

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



ОСНОВИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
робоча програма навчальної дисципліни

Галузь знань *12 Інформаційні технології*

Спеціальність *125 Кібербезпека*

Освітній рівень *перший(бакалаврський)*

Освітня програма *Кібербезпека*

Статус дисципліни

обов'язкова

Мова викладання, навчання та оцінювання

українська

Завідувач кафедри
кібербезпеки
та інформаційних технологій

Ольга СТАРКОВА

Харків
2022

ЗАТВЕРДЖЕНО

на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 30.08.2022 р.

Розробник(-и):

Семенов С.Г., д.т.н., проф., професор 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 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 стеганограми 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	Залік

Структурно-логічна схема вивчення навчальної дисципліни:

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

Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
<p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>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</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.)</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p> <p>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</p>	<p>РН-9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p>
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p>	<p>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</p>

Компетентності	Результати навчання
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p>	<p>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);</p>
<p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p>	<p>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</p>
<p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>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</p>

Компетентності	Результати навчання
<p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>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;</p>
<p>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</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>РН-33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p>

Компетентності	Результати навчання
<p>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</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>РН-34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p>

Компетентності	Результати навчання
<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>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</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.)</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>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 та/або кібербезпеки;</p>

Компетентності	Результати навчання
<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p> <p>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</p>	<p>РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p>
<p>КЗ 2. Знання та розуміння предметної області та розуміння професії</p> <p>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</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки</p> <p>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</p>	<p>РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;</p>

Компетентності	Результати навчання
<p>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</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>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;</p>
<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>РН–45 застосовувати рині класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p>

Компетентності	Результати навчання
<p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою</p> <p>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</p>	<p>РН-46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах</p>

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 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 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 за темами: Математична модель стеганосистем, Стеганографічні протоколи, Практичні аспекти вбудовування даних; презентації, бесіди за темами: Основні напрямки практичного використання стеганографічних методів захисту інформації, Класифікація стеганографічних систем та стегоконтейнерів; індивідуальні та групові проєкти за темами: Приховування даних у просторі області зображень, Метод приховування в найменш значущому біті даних.

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 – 100 балів; мінімальна сума – 60 балів);
- 2) підсумковий/семестровий контроль, що проводиться у формі заліку, 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 організувати 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 заліку, 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 100, а мінімальна – 60.

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 цей вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру. Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням 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.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Рейтинг-план навчальної дисципліни

Т е м а	Форми та види навчання		Форми оцінювання	Мак бал
Т е м а 1.	<i>Аудиторна робота</i>			
	Лекція	Лекція №1. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами освітньо-професійної програми. Цифрова стеганографія. Предмет, термінологія, галузь використання.		
	<i>Самостійна робота</i>			
Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою			
Т е м а 2.	<i>Аудиторна робота</i>			
	Лекція	Лекція №2. Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних.		
	Лабораторне заняття	Лабораторна робота 1. Програмні засоби стеганографічного захисту інформації.	Захист лабораторної роботи	10
<i>Самостійна робота</i>				
Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою			
Т	<i>Аудиторна робота</i>			

е м а 3	Лекція	Лекція №3. Основні напрямки практичного використання стеганографічних методів захисту інформації. Класифікація стеганографічних систем та стегоконтейнерів.		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 4.	<i>Аудиторна робота</i>			
	Лекція	Лекція №4. Особливості зорової системи людини. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.		
	Лабораторне заняття	Лабораторна робота 2. Приховування даних в просторової області зображень методом найменш значимого біта.	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 5.	<i>Аудиторна робота</i>			
	Лекція	Лекція №5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Особливості комп'ютерної обробки зображень.		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т	<i>Аудиторна робота</i>			

е м а 6.	Лекція	Лекція №6. Приховування даних у просторі області зображень. Метод приховування в найменш значущому біті даних.		
	Лабораторне заняття	Лабораторна робота 3. Приховування даних в просторовій області зображень методом перестановок.	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 7.	<i>Аудиторна робота</i>			
	Лекція	Лекція №7. Приховування даних у просторовій області зображень методом псевдовипадкової перестановки		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 8.	<i>Аудиторна робота</i>			
	Лекція	Лекція №8. Приховування даних у просторовій області зображень методом блокового приховування, заміни палітри та квантування зображення.		
	Лабораторне заняття	Лабораторна робота 4. Приховування даних в просторовій області зображень методом блочного приховування.	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т	<i>Аудиторна робота</i>			

е м а 9.	Лекція	Лекція №9. Приховування даних у частотній області зображень. Метод Коха та Жао.		
	Контрольна робота			20
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 1 0.	<i>Аудиторна робота</i>			
	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.		
	Лабораторне заняття	Лабораторна робота 5. Приховування даних в просторовій області зображень методом Коха-Жао.	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 1 1.	<i>Аудиторна робота</i>			
	Лекція	Лекція №11. Методи текстової стеганографії. Аналіз реалізації методів.		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т	<i>Аудиторна робота</i>			

е м а 1 2.	Лекція	Лекція №12. Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків.		
	Лабораторне заняття	Лабораторна робота 6. Робота з програмою стеганографічного захисту інформації Steganos Security Suite.	Захист лабораторної роботи	10
	Контрольна робота			20
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, Д.О. Прогонов. А. Ю. Пузыренко. – К. : «Центр учбової літератури», 2018. – 558 с.
2. Sheshang Degadwala Cryptography using Modified ASCII Conversion & Mathematical Function / Sheshang Degadwala , Abbas Tukiwala , Amit Nayak - LAP LAMBERT Academic Publishing (July 10, 2019) – 132p.

Додаткова

3. Rakesh Kumar All about Steganography and detection of Stegano Images Paperback – LAP LAMBERT Academic Publishing (January 30, 2018) - 56 p.
4. Ismael Abdul Sattar Steganography In Spatial Domain Paperback – LAP LAMBERT Academic Publishing (January 3, 2018) – 52 p.

Інформаційні ресурси

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