форма № Н - 3.04

Харківський національний університет радіоелектроніки
(повне найменування вищого навчального закладу)
Кафедра Безпеки інформаційних технологій

ЗАТВЕРДЖУЮ
Декан факультету КІУ

_____Ляшенко О.С.
(підпис, прізвище, ініціали)
"____" _____2017 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“СТЕГАНОГРАФІЧНІ СИСТЕМИ”
(шифр і назва навчальної дисципліни)

напрям підготовки 125 "Кібербезпека”
(шифр і назва напряму підготовки)

Спеціальність _____
(шифр і назва спеціальності)

спеціалізація Безпека інформаційних і комунікаційних систем
(назва спеціалізації)

факультет «Комп’ютерної інженерії і управління»
(назва інституту, факультету, відділення)

2017 – 2018 навчальний рік

Робоча програма дисципліни “СТЕГАНОГРАФІЧНІ СИСТЕМИ” для студентів
(назва навчальної дисципліни)
за напрямом підготовки 125 "Кібербезпека”, спеціалізація “Безпека інформаційних і комунікаційних систем.– 20 с.

Розробник: Федюшин О.І. доцент кафедри БІТ, к.т.н, доцент
(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робочу програму схвалено на засіданні кафедри Безпеки інформаційних технологій

Протокол від “29”_____08_____2017 року № __1_

Завідувач кафедри Безпеки інформаційних технологій

_____ (Халімов Г.З.)
(підпис) (прізвище та ініціали)

Схвалено методичною комісією факультету КІУ

Протокол від “_04__”_____09_____ 2017 р. № _1__

Голова методичної комісії _____ ___(Філіпенко І.В.)__
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td></td></tr>
<tr><td rowspan="2">Кількість кредитів – 4</td><td>Галузь знань
12 Інформаційні технології
(шифр і назва)</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>Напрям підготовки
125 “Кібербезпека”
(шифр і назва)</td></tr>
<tr><td>Модулів 2</td><td rowspan="5">Спеціалізація:
“Безпека інформаційних і комунікаційних систем</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів –4</td><td>4-й</td><td></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: контрольне розрахункове завдання</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 120</td><td>7-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання: аудиторних – 3,1 самостійної роботи студента –3,6</td><td rowspan="11">Освітньо-кваліфікаційний рівень: бакалавр</td><td>24 год.</td><td></td></tr>
<tr><td>Практичні</td><td>Семінарські</td></tr>
<tr><td>4год.</td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td></td></tr>
<tr><td colspan="2">Консультації</td></tr>
<tr><td>8 год.</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>64 год.</td><td></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Примітка**.**

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми навчання –47:53;

для заочної форми навчання –

2. Мета та завдання навчальної дисципліни

Предметом вивчення навчальної дисципліни є процеси, механізми, методи, системи та засоби стеганографічного захисту інформації в інформаційних системах (ІС) та інформаційно-телекомунікаційних системах (ІТС).

Програма навчальної дисципліни складається з таких розділів:

1. Вступ до цифрової стеганографії;

2. Стеганографічні методи приховування даних в контейнерах-зображеннях;

3. Стеганографічні методи приховування даних в аудіофайлах

4. Лінгвістична та технічна стеганографія.

2.1. *Метою* викладання навчальної дисципліни є формування у студентів певних професійних компетенцій, знань та вмінь у галузі цифрової стеганографії, методів та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

2.2. Основними *завданнями* з вивчення навчальної дисципліни є отримання студентами необхідних базових знань з теоретичних основ побудови стеганографічних систем захисту інформації, моделей та методів стеганографічного перетворення та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

2.3. Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких *результатів навчання*:

ЗНАТИ:

- визначення, класифікацію та основні властивості стеганографічних систем;
- математичні моделі стеганографічних перетворень та абстрактне визначення стеганографічних систем;
- методи та обчислювальні алгоритми стеганографічного захисту інформації при вбудовуванні даних в графічні зображення, аудіосигнали, текстові документи;
- визначення, класифікацію та основні атаки на стеганосистеми та методи протидії;

ВМІТИ:

- практично реалізовувати обчислювальні алгоритми стегнаографічного перетворення, зокрема, алгоритми приховування та вилучення даних із графічних зображень, аудіосигналів, текстових документів;

- оцінювати пропускну спроможність каналів передавання схованої інформації, рівень внесених похибок в контейнери-оригінали та ймовірнісні властивості стеганографічних систем (ймовірність помилкового вилучення інформаційних повідомлень, тощо);

- оцінювати стійкість стенографічних систем до різних атак на стеганографічні системи.

