Міністерство освіти і науки України
Харківський національний університет імені В.Н.Каразіна
Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”
В.о. декана факультету комп’ютерних наук
_____ Євгенія КОЛОВАНОВА
“ 30 ” ____червня____ 2023 р.

Робоча програма навчальної дисципліни

Моделі і методи комп'ютерної стеганографії

Рівень вищої освіти	третій (освітньо-науковий) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	освітньо-наукова програма підготовки докторів філософії
Вид дисципліни	вибіркова
Факультет	комп'ютерних наук

2023/2024 навчальний рік

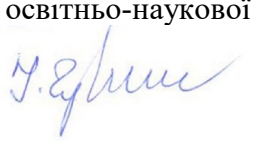
Програму рекомендовано до затвердження Вченою радою факультету комп'ютерних наук "29" червня 2023 року, протокол №14

РОЗРОБНИКИ ПРОГРАМИ: кандидат технічних наук, доцент кафедри безпеки інформаційних систем і технологій НАРЄЖНІЙ Олексій Павлович

Програму обговорено і схвалено на засіданні кафедри безпеки інформаційних систем і технологій "08" червня 2023 року, протокол № 12
В.о.завідувача кафедри безпеки інформаційних систем і технологій


Ігор СВАТОВСЬКИЙ

Програму погоджено з гарантом освітньо-наукової програми 125 "Кібербезпека"
Гарант освітньо-наукової програми "Кібербезпека"


Іван ГОРБЕНКО

Програму погоджено методичною комісією факультету комп'ютерних наук "21" червня 2023 року, протокол №12
Голова методичної комісії факультету комп'ютерних наук


Лариса ВАСИЛЬЄВА

ВСТУП

Програма навчальної дисципліни «Моделі і методи комп'ютерної стеганографії» складена відповідно до освітньо-наукової програми підготовки третього (освітньо-наукового) рівня спеціальності 125 Кібербезпека (ВБ 2.2).

1. Опис навчальної дисципліни

- Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є навчання аспірантів сучасним моделям і методам комп'ютерної стеганографії, зокрема новітнім технологіям приховування факту існування інформаційних повідомлень із застосуванням сучасних комп'ютерних засобів.

Аспіранти мають можливість використовувати отримані компетенції, знання і вміння при проведенні досліджень, виконанні наукової роботи, а також на практиці при підготовці апробацій розроблених ними моделей і методів комп'ютерної стеганографії.

- Основні завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є формування у аспірантів певних знань та вмінь з новітніх технологій приховування факту існування інформаційних повідомлень із застосуванням сучасних комп'ютерних засобів, моделей та методів стеганографічного перетворення та обчислювальних алгоритмів, а також створення прикладних додатків із застосуванням отриманих знань.

- Кількість кредитів – 6.

- Загальна кількість годин – 180.

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2й	1-й
Семестр	
2-й	1-й
Лекції	
16 год	
Практичні, семінарські заняття	
14 год	
Лабораторні заняття	
Самостійна робота	
150 год	
Індивідуальні завдання	

1.6. Заплановані результати навчання

МАТИ КОМПЕТЕНЦІЇ:

Загальні

- **ЗК 5.** Вміння виявляти, ставити та вирішувати проблеми.

Фахові компетентності

- **ФК 1.** Здатність використати сучасні досягнення науки і передових технологій;
- **ФК 6.** Професійне володіння комп'ютером та інформаційними технологіями;
- **ФК 7.** Здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування;
- **ФК 8.** Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних ітелекомунікаційних систем;
- **ФК 10.** Здатність застосовувати моделі і методи комп'ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і телекомунікаційних систем.

За результатами вивчення дисципліни аспіранти повинні

ЗНАТИ:

- математичні моделі, які застосовуються для опису сучасних стеганографічних перетворень, зокрема, при побудові стеганографічних систем за технологією прямого розширення спектру, кластерних файлових стеганосистем, мережевої стеганографії, стеганографічного 3D друку;
- сучасні методи та обчислювальні алгоритми комп'ютерної стеганографії, критерії та показники їхньої ефективності;

ВМІТИ:

- проводити порівняльні дослідження різних методів комп'ютерної стеганографії, визначати їх переваги та недоліки, обґрунтовувати обрання кращих альтернатив;
- реалізовувати у вигляді програмних та математичних моделей сучасні засоби стеганографічного перетворення, зокрема, стеганографічні системи за технологією прямого розширення спектру, кластерні файлові стеганосистеми, мережеву стеганографію, стеганографічний 3D друк;
- використовувати отриманні знання для проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування, застосовувати моделі і методи комп'ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і телекомунікаційних систем.

