Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Кафедра безпеки інформаційних систем і технологій

Ухвалено
Вченою радою
факультету комп'ютерних наук
Протокол № 12 від 31.08.2020
Голова Вченої ради

Назва курсу	Моделі і методи комп'ютерної стеганографії
Викладач (-і)	професор кафедри БІСТ Кузнецов О.О.
Профайл викладача (-ів)	http://www-csd.univer.kharkov.ua/about-us/sub-faculty/kafedra-bezpeki-informatsijnih-sistem-i/personalnij-sklad/
Контактний тел.	Кафедра: (057) 705-10-83
E-mail:	kuznetsov@karazin.ua
Сторінка курсу в системі дистанційного навчання	
Консультації	*Очні консультації*: розклад в університеті (на кафедрі). *Он лайн консультації*: через e-mail.

1. Коротка анотація до курсу

Курс спрямований на 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.

2. Мета та цілі курсу

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 цілі курсу – формування у аспірантів певних компетенцій, зокрема:

- вміння виявляти, ставити та вирішувати проблеми.
- здатність використати сучасні досягнення науки і передових технологій;
- професійне володіння комп'ютером та інформаційними технологіями;
- здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування;

− здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем;

− здатність застосовувати моделі і методи комп'ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і телекомунікаційних систем.

3. Формат курсу – очний.

4. Результати навчання

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.

5. Обсяг курсу

Вид заняття	Загальна кількість годин
Лекції	16
Семінарські заняття / практичні / лабораторні	14
Самостійна робота	150
Разом:	180

6. Ознаки курсу:

Рік викладання	Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
2021	4	125 Кібербезпека	2	Нормативна (Обов'язкова)

7. Пререквізити

Попередньо прослухані курси: «Математичні методи в кібербезпеці», «Методи побудови телекомунікаційних протоколів фізичного та канального рівнів» (підготовка магістрів за спеціальністю 125).

8. Технічне та програмне забезпечення /обладнання

Для виконання практичних робіт студентам знадобиться таке програмне забезпечення: вільне спеціальне програмне забезпечення, що дозволяє проводити моделювання та реалізацію методів комп'ютерної стеганографії.

9. Політики курсу

Політика доброчесного навчання та стимулювання: передбачає бонуси (додаткові бали за творчо інноваційно виконані завдання) та штрафи (позбавлення відповідних балів за невиконані завдання та пропуск занять без поважних причин).

Політика академічної доброчесності: виконання завдань за персональними варіантами та вхідними даними, що виключає можливість використання чужих результатів.

10. Схема курсу

Тиж. / акад. год.	**Тема, план, короткі тези**	**Форма діяльності (заняття)* / Формат****	**Матеріали**	**Завдання, год**
Тиж. 1 / 2 год.	Розділ 1. Л.1. Вступ. Покоління телекомунікаційних систем. Технології розширення спектру для підвищення ефективності телекомунікацій.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 2 / 2 год	Розділ 1. Л.2. Стеганографія з розширенням спектру. Застосування технології прямого розширення спектру в стеганографії.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 3 / 2 год	Розділ 1. ПЗ.1. Технології розширення спектру для підвищення ефективності телекомунікацій	Практичне заняття / *аудиторне або дистанційне*	Завдання до ПЗ.	Виконати завдання до ПЗ, 2 год
Тиж. 4 / 2 год	Розділ 1. Л.3. Моделі і методи стеганографії з розширенням спектру. Сучасні досягнення науки і передових технологій в комп'ютерній стеганографії, моделі та методи застосування технології прямого розширення спектру.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 5,6 / 4 год	Розділ 1. ПЗ.2. Застосування технології прямого розширення спектру в стеганографії	Практичне заняття / *аудиторне або дистанційне*	Завдання до ПЗ.	Виконати завдання до ПЗ, 4 год
Тиж. 7 / 2 год	Розділ 2. Л.4. Файлові системи. Основні властивості та класифікація кластерних файлових систем.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год