3. Програма навчальної дисципліни

МОДУЛЬ1.Стеганографічні системи.

Змістовний модуль 1. Вступ до стеганографії

Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання

1. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану

2. Цифрова стеганографія. Предмет, термінологія, галузь використання

Тема 2. Математична модель та структурна схема стеганосистеми

1. Структурна схема та формальне математичне визначення криптографічної (секретної) системи. Ймовірності показники та умова теоретично недешифрованої секретної системи.

2. Математична модель та структурна схема стеганографічної системи. Ймовірності показники та умова теоретично недетектованої стеганографічної системи.

Тема 3. Атаки на стегосистеми

1. Класифікація атак на секретні та стеганографічні системи

2. Атаки на системи прихованої передачі повідомлень та на системи цифрових водяних знаків (ЦВЗ).

МОДУЛЬ2. Стеганографічні методи приховування даних

Змістовний модуль 2. Стеганографічні методи приховування даних в контейнерах-зображеннях

Тема 4. Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень

1. Особливості ЗСЛ, які використовуються в стеганографії
2. Основні формати цифрових зображень. Растрові дані. Формат зображень Bitmap Picture (bmp)

Тема 5. Приховування даних у просторовій області нерухомих зображень

1. Методи приховування на основі модифікації найменш значущого біту даних (НЗБ)
2. Блокове приховування, метод квантування, метод «хреста»

Тема 6. Приховування даних із використанням технології прямого розширення спектру

1. Складні дискретні сигнали та технологія прямого розширення спектру
2. Приховування даних із застосуванням складних дискретних сигналів

Тема 7. Приховування даних у частотній області нерухомих зображень

1. Основні етапи алгоритму стиску зображень JPEG. Дискретно-косинусне перетворення
2. Метод Коха-Жао та його модифікації
3. Метод Фридріх

Змістовний модуль 3. Стеганографічні методи приховування даних в аудіофайлах

Тема 8. Особливості слухової системи людини (ССЛ), які використовуються в стеганографії. Основні формати аудіофайлів

1. Особливості ССЛ та їх застосування в стеганографії
2. Основні формати аудіофайлів. Формат аудіофайлів Waveform Audio Format (wav)

Тема 9. Приховування даних у просторовій області аудіо сигналів

1. Методи приховування на основі модифікації НЗБ

2. Метод кодування луна-сигналів

Тема 10. Приховування даних у частотній області аудіо сигналів

1. Основні властивості дискретного перетворення Фурье. Амплітудний, частотний та фазові спектри аудіосигналів

2. Метод фазового кодування

Змістовний модуль 4. Лінгвістична та технічна стеганографія

Тема 11. Приховування даних у текстових документах

1. Лінгвістичні властивості, які використовуються в стеганографії

2. Методи приховування даних на основі довільних інтервалів

3. Синтаксичні методи приховування даних

4. Семантичні методи приховування даних

Тема 12. Стеганографічні методи із застосуванням технологій 3D друку

1. Класифікація та основні властивості відомих технологій 3D друку

2. Штучна надмірність 3D моделей, яка використовується в стеганографії

3. Методи приховування даних із застосуванням технологій 3D друку

Тема 13. Приховування даних у кластерних файлових системах

1. Особливості побудови файлових систем зберігання даних

2. Штучна надмірність кластерних файлових систем, яка використовується в стеганографії