2. Тематичний план навчальної дисципліни

Розділ 1. Моделі і методи комп'ютерної стеганографії із застосуванням технології прямого розширення спектру.

Покоління телекомунікаційних систем. Технології розширення спектру для підвищення ефе- ктивності телекомунікацій. Застосування технології прямого розширення спектру в стеганогра- фії. Сучасні досягнення науки і передових

технологій в комп'ютерній стеганографії, моделі та методи застосування технології прямого розширення спектру.

Розділ 2. Моделі і методи комп'ютерної стеганографії із застосуванням кластерних файловихсистем.

Основні властивості та класифікація кластерних файлових систем. Приховування інформації шляхом перемішування кластерів різних покрівельних файлів. Додаткове приховування інфор-

мації при перемішуванні кластерів всередині покрівельних файлів. Додаткові шляхи збільшен- ня пропускної здатності та швидкості прихованих стеганографічних каналів.

Розділ 3. Моделі і методи мережевої стеганографії та стеганографічний 3D друк.

Моделі та методи мережевої стеганографії. Приховування інформації через маніпуляції із трафіком телекомунікаційної мережі. Новітні технології 3D друку. Методи приховування інфо- рмації із використовуванням стеганографічного 3D друку.

3. Структура навчальної дисципліни

Назви розділів	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Моделі і методи комп'ютерної стеганографії із застосуванням технології прямогорозширення спектру.												
Разом за розділом 1	62	6	6			50						
Розділ 2. Моделі і методи комп'ютерної стеганографії із застосуванням кластернихфайлових систем.												
Разом за розділом 2	62	6	6			50						
Розділ 3. Моделі і методи мережевої стеганографії та стеганографічний 3D друк.												
Разом за розділом 3	56	4	2			50						
Усього годин	**180**	**16**	**14**			**150**						

4. Теми семінарських (практичних, лабораторних) занять

№з/п	***Назва теми***	***Кількість годин***
1	Технології розширення спектру для підвищення ефективності теле-комунікацій	2
2	Застосування технології прямого розширення спектру в стеганог-рафії	4

3	Приховування інформації шляхом перемішування кластерів різнихпокрівельних файлів.	2
4	Додаткове приховування інформації при перемішуванні кластерів всередині покрівельних файлів. Додаткові шляхи збільшення про- пускної здатності та швидкості прихованих стеганографічних кана-лів	4
5	Методи приховування інформації із використовуванням стеганог-рафічного 3D друку.	2

5. Завдання для самостійної роботи

№з/п	Види, зміст самостійної роботи	***Кількість годин***
1	Покоління телекомунікаційних систем. Вивчення основних етапів роз- витку телекомунікацій, визначення основних відмінностей, переваг та еволюції телекомунікацій нової генерації.	10
2	Технології прямого розширення спектру частот та кодового розподілуканалів. Принципи побудови та практичне застосування. Сучасні прото- коли радіозв'язку, що використовують пряме розширення спектру та ко-довий розподіл каналів.	10
3	Основні положення дисертаційної роботи Лізи Марвел (дослідницька лабораторія збройних сил США) із застосування технології прямого ро- зширення спектру в стеганографії. Основні переваги та недоліки запро- понованих методів.	10
4	Основні положення нових методів на основі адресації дискретних сиг-налів. Основні переваги та недоліки. Порівняння методів Лізи Марвел та методів адресації.	20
5	Основні властивості та класифікація кластерних файлових систем.	10
6	Моделі та методи кластерних стеганосистем, запропонованих Хасаном Ханом.	20
7	Моделі та методи кластерних стеганосистем, запропонованих Альгима-нтасом Венчкаускасом.	20
8	Особливості сучасних протоколів комп'ютерних мереж. Штучна надмі- рність, яка може застосовуватися в стеганографічних цілях.	20
9	Новітні технології 3D друку.	20
10	Контрольна робота.	10
	Разом:	**150**

6. Індивідуальні завдання */Не передбачено/*

7. Методи контролю

Контроль засвоєння аспірантами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги аспірантів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

На практичних заняттях контроль засвоєння аспірантами навчального матеріалу здійснюється шляхом оцінки якості оформлення звіту і його захисту. Рівень знань, продемонстрований аспірантами при оформленні і захисті звітів з практичних занять оцінюється окремо для кожного практичного заняття (ПЗ) відповідною кількістю балів (максимальне значення балів наведено нижче в таблиці).

