Силабус дисципліни «Стеганографія»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР · ОП «ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС»

120

Годин загальний обсяг дисципліни

4

Кредити ЄКТС відповідно до стандарту

4

Змістовних модулі курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Стеганографія

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки курсу

Мета дисципліни

Дисципліна «Стеганографія» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері методів і засобів прихованої передачі та зберігання інформації. Курс спрямований на опанування теоретичних основ стеганографії, алгоритмів впровадження даних у цифрові мультимедійні об'єкти (зображення, аудіо, відео, текст), методів стегоаналізу та цифрових водяних знаків як інструментів захисту авторських прав і забезпечення конфіденційності в інформаційно-комунікаційних системах.

Форми навчання

- Лекції — 30 годин
- Практичні заняття — 30 годин
- Самостійна робота — 60 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання науково-технічної інформації у сфері стеганографії та захисту інформації: виявлення суттєвих властивостей стеганосистем, порівняння алгоритмів впровадження даних, формування обґрунтованих висновків щодо стійкості та ефективності стеганографічних методів. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час розробки та аналізу стеганографічних алгоритмів.

Здатність до усної та письмової фахової комунікації: чітко пояснювати принципи функціонування стеганосистем, аргументовано обґрунтовувати вибір методів захисту інформації. Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді під час виконання практичних завдань з програмної реалізації стеганографічних алгоритмів.

- Аналізувати методи та алгоритми стеганографії і стегоаналізу
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі та розподіляти обов'язки

Фахові компетентності

Розуміння сутності та закономірностей стеганографічного захисту інформації, його місця у системі забезпечення інформаційної безпеки в інформаційно-комунікаційних системах. Знання ключових понять, математичних моделей і алгоритмів цифрової стеганографії, вміння застосовувати їх у практичній діяльності фахівця з кібербезпеки та захисту інформації.

Здатність застосовувати методи впровадження даних у різні типи цифрових контейнерів для забезпечення конфіденційності та прихованості факту передачі інформації, а також виявляти стеганографічні вкраплення засобами стегоаналізу в умовах ІКС.

- Характеризувати моделі та класифікацію стеганосистем
- Застосовувати методи впровадження даних у зображення, аудіо та відео
- Реалізовувати стеганографічні алгоритми програмними засобами
- Виконувати стегоаналіз та виявляти приховані дані
- Застосовувати цифрові водяні знаки для захисту авторських прав

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять стеганографії: стегоконтейнер, стегоключ, пропускна здатність стеганоканалу, стеганографічна стійкість, невидимість, цифровий водяний знак, стегоаналіз, LSB-метод, методи на основі перетворень. Характеризувати математичні моделі стеганосистем та класифікацію стеганографічних методів захисту інформації.

2

Аналіз та оцінювання

Аналізувати стеганографічні системи з точки зору вимог інформаційної безпеки, виявляти вразливості та загрози розкриття прихованого повідомлення. Оцінювати стійкість стеганографічних алгоритмів до атак стегоаналізу, порівнювати ємність і якість контейнерів після впровадження даних.

3

Застосування знань

Застосовувати алгоритми просторової та частотної стеганографії для прихованої передачі інформації в цифрових зображеннях, аудіо- та відеофайлах. Розробляти та програмно реалізовувати стеганографічні алгоритми, проводити їх тестування та оцінку стійкості в умовах різних атак.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо вибору стеганографічних методів захисту інформації для конкретних умов функціонування ІКС. Формувати професійну відповідальність і розуміння важливості прихованого каналу зв'язку та меж етичного застосування стеганографії у фаховій діяльності.

Модуль 1. Теоретичні основи стеганографії та стеганосистем

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Поняття та сутність стеганографії. Місце стеганографії в системі захисту інформації. Історія розвитку стеганографії. Основні терміни та визначення: стеганографія, стегоконтейнер, стегоключ, стегоповідомлення, стегоканал, стеганографічна стійкість. Співвідношення стеганографії та криптографії. Принципи і вимоги до стеганографічних систем.

Тема 1.2

Математичні моделі стеганосистем. Загальна модель стеганографічної системи. Класифікація стеганографічних систем. Модель Сімонса. Показники якості стеганосистем: пропускна здатність каналу, непомітність, стійкість. Стеганографічний трикутник (ємність — непомітність — стійкість). Стеганографічні протоколи та їх аналіз.

