МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
М.В. Афанасьєв

ОСНОВИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузьзнань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**перший(бакалаврський)**
Освітня програма	**"КІБЕРБЕЗПЕКА "**

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

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 26.08.2019 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

1. Вступ

Анотація навчальної дисципліни:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. В даний час набули широкого поширення засоби і методи несанкціонованого доступу і отримання інформації в кіберпросторі. Вони знаходять все більше застосування не тільки в діяльності державних правоохоронних органів розвинених держав, а й в діяльності хакерів і різного роду злочинних кіберугрупувань.

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.

Мета навчальної дисципліни: метою 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.

Курс	**3**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**32**
	семінарські, практичні	**–**
	лабораторні	**32**
Самостійна робота		**86**
Формапідсумковогоконтролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи криптографічного захисту	Основи технічного захисту інформації
Комплексні системи захисту інформації	Проектування систем захисту мереж наступного покоління

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки.	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі кібербезпеки.
Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

3. 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

Структура та зміст дисципліни, зв’язок з іншими дисциплінами учбового плану, призначення стеганографічної системи, основна термінологія та визначення, потенціальні області використання стеганографії.

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

Загальна структурна схема стеганосистем як систем зв'язку, стеганографічні системи з відкритим та закритими ключами. Призначення стеганодектору.

Змістовий модуль 2. Стеганографічні методи захисту інформації.

Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації. Класифікація стеганографічних систем та стегоконтейнерів.

Основні напрями стегонографії. Вбудовування інформації з метою її прихованої передачі; вбудовування цифрових водяних знаків, вбудовування ідентифікаційних номерів, вбудовування заголовків. Загальна класифікацію контейнерів.

Тема 4. Особливості зорової системи людини. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.

Аналіз механізмів зорового сприйняття людини. Низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні. Високорівневі властивості зорової системи людини.

Тема 5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Особливості комп'ютерної обробки зображень.

Структура форматів BMP, GIF, TIFF, JPEG. Структура файлів растрового зображення. Дескриптор екрана форматі GIF, термінатор GIF, розширений блок GIF.

Тема 6. Приховування даних у просторої області зображень. Метод приховування в найменш значущому біті даних.

Метод приховування в найменш значущому біті даних.

Тема 7. Приховування даних у просторової області зображень методом псевдовипадкової перестановки

Метод псевдовипадкової перестановки для приховування даних у просторової області зображень.

Тема 8. Приховування даних у просторової області зображень методом блокового приховування, заміни палітри та квантування зображення.

Метод блокового приховування. Метод заміни палітри. Метод квантування зображення.

Тема 9. Приховування даних у частотній області зображень. Метод Коха та Жао.

Приховування даних у частотній області зображень методом Коха та Жао.

Змістовий модуль 3. Приховування даних в аудіосигналах

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.

Класи аудиосигналів.Опис форматів WAV, WMA, MP3, AAC, OGG Vorbis

Тема 11. Приховування даних у просторій множині аудіосигналу .. Приховування даних у частотній множині аудіо сигналу.

Приховування в найменш значущому біті даних та за допомогою ехосигналів.Фазове кодування.

Тема 12. Приховування даних в аудіосигналах за допомогою методів розширення спектра

Призначеня стегакодера й стеганодекодера. Вплив на ЦВДЗ застосування до аудіосигналу ковзного фільтра середніх частот

Змістовий модуль 4. Приховування даних у текстових файлах.

Тема 13. Методи текстової стеганографії. Аналіз реалізації методів.

Методи текстової стеганографії. Порівняння методів текстової стеганографії

Змістовий модуль 5. Атаки на стегосистеми та протидія їм.

Тема 14. Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків

Атаки на стеганосистеми цифрових відео знаків.

Тема 15. Методи протідії атакам на системи цифрових водяних знаків.

Статистичний стегоаналіз та протидії.

Методи протідії атакам на системи цифрових водяних знаків.

Тема 16. Практична оцінка стійкості стеганосистем . Теоретико-складнісний підхід до оцінки стійкості стеганосистем . Імітостійкість систем передачі прихованих повідомлень.

Класифікація атак зловмисника. Досконала стеганосистема.

Лабораторні роботи:

Лабораторна робота 1. Програмні засоби стеганографічного захисту інформації.

Лабораторна робота 2.Приховування даних в просторової області зображень методом найменш значимого біта.

Лабораторна робота 3. Приховування даних в просторової області зображень методом перестановок.

Лабораторна робота 4. Приховування даних в просторової області зображень методом блочного приховування.

Лабораторна робота 5. Приховування даних в просторової області зображень методом квантування.

Лабораторна робота 6. Приховування даних в просторової області зображень методом Коха-Жао.

Лабораторна робота 7. Приховування даних в аудіосигнали методом фазового кодування.

Лабораторна робота 8. Работа з програмою стеганографічного захисту інформації Steganos Security Suite.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

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

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

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

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв’язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення

інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та незалежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо конкретної проблеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на лабораторних заняттях.

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.

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.

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.

Розподіл балів за тижнями

(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля			Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Екзамен	Усього
Змістовий модуль1	**Тема 1**	1 тиждень	1				1
	Тема 2	2 тиждень	1	5			6
Змістовий модуль 2	**Тема 3**	3 тиждень	1				1
	Тема 4	4 тиждень	1	5			6
	Тема 5	5 тиждень	1				1
	Тема 6	6 тиждень	1	5			6
	Тема 7	7 тиждень	1				1
	Тема 8	8 тиждень	1	5			6
	Тема 9	9 тиждень	1		2		3
Змістовий модуль 3	**Тема 10**	10 тиждень	1	5			6
	Тема 11	11 тиждень	1				1
	Тема 12	12 тиждень	1	5			6
Змістовий модуль 4	**Тема 13**	13 тиждень	1				1
Змістовий модуль 5	**Тема 14**	14 тиждень	1	5			6
	Тема 15	15 тиждень	1				1
	Тема 16	16 тиждень	1	5	2		8
ЕКЗАМЕН						40	40
Усього			16	40	4	40	100

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
1 – 34	F		

5. Рекомендована література

5.1. 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.

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.

5.2. Інформаційні ресурси в Інтернеті

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