Додатково в межах годин, виділених на самостійну роботу (10 годин), проводиться контрольна робота (КР) за індивідуальними практичними завданнями підвищеної складності. КР оцінюється викладачем відповідною кількістю балів (максимальне значення балів наведенонижче в таблиці).

Максимальна кількість балів за результатами контролю поточної успішності протягом семестру складає 60 балів.

Таблиця 7.1 – Розподіл балів, які отримують аспіранти за результатами контролю поточноїуспішності

Вид заняття / контрольний захід	**Оцінка** N_{max}
Практичні заняття	
ПЗ 1	5
ПЗ 2	10
ПЗ 3	5
ПЗ 4	10
ПЗ 5	5
КР	25
Всього за семестр	60

Згідно рішення кафедри безпеки інформаційних систем і технологій до екзамену недопускаються аспіранти, які протягом семестру набрали менше 10 балів.

Підсумковий контроль здійснюється за результатами поточного контролю шляхомпідсумовування оцінок, отриманих за практичні заняття.

Максимальна кількість балів за результатами вивчення дисципліні складає 100 балів.

Схема нарахування балів наведена нижче в таблиці.

8. Схема нарахування балів

Бали за поточний контроль знань по розділам протягом семестру					КР	Разом сума балів у семестрі	Іспит	Загальна сума балів
ПЗ 1	ПЗ 2	ПЗ 3	ПЗ 4	ПЗ 5				
5	10	5	10	5	25	60	40	100

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних занять

Визначення	Кількість балів*

Завдання з практичного заняття виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту пока- зано розуміння суті і змісту проведених досліджень	$Nmax$
Завдання з практичного заняття виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теорети- чного матеріалу.	$[N_{max} - \lfloor N_{max} / 4 \rfloor, N_{max} - 1]$
Завдання з практичного заняття виконане в повному об- сязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були вияв- лені незначні помилки у знанні теоретичного матеріалу.	$[N_{max} - 2 \times \lfloor N_{max} / 4 \rfloor, Nmax - \lfloor N_{max} / 4 \rfloor - 1]$
Завдання з практичного заняття виконане. Звіт оформ- лений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матері- алу.	$[N_{max} - 3 \times \lfloor N_{max} / 4 \rfloor, N_{max} - 2 \times \lfloor N_{max} / 4 \rfloor - 1]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий ха- рактер. Звіт оформлений з помилками і суттєвими недо- ліками.	$[1, N_{max} - 3 \times \lfloor N_{max} / 4 \rfloor - 1]$

* $Nmax$

– максимальна кількість балів для відповідного заняття відповідно до таблиці 7.1.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка для чотирирівневої шкали оцінювання
90 – 100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

9. Рекомендована література

За розділом 1

- Buehrer, R. Michael. 2006. *Code Division Multiple Access (CDMA)*. Morgan & Claypool Publish- ers.
- Holmes, Jack Kenneth. 2007. *Spread Spectrum Systems for GNSS and Wireless Communications*. Artech House.
- Ipatov, Valery P. 2005. *Spread Spectrum and CDMA: Principles and Applications*. Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/0470091800 HYPERLINK "https://doi.org/10.1002/0470091800".
- Yang, Sung-Moon Michael. 2019. *Modern Digital Radio Communication Signals and Systems*. Springer International Publishing. https://doi.org/10.1007/978-3-319-71568-1.
- Eze, Peter U., U. Parampalli, Robin J. Evans, and D. Liu. 2018. “Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology*.”

In *2018 40th Annual Inter- national Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 1–4. https://doi.org/10.1109/EMBC.2018.8512344.