3. Методи приховування даних у кластерних файлових системах

Тема 14. Мережна стеганографія

1. Методи модифікації вмісту інформаційних пакетів

2. Методи модифікації полів заголовків телекомунікаційних протоколів

3. Гібридні методи

4. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
МОДУЛЬ 1.Стеганографічні системи												
Змістовний модуль 1. Вступ до стеганографії												
Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання	4	2				2						
Тема 2. Математична модель та структурна схема стеганосистеми. Критерії та показники ефективності стеганосистем	10	2	2			6						
Тема 3. Атаки на стегосистеми	4	2				2						
Разом за розділом 1	18	6	2			10						
МОДУЛЬ 2. Стеганографічні методи приховування даних												
Змістовний модуль 2. Стеганографічні методи приховування даних в контейнерах-зображеннях												
Тема 4. Особливості ЗСЛ, які використовуються в стеганографії. Основні формати цифрових зображень	4	2				2						
Тема 5. Приховування даних у просторовій області нерухомих зображень	12	2		8		2						

Тема 6. Приховування даних із використанням технології прямого розширення спектру	10	2		4		4						
Тема 7. Приховування даних у частотній області нерухомих зображень	8	2		4		2						
Разом за розділом 2	34	8	0	16		10						
Змістовний модуль 3. Стеганографічні методи приховування даних в аудіофайлах												
Тема 8. Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів	6	2				4						
Тема 9. Приховування даних у просторовій області аудіо сигналів	11	1		2		8						
Тема 10. Приховування даних у частотній області аудіо сигналів	11	1		2		8						
Разом за розділом 3	28	4	0	4		20						
Змістовний модуль 4. Лінгвістична та технічна стеганографія												
Тема 11. Приховування даних у текстових документах	9	1	2			6						
Тема 12. Стеганографічні методи із застосуванням	7	1				6						

технологій 3D друку												
Тема 13. Приховування даних у кластерних файлових системах	8	2				6						
Тема 14. Мережна стеганографія	8	2				6						
Разом за розділом 4	32	6	2			24						
Консультації за розкладом	8											
Усього годин	144	24	4	20		64						

5. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми (форма поточного контролю)	Кількість годин
1	Математична модель та структурна схема стеганосистеми. Критерії та показники ефективності стеганосистем. (ПЗ1)	2
2	Приховування даних у просторовій області нерухомих зображень. Методи приховування на основі модифікації НЗБ (ЛР1)	4
3	Приховування даних у просторовій області нерухомих зображень. Блокове приховування, метод квантування, метод «хреста» (ЛР2)	4
5	Приховування даних із застосуванням складних дискретних сигналів та технології прямого розширення спектру (ЛР3)	4
6	Приховування даних у частотній області нерухомих зображень. Метод Коха-Жао та його модифікації (ЛР4)	4
7	Стеганографічні методи приховування даних в аудіофайлах (ЛР5)	4
8	Приховування даних у текстових документах (ПЗ2)	2
	Разом	24

6. Самостійна робота

№ з/п	Назва теми	Кількість годин	Форма контролю
1	Цифрова стеганографія. Предмет, термінологія, галузь використання	2	Поточний контроль у формі усного опитування
2	Математична модель та структурна схема стеганосистеми (КР1)	6	Поточний контроль у формі усного опитування
3	Атаки на стегосистеми	2	Поточний контроль у формі усного опитування
4	Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень	2	Поточний контроль у формі усного опитування
5	Приховування даних у просторовій області нерухомих зображень(КР2)	2	Поточний контроль у формі усного опитування
6	Приховування даних із використанням технології прямого розширення спектру(КР3)	4	Поточний контроль у формі усного опитування
7	Приховування даних у частотній області нерухомих зображень(КР4)	2	Поточний контроль у формі усного опитування
8	Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів	4	Поточний контроль у формі усного опитування
9	Приховування даних у просторовій області аудіо сигналів(КР5)	8	Поточний контроль у формі усного опитування
10	Приховування даних у частотній області аудіо сигналів	8	Поточний контроль у формі усного опитування
11	Приховування даних у текстових документах (КР6)	6	Поточний контроль у формі усного опитування
12	Стеганографічні методи із застосуванням технологій 3D друку	6	Поточний контроль у формі усного опитування
13	Приховування даних у кластерних файлових системах	6	Поточний контроль у формі усного опитування
14	Мережева стеганографія(КР7)	6	Поточний контроль у формі усного опитування
	Разом	64	