Тема 1.3

Класифікація та галузі застосування стеганографічних методів. Класифікація за типом контейнера: зображення, аудіо, відео, текст, мережевий трафік. Класифікація за областю обробки: просторова область, область перетворень. Застосування стеганографії: прихована комунікація, захист авторських прав, аутентифікація, відстеження витоків. Правові та етичні аспекти застосування стеганографії.

Тема 1.4

Цифрові водяні знаки (ЦВЗ) як різновид стеганографії. Поняття, класифікація та властивості ЦВЗ: видимі та невидимі, крихкі та робастні. Сфери застосування ЦВЗ: захист авторських прав, контроль цілісності, аутентифікація мультимедіа. Порівняльний аналіз стеганографії та технологій ЦВЗ. Стандарти у сфері ЦВЗ та їх практичне застосування.

Модуль 2. Стеганографія зображень та аудіосигналів

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Методи стеганографії в просторовій області зображень. Особливості зорової системи людини та їх використання у стеганографії. Метод заміни молодших значущих бітів (LSB). Методи на основі псевдовипадкових послідовностей. Метод Куттера–Джордана–Боссена. Адаптивні методи просторової стеганографії. Оцінка ємності та якості зображення після впровадження (PSNR, SSIM).

Тема 2.2

Методи стеганографії в частотній області зображень. Перетворення ДКП, ДВП та їх застосування у стеганографії. Метод Коха–Жао. Стеганографія на основі JPEG-стиснення (F5, Outguess, JPHide). Методи на основі вейвлет-перетворення. Стеганографія в палітрових зображеннях. Порівняльний аналіз просторових та частотних методів за критеріями ємності і стійкості.

Тема 2.3

Стеганографія в аудіосигналах. Психоакустична модель слуху та її використання у стеганографії. Методи стеганографії в аудіо: LSB-метод, ехо-стеганографія, фазове кодування, метод розширення спектра. Стеганографія в аудіоформатах MP3, WAV, FLAC. Пропускна здатність аудіоканалу приховування. Оцінка стійкості аудіостеганографії до атак.

Модуль 3. Стеганографія відео, тексту та мережевих протоколів

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Відеостеганографія та захист авторських прав мультимедіа. Особливості відео як стегоконтейнера. Методи впровадження даних у відеопотоки: між- та внутрікадрові методи. Стеганографія у стиснених відеоформатах (H.264/AVC, H.265/HEVC). Цифрові водяні знаки для відео: робастні та крихкі схеми. Захист авторських прав потокового відео від несанкціонованого копіювання та модифікації.

Тема 3.2

Текстова стеганографія. Методи текстової стеганографії: структурні (міжрядкові та міжсимвольні інтервали), семантичні (синонімічна заміна), синтаксичні. Стеганографія в документах форматів PDF, DOCX. Лінгвістична стеганографія. Кодування даних через форматування тексту. Порівняльний аналіз методів текстової стеганографії за показниками непомітності та ємності.

Тема 3.3

Мережева стеганографія та приховані канали в ІКС. Поняття та класифікація прихованих каналів в комп'ютерних мережах. Стеганографія в заголовках мережевих протоколів (IP, TCP, UDP, HTTP). Метод LACK, VoIP-стеганографія. Виявлення та протидія прихованим каналам в ІКС. Нормативно-правові аспекти використання прихованих каналів в інформаційно-комунікаційних системах.

Модуль 4. Стегоаналіз та практична реалізація стеганосистем

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Основи стегоаналізу. Поняття, задачі та класифікація стегоаналізу: пасивний (виявлення факту наявності), активний (руйнування або модифікація). Статистичні методи стегоаналізу: χ^2-тест, RS-аналіз, SPA-аналіз. Атаки на стеганографічні системи: атака з відомим контейнером, з відомим повідомленням, з вибраним контейнером. Показники ефективності стегоаналізу.

Тема 4.2

Сучасні методи стегоаналізу на основі машинного навчання. Використання методів машинного навчання для виявлення стеганографічних вкраплень. Ознакові простори для стегоаналізу зображень: SPAM, SRM, maxSRM. Нейромережеві підходи до стегоаналізу (XuNet, SRNet). Методи протидії стегоаналізу: адаптивна стеганографія, мінімізація щільності вкраплення. Оцінка стійкості стеганосистем до сучасних атак.

