МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

ОСНОВИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузьзнань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший(бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри
кібербезпеки та інформаційних технологій *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 12 від 31.08.2020 р.

Розробник(-и):
Корольов Р.В., к.т.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Інформація є одним з найцінніших предметів сучасного життя. Отримання доступу до неї з появою глобальних комп'ютерних мереж стало неймовірно простим. У той же час, легкість і швидкість такого доступу значно підвищили і загрозу порушення безпеки даних при відсутності заходів щодо їх захисту, а саме, - загрозу неавторизованого доступу до інформації.

Переваги подання та передачі даних в цифровому вигляді (легкість відновлення, висока потенційна завадостійкість, перспективи використання універсальних апаратних і програмних рішень) можуть бути перекреслені з легкістю, з якою можливі їх викрадення і модифікація. Тому в усьому світі назріло питання розробки методів (заходів) щодо захисту інформації організаційного, методологічного і технічного характеру, серед них - методи криптографії та стеганографії.

Метою криптографії є приховання смислового вмісту повідомлень за рахунок їх спеціального перетворення (шифрування). На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення або факт передачі його по каналах зв'язку.

Метою навчальної дисципліни " Основи стеганографічного захисту інформації"є 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 стеганограмми та оцінки стійкості.

Результатами вивчення даної дисципліни є придбання навичок та принципів побудови, реалізації та застосування стеганографічних систем та протоколів, вміння застосовувати методи, алгоритми та засоби оцінки стеганостійкості та інших якісних показників стеганосистем та стеганографічних протоколів.

Характеристика навчальної дисципліни

Курс	**4**
Семестр	**1**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	Екзамен

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	Постреквізити
Комплексні системи захисту	Дипломний проект
ІС і Інтеронет-технології	
Математичні основи криптології	

Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–21вирішувати 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–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–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–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–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 ріні 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.

Програма навчальної дисципліни

Змістовий модуль 1. Вступ до стеганографії

Тема 1. *Структура та зміст дисципліни, її зв'язок з іншими дисциплінами учбового плану. Цифрова стеганографія. Предмет, термінологія, галузь використання.*

Тема 2. *Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних.*

Змістовий модуль 2. Стеганографічні методи захисту інформації

Тема 3. *Основні напрямки практичного використання стеганографічніх 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 просторої області зображень. Метод приховування в найменш значущому біті даних.*
Тема 7. *Приховування даних у просторової області зображень методом псевдовипадкової перестановки.*
Тема 8. *Приховування даних у просторової області зображень методом блокового приховування, заміни палітри та квантування зображення.*
Тема 9. *Приховування даних у частотній області зображень. Метод Коха та Жао.*
Тема 10. *Особливості слухової системи людини (ССЛ). Основні властивості ССЛ, 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 11. *Методи текстової стеганографії. Аналіз реалізації методів.*
Тема 12. *Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків.*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

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 проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- вміння організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності;
- вміння діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
- вміння вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою;
- вміння здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лабораторні заняття: максимальна кількість балів становить 42, а мінімальна – 21.

Контрольні роботи: максимальна кількість балів становить 6, а мінімальна – 3.

Лекційні заняття: максимальна кількість балів становить 12, а мінімальна – 6.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Зміст практичних завдань екзаменаційних білетів побудований таким чином, щоб перевірити ступінь відповідності підготовки студента вимогам положень освітньо-кваліфікаційної характеристики за напрямом підготовки.

Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – оцінюється 10 балами; третє завдання оцінюється 10 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної “Відомості обліку успішності”.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	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	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1.	***Аудиторна робота***			
	Лекція	Лекція №1. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами учбового плану. Цифрова стеганографія. Предмет, термінологія, галузь використання.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція №2. Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 1. Програмні засоби стеганографічного захисту інформації.	Захист лабораторної роботи	7
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція №3. Основні напрямки практичного використання стеганографічніх методів захисту інформації. Класифікація стеганографічніх систем та стегоконтейнерів.		1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 4.	***Аудиторна робота***			
	Лекція	Лекція №4. Особливості зорової системи людини. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 2. Приховування даних в просторової області зображень	Захист лабораторної роботи	7

		методом найменш значимого біта.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 5.	***Аудиторна робота***			
	Лекція	Лекція №5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Особливості комп'ютерної обробки зображень.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 6.	***Аудиторна робота***			
	Лекція	Лекція №6. Приховування даних у просторої області зображень. Метод приховування в найменш значущому біті даних.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 3. Приховування даних в просторової області зображень методом перестановок.	Захист лабораторної роботи	7
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 7.	***Аудиторна робота***			
	Лекція	Лекція №7. Приховування даних у просторової області зображень методом псевдовипадкової перестановки	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 8.	***Аудиторна робота***			
	Лекція	Лекція №8. Приховування даних у просторової області зображень методом блокового приховування, заміни палітри та квантування зображення.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 4. Приховування даних в просторової області зображень методом блочного приховування.	Захист лабораторної роботи	7
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 9.	***Аудиторна робота***			
	Лекція	Лекція №9. Приховування даних у частотній області зображень. Метод Коха та Жао.	Робота на лекції	1
			Контрольна робота	3
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 10.	***Аудиторна робота***			
	Лекція	Лекція №10. Особливості слухової системи людини (ССЛ). Основні властивості ССЛ, що використовуються при приховуванні даних в аудіо сигналах Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis). Особливості комп'ютерної обробки аудіо сигналів.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Приховування даних в просторової області зображень методом Коха-Жао.	Захист лабораторної роботи	7
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 11.	***Аудиторна робота***			
	Лекція	Лекція №11. Методи текстової стеганографії. Аналіз реалізації методів.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 12.	***Аудиторна робота***			
	Лекція	Лекція №12. Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 6. Работа з програмою стеганографічного	Захист лабораторної	7

		захисту інформації Steganos Security Suite.	роботи	
			Контрольна робота	3
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Кузнецов О.О. Стеганографія:навчальний посібник / О.О.Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

2. Барсуков В. С. Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века [Электронный ресурс] / В. С. Барсуков, А. П. Романцов // Специальная техника. – Режим доступа : http://st.ess.ru.

3. Грибунин В.Г. Стеганографическая защита речевых сигналов в каналах открытой телефонной связи / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // Сборник тезисов Российской НТК “Методы и технические средства обеспечения безопасности информации”. – СПб. : ГТУ, 2001. – С. 83–84.

4. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

5. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : «МК-Пресс», 2006. – 288 с.

6. Оков И. Н. Электронные водяные знаки как средство аутентификации передаваемых сообщений / И. Н. Оков, Р. М. Ковалев // Защита информации. Конфидент. – 2001. – № 3. – С. 80–85.

Додаткова

7. Основи комп’ютерної стеганографії : навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця : ВДТУ, 2003. – 143 с.

8. Cox I.J., Miller M.L., Bloom J.A., Fridrich J., Kalker T. Digital Watermarking and Steganography, 2008. — 623 p.

Інформаційні ресурси

9.web.archive.org/web/20140221205846/http://er.nau.edu.ua/bitstream/NAU/8049/1/CompSteganoRU.pdf

10. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “ Основи стеганографічного захисту інформації” https://pns.hneu.edu.ua/course/view.php?id=5390