7. Індивідуальні завдання

Індивідуальні завдання студентів пов’язані з вивченням окремих, в тому

іноземних джерел, за тематикою дисципліни, проведенням аналізу існуючих та перспективних засобів захисту інформації, дослідженням рівнів стійкості, розробленням імітаційних моделей та дослідженням ефективності в тому числі із застосуванням принципу масштабування. Теми індивідуальних завдань, як правило, пов'язуються з науковими та науково - методичними дослідженнями, які веде кафедра та інші підрозділи університету чи інші підприємства чи заклади тощо, фірми.

Основними формами реалізації результатів виконання індивідуального завдання є:

– доповідь чи виступ на семінарських чи практичних заняттях;

– доповідь на тематичних науково - практичних конференціях з опублікуванням тез чи доповідей;

– підготовка та опублікування наукових та науково - практичних статей;

– підготовка та подання результатів досліджень для використання в НДР та ДКР кафедри;

– участь в розробці науково - методичних та навчальних матеріалів;

– підготовка патентів на винаходи та корисні моделі;

– розробка та опис програмних продуктів та моделей тощо.

8. Методи навчання

Вивчення дисципліни передбачає: лекції, практичні та лабораторні заняття, контрольні роботи, самостійну роботу студентів.

Вивчення дисципліни «Стеганографічні системи» засновується на знаннях, отриманих в процесі вивчення дисциплін підготовки бакалаврів напряму «Кібербезпека»: «Інформаційно-комунікаційні системи», «Інформаційні технології», «Технології програмування», «Прикладна криптологія».

Організація навчання здійснюється за кредитно-модульною системою з рейтинговим оцінюванням знань студентів у відповідності з Концепцією впровадження в Україні Болонського процесу.

Методи навчання:

– словесні,

– наочні,

– практичні.

Словесні методи навчання:

– лекція,

– пояснення;
– диспути.

Лекція – основний вид навчальних занять. Структура лекції підпорядковується логіці предмета, вона повинна стимулювати конкретно-образне мислення та активізувати логічне мислення студентів. Висунені в лекції ідеї викладають на високому рівні, але з урахуванням рівня підготовки студентів. Усі поняття та терміни треба поясняти, аргументувати, широко застосовувати наочність, активізувати увагу студентів тощо. Предметом лекції має бути вивчення складних об'єктів, явищ, подій, процесів, що мають між собою зв'язки і залежності причинно-наслідкового характеру.

Лекція – вид навчальних занять, призначений для викладення теоретичного матеріалу. Як правило, окрема лекція є елементом курсу лекцій, що охоплює основний теоретичний матеріал одної або декількох тем навчальної дисципліни. Тематика лекцій визначається навчальною програмою дисципліни.

Лектор зобов'язаний дотримуватися навчальної програми щодо тем лекційних занять, але не обмежується в питаннях трактування навчального матеріалу, формах і засобах доведення його до осіб, які навчаються.

Лекція проводиться у відповідно обладнаних приміщеннях – аудиторіях. Якщо це передбачено навчальною програмою дисципліни, лекції можуть проводитися дистанційно з використанням електронних засобів комунікації.

Оцінки за роботу здобувачів вищої освіти на лекціях та результати поточного контролю (тестового контролю, експрес-контролю та ін.) під час лекцій враховуються при виставленні семестрової підсумкової оцінки.

Пояснення – доказовий виклад матеріалу, пов'язаний з вивченням правил, природничо-математичних законів та явищ. Викладач висуває певну тезу і подає систему її обґрунтування. Метод пояснення застосовують як на лекціях, так і під час практичних, лабораторних занять, консультацій тощо.

