



# СИЛАБУС ВИБІРКОВОЇ КОМПОНЕНТИ МАТЕМАТИЧНІ МЕТОДИ СТЕГANOГРАФІЇ

<b>Факультет</b>	Електроніки, автоматизація і метрології
<b>Кафедра</b>	Фізико-математичних наук
<b>Статус навчальної дисципліни</b>	<b>Вибіркова компонента освітніх програм першого (бакалаврський) рівня вищої освіти</b>
<b>Рекомендовано для спеціальностей</b>	053 Психологія; 051 Економіка; 061 Журналістика; 073 Менеджмент; 075 Маркетинг; 121 Інженерія програмного забезпечення; 122 Комп'ютерні науки; 125 Кібербезпека та захист інформації; 171 Електроніка; 172 Електронні комунікації та радіотехніка; 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 Інформаційно-вимірювальні технології; 176 Мікро- та наносистемна техніка; 275 Транспортні технології на автомобільному транспорті; 281 Публічне управління та адміністрування
<b>Форма навчання</b>	Денна, заочно-дистанційна

## Викладачі

Козін Олександр Борисович  
[alexnazaret1@gmail.com](mailto:alexnazaret1@gmail.com)



Доцент кафедри фізико-математичних наук,  
кандидат фіз.-мат. наук

## Загальна інформація про дисципліну

<b>Анотація до дисципліни</b>	Дисципліна «Математичні методи стеганографії» рекомендована для здобувачів першого (бакалаврського) рівня вищої освіти за всіма спеціальностями. В основу цього курсу входить вивчення: - основних методів комп'ютерних методів приховування передачі інформації шляхом збереження в таємниці самого факту (комп'ютерної стеганографії), які використовуються в професійній діяльності фахівця кібербезпеки, або інженерії програмного забезпечення;
-------------------------------	---

	<ul style="list-style-type: none"> <li>- елементів комп'ютерної стенографії для розв'язування завдань приховування факту існування інформації та створення водяних знаків;</li> <li>- застосування в практичній діяльності приховування фактів існування інформації та створення водяних знаків.</li> <li>- реалізації алгоритмів приховування та вилучення даних із графічних зображень, аудіосигналів, текстових документів за допомогою програмного забезпечення;</li> <li>- оцінювання стійкості стенографічних систем з використанням сучасної комп'ютерної техніки та Інтернет;</li> <li>- раціонального вибору математичного апарату та прикладного програмного забезпечення для розв'язування поставлених практичних задач;</li> <li>- складання і розв'язування наукових та професійних задач за своїм майбутнім фахом.</li> </ul>
<b>Мета дисципліни</b>	<p>Дисципліна «Математичні методи стенографії» має метою:</p> <ul style="list-style-type: none"> <li>- навчити студентів використовувати методи аналізу та захисту комп'ютерних даних,</li> <li>- дати математичне підґрунтя застосування методів комп'ютерної стенографії у практичній роботі, дослідженнях,</li> <li>- навчити логічно та аналітично мислити,</li> <li>- дати основу для розвитку навиків застосування комп'ютерної стенографії майбутньому фахівцеві,</li> <li>- за допомогою програмного забезпечення реалізовувати алгоритми приховування та вилучення даних із графічних зображень, аудіосигналів, текстових документів.</li> </ul>
<b>Компетентності, формуванню яких сприяє дисципліна</b>	<ul style="list-style-type: none"> <li>- Здатність застосовувати знання в практичних ситуаціях</li> <li>- Знання та розуміння предметної області та розуміння професійної діяльності.</li> <li>- Здатність до пошуку, оброблення та аналізу інформації.</li> <li>- Здатність до абстрактного мислення, аналізу та синтезу.</li> <li>- Здатність приймати обґрунтовані рішення</li> <li>- Здатність використовувати комп'ютерні технології та програмне забезпечення з обробки даних для вирішення практичних задач, аналізу інформації та підготовки аналітичних звітів.</li> </ul>
<b>Результати навчання</b>	<ul style="list-style-type: none"> <li>- Застосовувати ґрунтовні знання основних розділів вищої математики (лінійна та векторна алгебра, диференціальне числення, інтегральне числення, функції багатьох змінних, ряди диференціальні рівняння, теорія ймовірностей та математична статистика) в обсязі необхідному для користування математичним апаратом та методами за відповідною програмою підготовки.</li> <li>- Застосовувати основні фундаментальні та природничі знання, знання системного аналізу та технологій моделювання при проектування та розв'язання професійних задач.</li> </ul>
<b>Обсяг дисципліни</b>	Загальний обсяг дисципліни: 6 кредити ЄКТС 180 годин). Для денної форми навчання: лекції – 22 годин, практичні заняття – 22 годин, лабораторні заняття – 22 годин, самостійна робота – 114 годин
<b>Форма підсумкового контролю</b>	залік
<b>Терміни викладання</b>	