Тиж. 8 / 2 год	Розділ 2. Л.5. Кластерні стеганосистеми. Приховування інформації шляхом перемішування кластерів різних покрівельних файлів.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 9 / 2 год	Розділ 2. ПЗ.3. Приховування інформації шляхом перемішування кластерів різних покрівельних файлів.	Практичне заняття / *аудиторне або дистанційне*	Завдання до ПЗ.	Виконати завдання до ПЗ, 2 год
Тиж. 10 / 2 год	Розділ 2. Л.6. Моделі і методи файлової стеганографії.	Лекція / *аудиторна або*	Презентація лекції.	Ознайомитись з літературою,
	Додаткове приховування інформації при перемішуванні кластерів всередині покрівельних файлів. Додаткові шляхи збільшення пропускної здатності та швидкості прихованих стеганографічних каналів.	*дистанційна*		переглянути презентацію, 2 год
Тиж. 11, 12 / 4 год	Розділ 2. ПЗ.4. Додаткове приховування інформації при перемішуванні кластерів всередині покрівельних файлів. Додаткові шляхи збільшення пропускної здатності та швидкості прихованих стеганографічних каналів	Практичне заняття / *аудиторне або дистанційне*	Завдання до ПЗ.	Виконати завдання до ПЗ, 4 год
Тиж. 12 / 2 год	Розділ 2. Л.7. Мережева стеганографія. Моделі та методи мережевої стеганографії. Приховування інформації через маніпуляції із трафіком телекомунікаційної мережі.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 13 / 2 год	Розділ 2. Л.8. Стеганографічний 3D друк. Новітні технології 3D друку. Методи приховування інформації із використовуванням стеганографічного 3D друку.	Лекція / *аудиторна або дистанційна*	Презентація лекції.	Ознайомитись з літературою, переглянути презентацію, 2 год
Тиж. 14 / 2 год	Розділ 3. ПЗ.5. Методи приховування інформації із використовуванням стеганографічного 3D друку.	Практичне заняття / *аудиторне або дистанційне*	Завдання до ПЗ.	Виконати завдання до ПЗ, 2 год

11. Система оцінювання та вимоги

Загальна система оцінювання курсу	Участь в роботі впродовж семестру – до 60 балів (включно). Розподіл балів, що присвоюються аспірантам з навчальної дисципліни є сумою балів за виконання всіх практичних завдань та контрольної роботи. Контрольна робота проводиться в межах годин, виділених на самостійну роботу (10 годин).
Практичні заняття	Аспірант отримує максимальну кількість балів за практичне завдання, якщо: завдання виконане повністю та без допомоги викладача; аспірант самостійно може узагальнити, систематизувати матеріал та вільно застосовує його у стандартних ситуаціях та у ситуаціях невизначеності.
Умови допуску до підсумкового контролю	Набрання студентом не менше 10 балів протягом семестру.

Розподіл балів, які отримують аспіранти за результатами контролю поточної успішності

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

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	25	60	40	100
5	10	5	10	5				

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 показано 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 теоретичного матеріалу.	□*N* [*Nmax* −□□ *max*4 □□□,*Nmax* −1]
Завдання з практичного заняття виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу.	[*Nmax* − 2×□ *max*4 □□,*Nmax* −□□□*Nmax*4 □□−1] □*N* □ □ □

Завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	$[N_{max} - 3\times\lfloor \frac{N_{max}}{4} \rfloor, N_{max} - 2\times\lfloor \frac{N_{max}}{4} \rfloor - 1]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	$[1, N_{max} - 3\times\lfloor \frac{N_{max}}{4} \rfloor - 1]$

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

12. Рекомендована література

Основна література

За розділом 1

1. Buehrer, R. Michael. 2006. *Code Division Multiple Access (CDMA)*. Morgan & Claypool Publishers.
2. Holmes, Jack Kenneth. 2007. *Spread Spectrum Systems for GNSS and Wireless Communications*. Artech House.
3. Ipatov, Valery P. 2005. *Spread Spectrum and CDMA: Principles and Applications*. Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/0470091800.
4. 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.
5. 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 International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 1–4. https://doi.org/10.1109/EMBC.2018.8512344.
6. Marvel, Lisa M., Charles G. Boncelet, and Charles T. Retter. 1998. "Methodology of Spread-Spectrum Image Steganography." ARL-TR-1698. ARMY RESEARCH LAB ABERDEEN PROVING GROUND MD. https://apps.dtic.mil/docs/citations/ADA349102.
7. 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.
8. "US-6557103-B1 - Spread Spectrum Image Steganography | Unified Patents." n.d. Accessed September 14, 2020. https://portal.unifiedpatents.com/patents/patent/US-6557103-B1.
9. 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 International Workshop on Cyber Hygiene (CybHyg-2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine, November 30, 2019.*, 2654:122–31. CEUR Workshop Proceedings. CEURWS.org. http://ceur-ws.org/Vol-2654/paper9.pdf.
10. 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 International 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 Proceedings. CEURWS.org. http://ceur-ws.org/Vol-2608/paper50.pdf.
11. 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. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kharkiv, Ukraine, October 06-10, 2020.*, 214–27. http://ceur-ws.org/Vol-2732/20200214.pdf.
12. 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 (SMSDP2010): Proceedings. – Kiev: National Aviation University "NAU-Druk" Publishung House – 2010. – pp. 143 – 146.