Семінарські заняття як метод навчання базується на обміні думками між студентами, викладачем та студентами. Цей метод сприяє формуванню вмінь мислити самостійно, виважено аргументувати свої думки та поважно ставитися до думок інших. Наукова суперечка не лише поглиблює знання студентів, а й викликає особливий інтерес до навчання. Здійснюється під час проведення спеціальних семінарів. **Семінарське заняття** базуються в тому числі на визначенні стану проблемних питань криптосистем та крипто протоколів та можливих шляхів їх розв’язання.

Наочні методи навчання:

- спостереження,
- ілюстрація,
- демонстрація.

Ілюстрація – показ ілюстрованих посібників (плакатів, карт, рисунків на дошці та екрані, таблиць тощо). Ілюстрація передбачає показ матеріалів у статичному вигляді.

Демонстрація – передбачає показ матеріалів у динаміці: демонстрація роботи приладів, технічних пристроїв, різного роду дослідів, при використанні комп'ютерного проектора та ін.

Практичні методи навчання:

- лабораторні роботи,
- практичні заняття,
- науково-дослідне завдання.

Практична робота як метод навчання передбачає застосування знань у ситуаціях, наближених до майбутньої професійної діяльності. Упродовж цієї роботи треба провести якісь заміри, зіставити, визначити ознаки та властивості предметів або явищ, зробити висновки.

Практичне заняття – вид навчального заняття, на якому особи, які навчаються, під керівництвом науково-педагогічного працівника закріплюють теоретичні положення навчальної дисципліни і набувають вмінь та навичок їх практичного застосування шляхом індивідуального виконання відповідно сформульованих завдань

Практичні заняття проводяться в аудиторіях або в навчальних лабораторіях, оснащених необхідними технічними засобами навчання, обчислювальною технікою тощо. З окремих навчальних дисциплін допускається поділ академічної групи на підгрупи, що повинно бути зазначено в робочих навчальних планах. Перелік тем практичних занять визначається програмою навчальної дисципліни.

Практичне заняття включає проведення контролю знань, вмінь та навичок, постановку загальної проблеми (завдання) науково-педагогічним працівником та її обговорення за участю осіб, які навчаються, розв'язання задач з їх обговоренням, розв'язання контрольних завдань, їх перевірку та оцінювання.

Лабораторне заняття – вид навчального заняття, на якому особа, яка навчається, під керівництвом науково-педагогічного працівника проводить натурні або імітаційні експерименти чи дослідження з метою практичного підтвердження окремих теоретичних положень, набуває практичних навичок роботи з лабораторним обладнанням, оснащенням, обчислювальною технікою, вимірювальною апаратурою, оволодіває методиками експериментальних досліджень в конкретній предметній галузі та обробки отриманих результатів.

Лабораторні заняття проводяться у спеціально оснащених навчальних лабораторіях з використанням обладнання, пристосованого до умов освітнього процесу (лабораторних макетів, установок тощо). Лабораторні заняття можуть проводитися також в умовах реального професійного середовища (на підприємстві, в наукових лабораторіях тощо). Лабораторні заняття забезпечуються відповідними методичними матеріалами.

Для проведення лабораторних занять академічна група поділяється на дві (іноді три) підгрупи. Такий поділ навчальних груп повинен бути зазначений у робочих навчальних планах. Теми лабораторних занять визначаються програмою навчальної дисципліни. Заміна лабораторних занять іншими видами навчальних занять, як правило, не дозволяється.

Лабораторне заняття включає проведення контролю підготовленості осіб, які навчаються, до виконання конкретної лабораторної роботи, виконання власне лабораторних досліджень, оформлення індивідуального письмового звіту про виконану роботу та його захист перед науково-педагогічним працівником. Виконання лабораторної роботи оцінюється науково-педагогічним працівником. Якщо це передбачено навчальною програмою дисципліни, лабораторні заняття можуть проводитися дистанційно віртуальні з використанням електронних засобів комунікації.

Науково-дослідне завдання. У них знання знаходять відображення в аналізах явищ, розрахунках, кресленнях, графіках, діаграмах, таблицях, ескізах, ілюстраціях тощо.