Тема 4.3

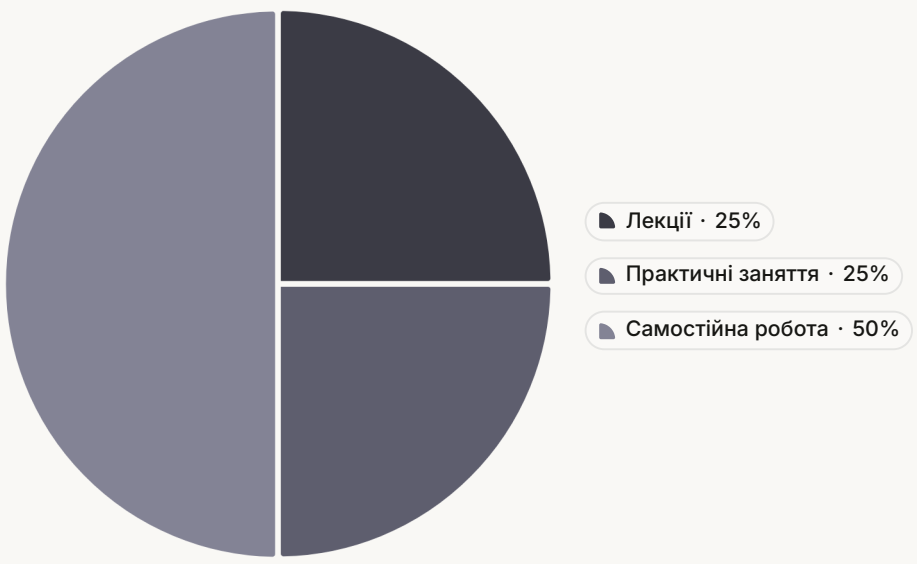
Програмна реалізація стеганографічних систем. Огляд програмних засобів стеганографії: OpenStego, SilentEye, Steghide, OutGuess. Принципи розробки власного стеганографічного застосунку. Реалізація алгоритмів LSB та DCT-стеганографії мовою Python. Тестування стеганографічних алгоритмів та оцінка їх параметрів. Виявлення стеганографії за допомогою спеціалізованих інструментів стегоаналізу.

Тема 4.4

Комплексний захист інформації засобами стеганографії в ІКС. Інтеграція стеганографії та криптографії для забезпечення багаторівневого захисту: стегокриптографічні системи. Практичні сценарії застосування стеганографії в сучасних ІКС. Стандарти та нормативно-правова база у сфері захисту мультимедіа та авторських прав. Перспективи розвитку стеганографії в умовах квантових обчислень та ШІ.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Поняття та сутність стеганографії	2	2	4
	Тема 1.2 — Математичні моделі стеганосистем	2	2	4
	Тема 1.3 — Класифікація та галузі застосування	2	2	4
	Тема 1.4 — Цифрові водяні знаки	2	2	4
Модуль 2	Тема 2.1 — Стеганографія в просторовій області	2	4	6
	Тема 2.2 — Стеганографія в частотній області	2	4	6
	Тема 2.3 — Стеганографія аудіосигналів	2	4	6
Модуль 3	Тема 3.1 — Відеостеганографія та захист авторських прав	2	2	6
	Тема 3.2 — Текстова стеганографія	2	2	6
	Тема 3.3 — Мережева стеганографія та приховані канали	4	2	6
Модуль 4	Тема 4.1 — Основи стегоаналізу	2	2	4
	Тема 4.2 — Стегоаналіз на основі машинного навчання	2	2	4
	Тема 4.3 — Програмна реалізація стеганосистем	2	2	6
	Тема 4.4 — Комплексний захист засобами стеганографії в ІКС	2	2	4
Разом		**30**	**30**	**60**



Структура навчального часу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

- **Лекції (30 год. — 25%):** подача ключового теоретичного матеріалу з основ стеганографії та стегоаналізу
- **Практичні (30 год. — 25%):** відпрацювання навичок реалізації та аналізу стеганографічних алгоритмів
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, програмна реалізація, підготовка завдань

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками зі стеганографії та захисту інформації, науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до класифікації та оцінки стеганографічних систем.

Індивідуальні завдання

Виконання аналітичних та практичних завдань щодо програмної реалізації стеганографічних алгоритмів мовою Python, підготовка аналітичних звітів з оцінки стійкості та ємності стеганосистем, дослідження методів стегоаналізу.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), НБУВ (**nbuv.gov.ua**), журналу «Кібербезпека: освіта, наука, техніка» (**csecurity.kubg.edu.ua**). Аналіз наукових публікацій, методичних рекомендацій та стандартів у сфері стеганографії та інформаційної безпеки.