- Marvel, Lisa M., Charles G. Boncelet, and Charles T. Retter. 1998. "Methodology of Spread- Spectrum Image Steganography." ARL-TR-1698. ARMY RESEARCH LAB ABERDEEN PROV- ING GROUND MD. https://apps.dtic.mil/docs/citations/ADA349102 HYPERLINK "https://apps.dtic.mil/docs/citations/ADA349102".
- Marvel, L.M., C.G. Boncelet, and C.T. Retter. 1999. "Spread Spectrum Image Steganography." *IEEE Transactions on Image Processing* 8 (8): 1075–83. https://doi.org/10.1109/83.777088 HYPERLINK "https://doi.org/10.1109/83.777088".
- "US-6557103-B1 - Spread Spectrum Image Steganography | Unified Patents." n.d. Accessed Sep- tember 14, 2020. https://portal.unifiedpatents.com/patents/patent/US-6557103-B1.
- Kuznetsov, A., O. Smirnov, A. Arischenko, I. Chepurko, A. Onikiychuk, and T. Kuznetsova. 2020. "Pseudorandom Sequences for Spread Spectrum Image Steganography." In *Proceedings of the In- ternational Workshop on Cyber Hygiene (CybHyg-2019) Co-Located with 1st International Confer- ence on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine, November 30, 2019.*, 2654:122–31. CEUR Workshop Proceedings. CEUR-WS.org. http://ceur-ws.org/Vol-2654/paper9.pdf.
- Kuznetsov, Alexandr, Alexey Smirnov, Ludmila Gorbacheva, and Vitalina Babenko. 2020. "Hiding Data in Cover Images Using a Pseudo-Random Sequences." In *Proceedings of The Third Interna- tional Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020*, edited by Sergey Subbotin, 2608:646–60. CEUR Workshop Pro- ceedings. CEUR-WS.org. http://ceur-ws.org/Vol-2608/paper50.pdf HYPERLINK "http://ceur-ws.org/Vol-2608/paper50.pdf".
- Kuznetsov, Alexandr, Alexey Smirnov, Diana Kovalchuk, and Tetiana Kuznetsova. 2020. "New Technique for Hiding Data Using Adaptively Generated Pseudorandom Sequences." In *Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. In- tegration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kharkiv, Ukraine, Oc- tober 06-10, 2020.*, 214–27. http://ceur-ws.org/Vol-2732/20200214.pdf HYPERLINK "http://ceur-ws.org/Vol-2732/20200214.pdf".
- Смірнов, Олексій, Людмила Горбачова, Олександр Кузнецов. 2020. "Приховування інформації у зображеннях з використанням псевдовипадкових послідовностей." *Комп'ютерні науки та кібербезпека*, no. 1 (June): 4–13. https://doi.org/10.26565/2519-2310-2020-1-01.
- Kuznetsov A. Use of Complex Discrete Signals for Steganographic Information Security / Kuznetsov A., Serhiienko R., Kovtun V., Botnov A // Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – Kiev: National Aviation University "NAU-Druk" Publishung House – 2010. – pp. 143 – 146.

За розділом 2

- L. Yang, P. Chen, G. Zhu and L. Yu, "Repairing algorithm design for FAT file system in embedded system," *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, XianNing, 2011, pp. 3393-3396.
- Z. Jinhai, "Research of embedded FAT file system," *2011 International Conference on Uncertainty Reasoning and Knowledge Engineering*, Bali, 2011, pp. 44-47.
- H. Zhao, X. Li, L. Chang and X. Zang, "Fat File System Design and Research," *2015 International Conference on Network and Information Systems for Computers*, Wuhan, 2015, pp. 568-571.