За розділом 2

13. 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.
14. Z. Jinhai, "Research of embedded FAT file system," *2011 International Conference on Uncertainty Reasoning and Knowledge Engineering*, Bali, 2011, pp. 44-47.
15. 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.
16. 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.
17. Khan, Hassan, Mobin Javed, Fauzan Mirza, and Syed Ali Khayam. 2012. "Evading Disk Investigation and Forensics Using a Cluster-Based Covert Channel," May.
18. Kuznetsov, Aleksandr, Kiril Shekhanin, Andriy Kolgatin, Katerina Kuznetsova, and Yevgeny Demenko. 2018. "Hiding Data in the File Structure." *Комп'ютерні Науки Та Кібербезпека*, no. 1 (November): 43–52.
19. 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.
20. **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.
21. 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 International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 337–42. https://doi.org/10.1109/DESSERT.2018.8409155.
22. Shekhanin, K. Yu, A. O. Kolhatin, E. E. Demenko, and A. A. Kuznetsov. 2019. "ON HIDING DATA INTO THE STRUCTURE OF THE FAT FAMILY FILE SYSTEM." *Telecommunications and Radio Engineering* 78 (11). https://doi.org/10.1615/TelecomRadEng.v78.i11.50.
23. Shekhanin, Kyryl, Alexandr Kuznetsov, Victor Krasnobayev, and Oleksii Smirnov. 2020. "Detecting Hidden Information in FAT." *International Journal of Computer Network and Information Security* 12 (3): 33–43. https://doi.org/10.5815/ijcnis.2020.03.04. **За розділом 3**
24. Thurston R. Steganography developers turn their attention to hiding information in VoIP. [Електронний ресурс] – Режим доступу: http://www.scmagazineuk.com/ steganography-developersturn-their-attention-to-hiding-information-in-voip/article/112102/
25. Sekhar A. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 4, Special Issue 1, June 2015 [Електронний ресурс] – Режим доступу: http://www.ijarcce.com/upload/2015/ si/icrtcc-15/IJARCCE%2017.pdf
26. Ziyad Tariq Mustafa, Authman Waleed Khalid. Diyala journal for pure sciences. Packet Steganography Using IP ID. [Електронний ресурс]. – Режим доступу: http://www.sciencesmag.uodiyala.edu.iq/uploads/Volume%2010/Issue%204/English/1-10%20E.pdf
27. 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.

28. 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.
29. Кузнецов, О. О., О. О. Стефанович, Д. І. Прокопович-Ткаченко, and К. О. Кузнецова. 2018. “3D стеганографічне приховування інформації.” *Радіотехніка* 4 (195): 193–202. https://doi.org/10.30837/rt.2018.4.195.19.
30. Kuznetsov, Alexandr, Oleh Stefanovych, Yuriy Gorbenko, Oleksii Smirnov, Victor Krasnobaev, and Kateryna Kuznetsova. 2019. “Information Hiding Using 3D-Printing Technology.” In *2019 10th IEEE 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.
31. Kuznetsov, Alexandr, Oleh Stefanovych, Kateryna Kuznetsova, Mykola Pastukhov, and Dmytro Prokopovych-Tkachenko. 2018. “Method of 3D-Steganography.” *Комп’ютерні Науки Та Кібербезпека*, no. 4: 4–12.

Допоміжна література

32. Alford, Robert S. 2018. *Computer Systems Engineering Management*. CRC Press. https://doi.org/10.1201/9781351070829.
33. Kopetz, Hermann, ed. 1997. “Real-Time Operating Systems.” In *Real-Time Systems: Design Principles 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.
34. Yadin, Aharon. 2016. *Computer Systems Architecture*. Chapman and Hall/CRC. https://doi.org/10.1201/9781315373287.
35. Gass, Saul I., and Michael C. Fu, eds. 2013. “Shortest Path Problem.” In *Encyclopedia of Operations Research and Management Science*, 1393–1393. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-1153-7_200762.
36. 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.
37. 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 and Communication Systems, 70 (January): 123–29. https://doi.org/10.1016/j.procs.2015.10.056.

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

1. 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).
2. 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).
3. “3D Printing Technologies and Techniques.” n.d. Accessed February 4, 2021. https://www.sculpteo.com/en/3d-printing/3d-printing-technologies/.
4. “Overview over 3D Printing Technologies - Additively.” n.d. Accessed February 4, 2021. https://www.additively.com/en/learn-about/3d-printing-technologies.
5. “The Types of 3D Printing Technology | All3DP.” n.d. Accessed February 4, 2021. https://all3dp.com/1/types-of-3d-printers-3d-printing-technology/.
6. “Types of 3D Printing Technologies.” 2019. MakerBot. April 17, 2019. https://www.makerbot.com/stories/design/types-of-3d-printing-technologies/.