Підготовка до занять

Підготовка до практичних занять шляхом опрацювання алгоритмів та їх математичного підґрунтя; підготовка до тестувань через вивчення ключових термінів та визначень; систематизація знань перед контрольними роботами з модулів дисципліни.

Методи викладання

→ Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, математичних моделей і прикладів реалізації алгоритмів; студенти ведуть конспекти та задають уточнювальні запитання.

→ Кейс-стаді

Аналіз реальних сценаріїв виявлення прихованих каналів та стеганографічних атак; студенти виявляють проблему, пропонують методи стегоаналізу та обґрунтовують висновки щодо стійкості системи.

→ Практичні вправи

Реалізація стеганографічних алгоритмів (LSB, DCT, ехо-стеганографія) мовою Python; впровадження даних у різні типи контейнерів; оцінка якості та стійкості отриманих стегоконтейнерів.

→ Робота зі спеціалізованим ПЗ

Практичне використання інструментів стеганографії та стегоаналізу (Steghide, OpenStego, StegSpy, zsteg); формування навичок роботи з реальними інструментами захисту інформації.

→ Самостійне дослідження

Підготовка аналітичних звітів і презентацій за обраною темою (сучасні методи стеганографії, застосування ШІ у стегоаналізі тощо); розвиток навичок самостійного пошуку наукової інформації.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання завдань, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові відповіді на запитання, виконання практичних завдань з реалізації стеганографічних алгоритмів та участь у вирішенні кейсів зі стегоаналізу.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання або звіт, які охоплюють теми змістовних модулів (теоретичні питання, реалізація алгоритму, аналіз стійкості стеганосистеми, оцінка метрик якості контейнера). Оцінюються повнота відповіді, правильність реалізації та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання з усіх чотирьох модулів курсу. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали оцінювання: 100-бальна система з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Усі методи контролю спрямовані на формування компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: підручник. — Житомир : ЖНАЕУ, 2023. — 636 с.
2. Дудикевич В. Б., Хорошко В. О. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 312 с.
3. Корченко О. Г., Архипов О. Є. Системи захисту інформації: стандарти та нормативна база: підручник. — Київ : НАУ, 2022. — 398 с.
4. Малахов С. В., Гончаров М. А. Синтез імовірнісних карт градієнтів яскравості цифрових зображень для коригування параметрів стеганографічної вставки даних // Grail of Science. — 2024. — № 47. — С. 545–554.
5. Бодня М., Єсіна М., Пономар В. Дослідження можливостей застосування стеганографічних та криптографічних алгоритмів для приховування інформації // Комп'ютерні науки та кібербезпека. — 2024. — № 2. — С. 43–57.
6. Козіна Г. Л., Савченко І., Воскобойник В., Карпуков Л. Стеганографічна система захисту фотографій з використанням крихких водяних знаків // Системи та технології. — 2023. — № 64(2). — С. 75–81.
7. Рубан І. В., Болгова Н. М., Мартовицький В. О. Інформаційна технологія підтвердження права власності на цифрові зображення // Сучасні інформаційні системи. — 2022. — Т. 6, № 1. — С. 118–123.
8. Салієва О., Грицак А., Білик О., Гуменюк В. Стеганографічні методи захисту відеоконтенту з використанням крихких цифрових водяних знаків // Вісник ХНТУ. — 2023.
9. Леськів А. В., Паращук С. Д. Електронний документообіг та захист інформації в органах державної влади: навч. посіб. — Київ : Академперіодика, 2024. — 268 с.
10. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник. — Київ : ДУІКТ, 2022. — 476 с.

Офіційні інтернет-ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. Офіційний сайт Верховної Ради України. — URL: **https://zakon.rada.gov.ua/**
3. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
4. Міністерство цифрової трансформації України. — URL: **https://thedigital.gov.ua/**
5. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
6. Журнал «Захист інформації» (електронне видання). — URL: **https://захист-інформації.укр/**
7. Сучасні інформаційні системи (Advanced Information Systems). — URL: **https://ais.khpi.edu.ua/**
8. Репозитарій ХНЕУ ім. С. Кузнеця (матеріали зі стеганографії). — URL: **https://repository.hneu.edu.ua/**

Рекомендована література охоплює видання та статті **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення ОП «Організація захисту інформації в ІКС».