



## Силабус освітнього компонента

Програма навчальної дисципліни



# Основи стеганографічного захисту інформації

### Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

### Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

### Освітня програма

Кібербезпека

### Кафедра

Кібербезпеки (328)

### Рівень освіти

Бакалавр

### Тип дисципліни

Спеціальна (фахова), Обов'язкова

### Семестр

5

### Мова викладання

Українська

## Викладачі, розробники



### КОРОЛЬОВ Роман Володимирович

[korolevrv01@ukr.net](mailto:korolevrv01@ukr.net)

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХП».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелідженс», «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

## Загальна інформація

### Анотація

Навчальна дисципліна "Основи стеганографічного захисту інформації" є обов'язковою навчальною дисципліною. Дисципліна спрямована на придбання студентами навичок та принципів побудови, реалізації та застосування стеганографічних систем та протоколів, вміня застосовувати методи, алгоритми та засоби оцінки стеганостійкості та інших якісних показників стеганосистем та стеганографічних протоколів.

### Мета та цілі дисципліни

Отримання студентами необхідних базових знань з цифрової стеганографії, яка використовується для приховування факту існування інформації та створення водяних знаків. Особливу увагу в курсі приділяють вивченню проблематики використання цифрової стеганографії у сучасному інформаційному просторі, аналізу атак на стеганограми та оцінки стійкості.

### Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

## Компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

## Результати навчання

РН-1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

РН-2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН-3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН-4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН-5. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН-7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

РН-8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

РН-11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

РН-12. Розробляти моделі загроз та порушника.

РН-13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

- РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
- РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
- РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- РН-19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
- РН-21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- РН-23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- РН-25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
- РН-26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
- РН-27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- РН-29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
- РН-30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
- РН-32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
- РН-33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
- РН-34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
- РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН-41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН-42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

РН-43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

РН-44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

РН-45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

РН-46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

РН-48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН-49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН-51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

РН-52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

РН-53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН-54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

## **Обсяг дисципліни**

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

## **Передумови вивчення дисципліни (пререквізити)**

Основи криптографічного захисту, Математичні основи криптології.

## **Особливості дисципліни, методи та технології навчання**

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проекти, майстер-класи.

## **Програма навчальної дисципліни**

### **Теми лекційних занять**

#### **Тема 1. Цифрова стеганографія.**

Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану. Предмет, термінологія, галузь використання.

#### **Тема 2. Математична модель стеганосистем.**

Стеганографічні протоколи. Практичні аспекти вбудовування даних.

**Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації.**

Класифікація стеганографічних систем та стегоконтейнерів.

**Тема 4. Особливості зорової системи людини.**

Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.

**Тема 5. Цифрові формати нерухомих зображень.**

Формати BMP, GIF, TIFF, JPEG. Особливості комп'ютерної обробки зображень.

**Тема 6. Приховування даних у просторовій області зображень.**

Метод приховування в найменш значущому біті даних.

**Тема 7. Приховування даних у частотній області зображень. Метод Коха та Жао.**

Приховування конфіденційної інформації в частотній множині зображення.

**Тема 8. Особливості слухової системи людини.**

Основні властивості слухової системи людини, що використовуються при приховуванні даних в аудіо сигналах. Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis).

Особливості комп'ютерної обробки аудіо сигналів.

**Тема 9. Цифрові водяні знаки.**

Узагальнена модель системи цифрових водяних знаків. Класифікація системи цифрових водяних знаків.

**Тема 10. Цифрові відбитки.**

Термінологія й основні положення. Статистична реєстрація відбитка. Схема асиметричної реєстрації відбитка.

**Тема 11. Приховані канали в комп'ютерних системах і мережах.**

Приховані канали в операційних системах. Приховування даних у виконуваних файлах. Поняття клептрографії.

## **Теми практичних занять**

Практичні роботи в рамках дисципліни не передбачені.

## **Теми лабораторних робіт**

**Тема 1. Програмні засоби стеганографічного захисту інформації.**

**Тема 2. Работа з програмою стеганографічного захисту інформації Steganos Security Suite.**

**Тема 3. Приховування даних в просторовій області зображень методом найменш значимого біта.**

**Тема 4. Приховування даних в просторовій області зображень методом перестановок.**

## **Самостійна робота**

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

## **Неформальна освіта**

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.



## Література та навчальні матеріали

### Основна література:

1. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу:  
<http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>
2. Кузнецов О.О. Стеганографія: навчальний посібник / О.О.Кузнецов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2015. – 232 с.  
<http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/2289/1/%d0%a1%d1%82%d0%b5%d0%b3%d0%b0%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d0%b8%d1%8f.pdf>
3. Хорошко В.О. Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпинець – Вінниця : ВНТУ, 2017. – 155 с.  
[https://learn.ztu.edu.ua/pluginfile.php/272322/mod\\_resource/content/1/Xoroshko\\_Komputer\\_2017\\_155.pdf](https://learn.ztu.edu.ua/pluginfile.php/272322/mod_resource/content/1/Xoroshko_Komputer_2017_155.pdf)
4. Козюра В.Д. Захист інформації в комп'ютерних системах :підручник / В.Д.Козюра, В.О.Хорошко, М.Є.Шелест – Ніжин : ФОП Лукьяненко В.В., ТПК «Орхідея», 2020. – 236 с.  
<http://ir.stu.cn.ua/bitstream/handle/123456789/19248/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B2%20%D0%BA%D0%BE%D0%BC%D0%BF.%20%D1%81%D0%B8%D1%81.%20New%20booklet%201.pdf?sequence=1&isAllowed=y>
5. Конахович Г.Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник /Г.Ф. Конахович, Д.О.Прогонов, О.Ю. Пузиренко. – К. – «Alex Print Centre», 2018/ – 558 с.  
[https://books.google.com.ua/books?id=clcDwAAQBAJ&printsec=frontcover&hl=uk&source=gbg\\_summary\\_r&cad=0#v=onepage&q&f=false](https://books.google.com.ua/books?id=clcDwAAQBAJ&printsec=frontcover&hl=uk&source=gbg_summary_r&cad=0#v=onepage&q&f=false).

### Додаткова література :

6. Євсєєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с. – Режим доступу:  
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>
7. Євсєєв С.П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів "Новий світ-2000", 2021. – 120 с. – Режим доступу:  
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>
8. 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-GBG006AnvjQHU1SdBl3xCaUju>
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.  
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>
10. 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-GBG006AnvjQHU1SdBl3xCaUju>
11. 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.  
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBG006AnvjQHU1SdBl3xCaUju>.

## Система оцінювання

### Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

### Шкала оцінювання

| Сума балів | Національна оцінка                            | ECTS |
|------------|-----------------------------------------------|------|
| 90–100     | Відмінно                                      | A    |
| 82–89      | Добре                                         | B    |
| 75–81      | Добре                                         | C    |
| 64–74      | Задовільно                                    | D    |
| 60–63      | Задовільно                                    | E    |
| 35–59      | Незадовільно<br>(потрібне додаткове вивчення) | FX   |
| 1–34       | Незадовільно<br>(потрібне повторне вивчення)  | F    |

## Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

## Погодження

Силабус погоджено

28.08.2024



Завідувач кафедри

Сергій ВСЕЄВ

28.08.2024



Гарант ОП

Сергій ВСЕЄВ