Самостійна робота є основним засобом засвоєння навчального матеріалу у вільний від аудиторних занять час. Самостійна робота включає: опрацювання навчального матеріалу, виконання індивідуальних завдань, науково-дослідну роботу. Навчальний час, відведений на самостійну роботу студента денної форми навчання, регламентується навчальним планом та робочим навчальним планом. Зміст самостійної роботи над конкретною дисципліною визначається програмою навчальної дисципліни, методичними

матеріалами, завданнями та вказівками науково-педагогічного працівника. Самостійна робота осіб, які навчаються, забезпечується системою навчально-методичного забезпечення, передбаченою програмою навчальної дисципліни: підручниками, навчальними та методичними посібниками, конспектами лекцій, збірниками завдань, комплектами індивідуальних семестрових завдань, практикумами, методичними рекомендаціями з організації самостійної роботи та виконання окремих завдань, електронними та іншими навчально-методичними матеріалами, дистанційними курсами. Методичні матеріали для самостійної роботи студентів повинні передбачати можливість проведення самоконтролю з боку студента. Для самостійної роботи рекомендується відповідна наукова та професійна монографічна і періодична література. Самостійна робота з вивчення навчального матеріалу з конкретної дисципліни може проходити в Центральній науковій бібліотеці університету, навчальних кабінетах, комп'ютерних класах, лабораторіях, у домашніх умовах, а також у дистанційній формі за використанням системи підтримки дистанційного навчання та матеріалів дистанційних курсів. Для забезпечення належних умов для самостійної роботи ця робота організовується, у разі необхідності, за попередньо складеним на факультеті графіком, що гарантує можливість індивідуального доступу особи, яка навчається, до необхідних дидактичних і технічних засобів загального користування. Графік оприлюднюється на початку навчального семестру. При організації самостійної роботи з використанням складного обладнання, установок, інформаційних систем (комп'ютерних баз даних, систем автоматизованого проектування, автоматизованих навчальних систем, системи підтримки дистанційного навчання тощо) забезпечується можливість одержання необхідної консультації або допомоги з боку спеціалістів кафедри. Контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу, є обов'язковим. Форми контролю визначаються програмою навчальної дисципліни і можуть включати виконання контрольних робіт, включених до навчального плану, курсових робіт, індивідуальних завдань, тестів, розрахунково-графічних робіт, рефератів, винесення самостійно засвоєного матеріалу на підсумковий семестровий контроль (разом з матеріалом, що вивчався при проведенні аудиторних навчальних занять) тощо.

9. Методи контролю

Вивчення дисципліни передбачає проведення поточного контролю в межах загального обсягу годин, а також проведення підсумкового семестрового контролю.

Поточний контроль.

Поточний контроль засвоювання теоретичного матеріалу під час проведення лекцій проводиться у формі усного опитування.

Для перевірки рівня підготовленості студента до виконання конкретної лабораторної роботи під час проведення практичних занять здійснюється поточний контроль, який проводиться у формі письмових контрольних робіт в межах загального обсягу годин. Для перевірки виконання лабораторної роботи проводиться поточний контроль, під час якого оцінюється оформлення індивідуального письмового звіту про виконану лабораторну роботу та його захист перед науково-педагогічним працівником. Лабораторні заняття можуть проводитися дистанційно з використанням електронних засобів комунікації.

Поточний контроль за темами, при вивченні яких не заплановано проведення лабораторних робіт, проводиться у формі письмових контрольних робіт в межах загального обсягу годин.

Поточний контроль засвоєння навчального матеріалу, віднесеного до самостійної роботи, проводиться у формі усного опитування.

Підсумковий семестровий контроль проводиться з метою оцінки результатів навчання за дисципліну. Він проводиться у формі семестрового екзамену. Семестрові екзамени та заліки проводяться в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни, і в терміни, встановлені навчальним планом. Семестрові екзамени проводяться в письмовій формі (припускається використання контролю з використанням комп′ютерів, інформаційно-комунікативних технологій). Екзамени складаються студентами в період екзаменаційних сесій, передбачених навчальним планом. Екзамени проводяться згідно з розкладом, який доводиться до відома викладачів і студентів не пізніше, як за місяць до початку сесії. Результати складання екзамену оцінюються за національною шкалою ("відмінно", "добре", "задовільно", "незадовільно"), кількістю балів 1 … 100 і вносяться в екзаменаційну відомість та залікову книжку студента.

