| | |
|---|---|
| | **СИЛАБУС**<br>**НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**<br>**«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»**<br>**Рівень вищої освіти: Перший (бакалаврський)**<br>**Спеціальність: 122 Комп'ютерні науки**<br>**Рік навчання: 3-й, семестр 6-й**<br>**Кількість кредитів ECTS: 5 кредитів**<br>**Назва кафедри: Комп'ютерних наук та цифрової економіки**<br>**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 обов'язковою 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 – екзамен.

При вивченні даної дисципліни можуть використовуватись знання, отримані з таких дисциплін: «Лінійна алгебра та аналітична геометрія», «Математичний аналіз», «Організація баз даних та знань», «Теорія ймовірностей та математична статистика», «Інформаційні технології», «Комп'ютерна схемотехніка та архітектура комп'ютерів», «Проєктування інформаційних систем».

### Призначення навчальної дисципліни

Освітня компонента «Технології захисту інформації» спрямована на отримання здобувачами таких важливих і універсальних компетентностей:

- здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук, інформаційних технологій:
- здатність розуміти та застосовувати сучасні інформаційні технології у галузі інформаційної безпеки та криптографічних методів захисту інформації,

забезпечення цілісності даних, конфіденційності, контролю передачі інформації, ідентифікації, автентифікації, стеганографії, інтегрованих систем, політики безпеки, менеджменту в галузі безпеки.

### Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Технології захисту інформації» є формування теоретичних знань щодо можливих небезпек, загроз і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту інформації в комп'ютерних мережах, інформаційних системах АПК та програмній продукції. Ознайомлення із сучасними підходами до збереження та захисту інформації, зі складом і змістом технологічних процедур, протоколів і операцій криптографії, крипто-аналізу, стеганографії, що використовуються для вирішення проблем політики безпеки та захисту інформаційних ресурсів.

### 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 навики у галузі інформаційної безпеки та криптографічних методів захисту інформації; підготовити фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності при передачі інформації, ідентифікації, автентифікації, криптографії, інтегрованих систем, політики безпеки, менеджменту в галузі безпеки.

## 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 складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

*Загальні компетентності (ЗК)*

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК12. Здатність оцінювати та забезпечувати якість виконуваних робіт.

*Спеціальні (фахові) компетентності (СК)*

СК6. Здатність до системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв'язування системних задач, що мають суперечливі цілі, невизначеності та ризики.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК15. Здатність до аналізу та функціонального моделювання бізнес-процесів, побудови та практичного застосування функціональних моделей організаційно-економічних і виробничо-технічних систем, методів оцінювання ризиків їх проектування.

## ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ ВІДПОВІДНО ДО ОСВІТНЬОЇ ПРОГРАМИ

РН1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

РН2. Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації.

РН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

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, виноситься 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 до лекційних та практичних занять | 20 | щотижнево | Усне та письмове опитування |
| 2 | Підготовка самостійних питань з тематики дисципліни | 40 | щотижнево | Усне та письмове опитування |
| 3 | Індивідуальні творчі завдання (виконання презентації, презентації за заданою проблемною тематикою, дослідницькі проєкти) | 20 | 4 рази на семестр | Спостереження за виконанням, обговорення, виступ з презентацією, презентація проєкту, усний захист |
| 4 | Підготовка до контрольних робіт та тестування | 20 | 2 рази на семестр | Тестування у системі Сократ |
| **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., Євсеєв 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. Євсеєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. Харків: Вид. "Новий Світ-2000", 2023. 657 с. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

8. Євсеєв С.П. Кібербезпека: Криптографія з Python: навч. посібник. Львів "Новий світ 2000", 2021. 120 с. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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., 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

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 URL: 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. Євсеєв, 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 поблокових 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_IMTCK_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., Nikolskyy 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

## 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_zahystu_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 проєкти) | 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 (виконання гугл-презентації, презентації за заданою проблемною тематикою, дослідницькі проєкти) | 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 | незадовільно з можливістю повторного складання |
| 0-34 | F | незадовільно з обов’язковим повторним вивченням дисципліни |