- Khan, Hassan, Mobin Javed, Syed Ali Khayam, and Fauzan Mirza. n.d. “Designing a Cluster-Based Covert Channel to Evade Disk Investigation and Forensics.” *Computers & Security* 30 (1): 35– 49.
- Khan, Hassan, Mobin Javed, Fauzan Mirza, and Syed Ali Khayam. 2012. “Evading Disk Investiga- tion and Forensics Using a Cluster-Based Covert Channel,” May.
- Kuznetsov, Aleksandr, Kiril Shekhanin, Andriy Kolgatin, Katerina Kuznetsova, and Yevgeny De- menko. 2018. “Hiding Data in the File Structure.” *Комп’ютерні Науки Та Кібербезпека*, no. 1 (November): 43–52.
- Venčkauskas, Algimantas, Nerijus Morkevicius, Grigas Petraitis, and Jonas Ceponis. 2013. “Covert Channel for Cluster-Based File Systems Using Multiple Cover Files.” *Information Technology and Control* 42 (September). https://doi.org/10.5755/j01.itc.42.3.3328 HYPERLINK "https://doi.org/10.5755/j01.itc.42.3.3328".
- 刘玉, 刘洋, 饶炤骅, 朱光喜, 王长强, 熊祖彪, 李伟霞, and 徐一新. 2003. Files hiding method based on FAT32 disk files system structure. China CN1434450A, filed January 25, 2003, and issued August 6, 2003. https://patents.google.com/patent/CN1434450A/en HYPERLINK "https://patents.google.com/patent/CN1434450A/en".
- Kuznetsov, Alexandr, Kyryl Shekhanin, Andrii Kolhatin, Ivan Mikheev, and Ivan Belozertsev. 2018. “Hiding Data in the Structure of the FAT Family File System.” In *2018 IEEE 9th Internation- al Conference on Dependable Systems, Services and Technologies (DESSERT)*, 337–42. https://doi.org/10.1109/DESSERT.2018.8409155.
- Shekhanin, K. Yu, A. O. Kolhatin, E. E. Demenko, and A. A. Kuznetsov. 2019. “ON HIDING DA- TA INTO THE STRUCTURE OF THE FAT FAMILY FILE SYSTEM.” *Telecommunications and Radio Engineering* 78 (11). https://doi.org/10.1615/TelecomRadEng.v78.i11.50 HYPERLINK "https://doi.org/10.1615/TelecomRadEng.v78.i11.50".
- Shekhanin, Kyryl, Alexandr Kuznetsov, Victor Krasnobayev, and Oleksii Smirnov. 2020. “Detect- ing Hidden Information in FAT.” *International Journal of Computer Network and Information Se- curity* 12 (3): 33–43. https://doi.org/10.5815/ijcnis.2020.03.04.

За розділом 3

- Коркач И.В., Пирогова Ю.И. Використання технологій IP-телефонії для прихованої передачі информації. - [Електронний ресурс], - Режим доступу: http://tzi.ua/ ru/vikoristannya_tehnologj_ip-telefon_dlya_prihovano_ HYPERLINK "http://tzi.ua/ru/vikoristannya_tehnologj_ip-telefon_dlya_prihovano_peredach_nformac.html" HYPERLINK "http://tzi.ua/ru/vikoristannya_tehnologj_ip-telefon_dlya_prihovano_peredach_nformac.html"peredach_nformac.html.
- Генне О.В. Основні положення стеганографії [Електронний ресурс] – Режим доступу: http://easy-code.com.ua/2010/11/osnovni-polozhennya-stenografii/.
- Thurston R. Steganography developers turn their attention to hiding information in VoIP. [Електронний ресурс] – Режим доступу: http://www.scmagazineuk.com/ HYPERLINK "http://www.scmagazineuk.com/steganography-developers-turn-their-attention-to-hiding-information-in-voip/article/112102/" HYPERLINK "http://www.scmagazineuk.com/steganography-developers-turn-their-attention-to-hiding-information-in-voip/article/112102/"steganography- developers-turn-their-attention-to-hiding-information-in-voip/article/112102/
- Sekhar A. International Journal of Advanced Research in Computer and Communication Engineer- ing. Vol. 4, Special Issue 1, June 2015 [Електронний ресурс] – Режим доступу: http://www.ijarcce.com/upload/2015/ HYPERLINK "http://www.ijarcce.com/upload/2015/si/icrtcc-15/IJARCCE%2017.pdf" HYPERLINK

"http://www.ijarcce.com/upload/2015/si/icrtcc-15/IJARCCE%2017.pdf"si/icrtcc-15/IJARCCE%2017.pdf