### Програма дисципліни

<b>Тема 1.</b>	<p><b>Тема 1. Вступ до курсу.</b> Вступ до курсу. Структура та зміст дисципліни. Предмет, термінологія, галузь використання. Історія розвитку. Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних. Вивчення принципів стеганографії. Комп'ютерна та цифрова стеганографія.</p>
<b>Тема 2.</b>	<p><b>Тема 2. Математичні методи стеганографічного захисту інформації.</b> Особливості зорової системи людини (ЗСЛ). Основні властивості ЗСЛ, що використовуються при приховуванні даних в зображеннях. Застосування інформаційних електронних технологій (спеціальних пакетів прикладних програм: MathCad, MatLab, Scilab для розв'язування завдань стеганографії. Приховування даних у просторовій області зображень. Методи приховування в найменш значущому біті даних. Практичне використання програмного забезпечення Hex Editor Neo. Приховування даних у просторовій області зображень (блокове приховування, метод квантування). Приховування даних у просторовій області зображень із застосуванням дискретних сигналів. Приховування даних у частотній області зображень. Метод інтегральних перетворень. Приховування даних у просторовій області аудіо сигналу (в найменш значущому біті даних), у частотній області аудіо сигналу (фазове кодування). Математичні основи приховування цифрових даних у текстовому документі. Приховування інформації у графічні та аудіо файли. Сучасні методи комп'ютерної стеганографії. Steganos Privacy Suite та її можливості. Приховування текстової інформації у графічному файлі за допомогою матриць. Приховування текстової інформації у рамці графічного об'єкта. Приховування (розміщення, впровадження) тексту у графічному контейнері та його вилучення (за допомогою програмного пакету S-Tools).</p>

### Список рекомендованих джерел

#### Базови

1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.
2. Конахович Г. Ф. Комп'ютерна стеганографія / Г. Ф. Конахович, О. Ю. Пузиренко // Теорія і практика. — К. : МК-Пресс. — 2006.
3. Пузиренко О. Ю. Використання пакету Mathcad v.12 для стеганографічного приховання секретних повідомлень у графічних файлах / Г. Ф. Конахович, О. Ю. Пузиренко // Захист інформації: Зб. наук. пр. — К. : НАУ, 2005. — № 3(26). — С. 21–34.
4. Пузиренко О. Ю. Класифікація методів стеганографічного захисту інформації у цифровому звуковому мовленні за схильністю до атак і потребою в оцінці стійкості / О. Ю. Пузиренко, О. В. Шевченко // Захист інформації: Зб. наук. пр. — К. : НАУ, 2011. — Вип. 18. — С. 52–55.
5. Pfitzmann B. Information Hiding Terminology, in Information Hiding, Springer Lecture Notes in Computer Science, v.1174, 1996, 347-350.

6. Aura T. Invisible communication. In Proc. of the HUT Seminar on Network Security '95, Espoo, Finland, November 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.
7. Ross J. Anderson. Stretching the limits of steganography. In IH96 [3], pages 39-48.
8. Zollner J., Federrath H., Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, 344-354.
9. E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.
10. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, vol. 31, no. 2, pp.26-34.

### Допоміжні

1. Тарасов Д. О. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д. О. Тарасов, А. С. Мельник, М. М. Голобородько // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка». — 2010. — № 673. — С. 365–374.
2. Стасюк О. І. та ін. Сучасні стеганографічні методи захисту інформації / О. І. Стасюк та ін. // Захист інформації. — 2011. — Т. 13. — № 1 (50).
3. Конахович Г. Ф. Сучасні методи квантової стеганографії / Г. Ф. Конахович // Захист інформації. — 2011. — Т. 13. — № 2 (51).
4. Юдін О. К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О. К. Юдін, Р. В. Зюбіна, О. В. Фролов // Радиоэлектроника и информатика. — Х. : НХНУРЕ, 2015. — № 3. — С. 24–31.

## Інформація про консультації

Очні консультації щопонеділка у 2023-2024 н/р, з 14-15 до 15-15 год., ауд. 104/а за попередньою домовленістю.

Онлайн консультації: Telegram (+38097-59-86-586) в робочі дні з 15.00 до 19.00 за попередньою домовленістю.

## Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою		Нарахування балів	Бали нараховуються таким чином: <i>Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.</i>
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано		
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	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		

### Політика опанування дисципліни

**Відвідування:** Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

**Дотримання принципів академічної доброчесності:** Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck**.

**Умови зарахування пропущених занять:** Здача індивідуальних домашніх завдань.

**Інші умови:** Навчально-методичні матеріали дисципліни розміщені за посиланням:

1. Cachin C. An information-theoretic model for steganography [Electronic resource]/ Christian Cachin // [Information and Computation, 2004], vol. 192, pp. 41-56. – Mode of access: <http://www.sciencedirect.com/science/article/pii/S0890540104000409> (Accessed 18 May 2017). – Title from the screen.
2. Pfitzmann B. Information Hiding Terminology [Electronic Resource]/ Birgit Pfitzmann// [Information Hiding, 1996], vol. 1174, pp. 347-350. – Mode of access: <https://www.bibsonomy.org/bibtex/2a2a3c63d0ffb9905c76e9842a2419cbb/dblp> (Accessed 18 May 2017). – Title from the screen.