Для оперативного контролю степені засвоєння матеріалу протягом семестру застосовуються наступні заходи:

– контроль присутності студентів (пропуск лекції без поважної причини – "мінус" один бал);

– контроль і оцінка виконання індивідуального завдання практичного заняття – перевірка роботи комп'ютерної програми (Mathcad-документу) та усна співбесіда;

– контроль знання відповідей на контрольні питання.

Під час проведення підсумкового семестрового контролю виконується перевірка якості конспекту лекцій та практичних занять.

10.Розподіл балів, які отримують студенти

Поточний контроль												Разом	Екзамен	Сума
КР1	ЛР1	КР2	ЛР2	КР3	ЛР3	КР4	ЛР4	КР5	ЛР5	КР6	КР7	60	40	100
5	5	5	5	5	5	5	5	5	5	5	5			

КР - поточний контроль у формі письмової контрольної роботи

ЛР - поточний контроль у формі захисту індивідуального письмового звіту про виконану лабораторну роботу

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену	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

11. Рекомендоване методичне забезпечення

1. Методичні вказівки до практичних робіт з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІТ.

2. Методичні вказівки до лабораторних робіт з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІТ.

3. Приклади реалізації алгоритмів стеганографічного перетворення на мові символьної математики MathCad. Електронний ресурс кафедри БІТ.

4. Плани проведення консультацій (друкований та електронній варіанти).

5. Навчальна програма з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІТ.

6. Завдання до контрольних робіт (3 роботи). Електронний ресурс кафедри БІТ.

7. Перелік питань до екзамену за дисципліною "Стеганографічні системи". Електронний ресурс кафедри БІТ.

8. Екзаменаційні білети за дисципліною "Стеганографічні системи". Електронний ресурс кафедри БІТ.

Базова література

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 878 с.

2. Есин В. И., Кузнєцов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

3. Кузнецов О.О. Семенов С.Г. Протоколи захисту інформації у комп'ютерних системах та мережах. Х.:ХНУРЕ, 2009р. – 184.

4. Грибунин В.Г., Оков И. Н., Туринцев И. В.. Цифровая стеганография. Серия: Аспекты защиты. – Солон-Пресс, 2002 г. – 272 с.

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

6. Simmons G.J. The prisoner`s problem and the subliminal channel, Proc. Workshop on Communications Security (Crypto`83), 1984, 51-67.

7. Pfitzmann B. Information Hiding Terminology, in Information Hiding, Springer Lecture Notes in Computer Science, v.1174, 1996, 347-350.

8. Aura T. Invisible communication. In Proc. of the HUT Seminar on Network Security '95, Espoo, Finland, November 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.

9. Ross J. Anderson. Stretching the limits of steganography. In IH96 [3], pages 39-48.

10. Zollner J., Federrath H.,Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, 344-354.

11. E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international

workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.

Допоміжна література

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.

2. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, vol. 31, no. 2, pp.26-34.

3. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM Systems Journal, 35(3 & 4):313{336, 1996.

4. Raymond B. Wolfgang and Edward J. Delp. A watermark for digital images. In International Conference on Images Processing, pages 219-222, Lausanne, Switzer-land, September 1996. IEEE.

5. Kahn D. The Codebreakers. N-Y, 1967.

6. Жельников В. Криптография от папируса до компьютера. М., 1996.

7. Радіотехніка. Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000 – 2015 рр.

8. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» 2006 – 2015 рр.

Інформаційні ресурси

1. www.nist.gov
2. www.eprint.iacr.org
3. www.citeseer.ist.psu.edu
4. www.springerlink.com
5. www.cacr.math.uwaterloo.ca
6. www.financialcryptography.com
7. www.austinlinks.com
8. www.world.std.com/~franl/crypto.html
9. www.cryptonessie.org
10. www.osti.gov/eprints