- Ziyad Tariq Mustafa, Authman Waleed Khalid. Diyala journal for pure sciences. Packet Steganog- raphy Using IP ID. [Електронний ресурс]. – Режим доступу: http://www.sciencesmag.uodiyala.edu.iq/uploads/Volume%2010/Issue%204/English/1-10%20E.pdf
- K. Szczypiorski, HICCUPS: Hidden Communication System for Cor- rupted Networks, In Proc. of The Tenth International MultiConference on Advanced Computer Systems ACS‟2003, pp. 31-40.
- Кузнєцов, О. О., В. А. Тимченко, Б. С. Дубровний. 2015. “Аналіз та порівняльні дослідження методів мережної стеганографії.” *Прикладна радіоелектроніка*, no. 14, № 4: 384–89.
- Kuznetsov, A. A., O. O. Stefanovych, D. I. Prokopovych-Tkachenko, and K. O. Kuznetsova. 2019. “3D STEGANOGRAPHY INFORMATION HIDING.” *Telecommunications and Radio Engineering.* 78 (12). https://doi.org/10.1615/TelecomRadEng.v78.i12.30.
- Кузнецов, О. О., О. О. Стефанович, Д. І. Прокопович-Ткаченко, К. О. Кузнецова. 2018. “3D стеганографічне приховування інформації.” *Радіотехніка* 4 (195): 193–202. https://doi.org/10.30837/rt.2018.4.195.19 HYPERLINK "https://doi.org/10.30837/rt.2018.4.195.19".
- Kuznetsov, Alexandr, Oleh Stefanovych, Yuriy Gorbenko, Oleksii Smirnov, Victor Krasnobaev, and Kateryna Kuznetsova. 2019. “Information Hiding Using 3D-Printing Technology.” In *2019 10thIEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2:701–6. https://doi.org/10.1109/IDAACS.2019.8924352 HYPERLINK "https://doi.org/10.1109/IDAACS.2019.8924352".
- Kuznetsov, Alexandr, Oleh Stefanovych, Kateryna Kuznetsova, Mykola Pastukhov, and DmytroProkopovych-Tkachenko. 2018. “Method of 3D-Steganography.” *Комп’ютерні Науки Та Кібербезпека*, no. 4: 4–12.

9.2. Допоміжна література

- Alford, Robert S. 2018. *Computer Systems Engineering Management*. CRC Press. https://doi.org/10.1201/9781351070829.
- Kopetz, Hermann, ed. 1997. “Real-Time Operating Systems.” In *Real-Time Systems: Design Prin- ciples for Distributed Embedded Applications*, 211–25. The International Series in Engineering and Computer Science. Boston, MA: Springer US. https://doi.org/10.1007/0-306-47055-1_10 HYPERLINK "https://doi.org/10.1007/0-306-47055-1_10".
- Yadin, Aharon. 2016. *Computer Systems Architecture*. Chapman and Hall/CRC. https://doi.org/10.1201/9781315373287.
- Gass, Saul I., and Michael C. Fu, eds. 2013. “Shortest Path Problem.” In *Encyclopedia of Opera- tions Research and Management Science*, 1393–1393. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-1153-7_200762.
- Goto, S., T. Ohtsuki, and T. Yoshimura. 1976. “Sparse Matrix Techniques for the Shortest Path Problem.” *IEEE Transactions on Circuits and Systems* 23 (12): 752–58. https://doi.org/10.1109/TCS.1976.1084155.
- Kumar, Gaurav, Rakesh Kumar Bajaj, and Neeraj Gandotra. 2015. “Algorithm for Shortest Path Problem in a Network with Interval-Valued Intuitionistic Trapezoidal Fuzzy Number.” *Procedia*

Computer Science, Proceedings of the 4th International Conference on Eco-friendly Computing andCommunication Systems, 70 (January): 123–29. https://doi.org/10.1016/j.procs.2015.10.056 HYPERLINK "https://doi.org/10.1016/j.procs.2015.10.056".

9.3. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

- Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення. ДСТУ 3008-2015. – Чинний від 2017-07-01. – К. : ДП «УкрНДНЦ», 2016. – 26 с. – (Національний стандарт України).
- Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. ДСТУ 8302:2015. – Чинний від 2016-07-01. – К. : ДП «УкрНДНЦ», 2016. – 16 с. – (Національний стандарт України).
- “3D Printing Technologies and Techniques.” n.d. Accessed February 4, 2021. https://www.sculpteo.com/en/3d-printing/3d-printing-technologies/.
- “Overview over 3D Printing Technologies - Additively.” n.d. Accessed February 4, 2021. https://www.additively.com/en/learn-about/3d-printing-technologies.
- “The Types of 3D Printing Technology | All3DP.” n.d. Accessed February 4, 2021. https://all3dp.com/1/types-of-3d-printers-3d-printing-technology/.
- “Types of 3D Printing Technologies.” 2019. MakerBot. April 17, 2019. https://www.makerbot.com/stories/design/types-of-3d-printing-technologies/.