobile and Aerial Robotic Systems*. Hershey, PA: IGI Global, 2020. P. 170-214. <http://doi:10.4018/978-1-5225-9924-1.ch005> URL : <http://socrates.vsau.org/repository/getfile.php/28102.pdf>

8. Красиленко В.Г., Нікітович Д.В., Яцковська Р.О., Яцковський В.І. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису. *Системи обробки інформації*. Харків : Харківський університет Повітряних Сил імені Івана Кожедуба, 2019. № 1(156). С. 92-100.

9. Krasilenko V.G., Lazarev A.A., Nikitovich D.V. The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. *Актуальні проблеми інформаційних систем і технологій*. 2020. С. 270-282.

10. Красиленко В.Г. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // *Електроніка та інформаційні технології: збірник наукових праць*. – Львів: Львівський національний університет імені Івана Франка, 2017. – Вип. 7. С. 20-42. – Режим доступу: <http://elit.lnu.edu.ua/issue.php?lang=&number=7>

11. Krasilenko V.G. Simulating and research of block parametric matrix affine-permutation ciphers (BP_MAPCs) for cryptographic transformations / V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich // тези доповідей П'ятнадцятої міжнародної науково-практичної конференції "Математичне та імітаційне моделювання систем. МОДС 2020", м. Чернігів, 29 червня – 01 липня 2020 р. – Чернігів: ЧНТУ, 2020. С. 123-128. Режим доступу: https://drive.google.com/file/d/1yj_eIMbJtoA1z5r_Q9SW7iNm_5PjYTrm/view

12. Красиленко В.Г. Моделювання поблочових матричних афінно-перестановочних шифрів з ізоморфними представленнями блоків і ключів зображеннями / В.Г. Красиленко, Д.В. Нікітович // *Матеріали другої міжнародної науково-практичної конференції «Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2020)»*, м.Черкаси, 27-29 травня 2020 року – Черкаси: ЧНУ, 2020. С. 11-18. Режим доступу: https://fotius.cdu.edu.ua/wp-content/uploads/2020/05/BOOK_IMTСК_2020.pdf#page=11

13. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.

14. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. 53 с.

15. Krasilenko V. G., Pidlubnyi V. F., Nikitovich D. V. Modeling a method for generating a stream of secret keys in the form of permutation matrices for encryption-masking of video frames and studying its characteristics, *2023 2nd International Conference on Innovative Solutions in Software Engineering (ICISSE)*, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, 2023. P. 222-231. URL: <https://doi.org/10.5281/zenodo.10397356>.

16. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.

17. Krasilenko V.G., Kychak V. M., Nikolskyu A. I., Lazarev A. A., Nikitovych D. V. Using Mathcad and LabView for modeling algorithms for detection, localization and tracking of moving objects in video streams. *Вісник Хмельницького національного університету. Серія: технічні науки*. 2024. №1 (331). С. 196-204. URL: <https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/30/33>

18. 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>

19. 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>

20. Kychak V.M., Krasilenko V.G., Nikitovych 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>

Інтернет ресурси

1. <http://www.studentam.kiev.ua/>
2. 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
3. Захист інформації. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації.
4. 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_zahys

tu_informaciyi.

5. <http://kist.ntu.edu.ua/textPhD/tzi.pdf>
6. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
7. <http://repository.hneu.edu.ua/handle/123456789/22547>
8. <http://dspace.wunu.edu.ua/retrieve/52646/lekzii.pdf>
9. https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf
10. <https://dspace.nuft.edu.ua/jspui/handle/123456789/13418>
11. <http://er.nau.edu.ua/handle/NAU/32583>

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

	Вид навчальної діяльності	Бали
Атестація 1		
1	Участь у дискусіях на лекційних заняттях	3
2	Участь у роботі на практичних заняттях	6
3	Виконання домашніх завдань	5
4	Виконання контрольних робіт, тестування	10
5	Індивідуальні та групові творчі завдання (вирішення і письмове оформлення завдань, схем, діаграм, інших робіт графічного характеру; презентації за заданою проблемною тематикою, дослідницькі проекти)	6
	Всього за атестацію 1	30
Атестація 2		
6	Участь у дискусіях на лекційних заняттях	3
7	Участь у роботі на практичних заняттях	6
8	Виконання домашніх завдань	5
9	Виконання контрольних робіт, тестування	10
10	Індивідуальні та групові творчі завдання (презентації за заданою проблемною тематикою, дослідницькі проекти)	6
	Всього за атестацію 2	30
11	Показники наукової, інноваційної, навчальної, виховної роботи та студентської активності	10
	Підсумкове тестування	30
	Разом	100

Якщо здобувач упродовж семестру за підсумками контрольних заходів набрав менше 35 балів, то він не допускається до екзамену. Крім того, обов'язковим при мінімальній кількості балів за підсумками контрольних заходів є виконання індивідуальної творчої роботи (презентації).

Під час виконання навчальних завдань, завдань 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 посилання 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.

Відповідність шкал оцінок якості засвоєння навчального матеріалу

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою для екзамену
90 – 100	A	відмінно
82-89	B	добре
75-81	C	
66-74	D	задовільно
60-65	E	
35-59	FX	незараховано з можливістю повторного складання
0-34	F	незараховано з обов'язковим повторним вивченням дисципліни