Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи технічного захисту інформації
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека»
(шифр і назва галузі знань)

Освітня програма: «Безпека інформаційних і комунікаційних систем»
(найменування освітньої програми)

Освітня програма «Кібербезпека»
(найменування освітньої програми)

Форма навчання: денна

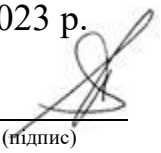
Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Перепелицин А. Є., доцент, к.т.н., доцент 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від « 30 » 08 2023 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 3</td><td>2023/ 2024</td></tr>
<tr><td>Індивідуальне завдання: РГР
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 64*/150</td><td>4</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="3">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 5.4</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td></td><td>Лабораторні *</td></tr>
<tr><td></td><td>32 годин</td></tr>
<tr><td></td><td>Самостійна робота</td></tr>
<tr><td></td><td>86 годин</td></tr>
<tr><td></td><td>Вид контролю</td></tr>
<tr><td></td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *64/86*.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета: діяльності на основі застосування системи теоретичних знань, практичних навичок обґрунтування, вибору та аналізу систем технічного захисту інформації.

Завдання: здійснювати порівняльний аналіз систем технічного захисту інформації та оцінку їх ефективності; здійснювати розрахунок та вибір конкретних датчиків та мереж охорони, обмеження доступу, сигналізації; використовувати сучасні мікропроцесори програмно-апаратні засоби для вирішення задач технічного захисту інформації.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

- КЗ1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ2. Знання та розуміння предметної області та розуміння професії.
- КЗ3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- КЗ5. Здатність до пошуку, оброблення та аналізу інформації.
- КФ3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
- КФ4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки
- КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання.

В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

- ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

- ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- ПРН4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
- ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
- ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
- ПРН36. Виявляти небезпечні сигнали технічних засобів.
- ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
- ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

Пререквізити - "Дискретна математика" (ОК2), "Теорія інформації та кодування" (ОК14), "Прикладна криптологія" (ОК16).

Кореквізити - "Апаратні та програмні засоби захисту інформації" (ОК11), "Комплексні системи захисту інформації: проектування, впровадження, супровід" (КП) (ОК28), "Дипломний проект (робота) бакалавра" (ОК33).

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Технічні засоби обмеження доступу до інформації.

Тема 1. Вступ. Призначення та законодавча база технічного захисту інформації Законодавча база ТЗІ. Способи знімання інформації. Засоби виявлення.

Тема 1. Системи охорони (далі – СО) об'єктів

Завдання і структура системи охорони об'єкта, сучасні вимоги, що пред'являються до СО. Класифікація та призначення інженерно-технічних засобів охорони. Принципи побудови комплексу інженерно-технічних засобів охорони системи охорони об'єкта.

Тема 1. Датчики та прилади систем зовнішнього виявлення.

Інфрачервоні та радіопроменеві бар'єри. Радіохвильовий лінійний сповіщувач. Камери спостереження. Системи пропуску.

Тема 1. Оптичні засоби зовнішнього спостереження

Лазерні системи. Засоби зовнішнього відеоспостереження. Види відеокамер.

Тема 1. Роботизовані камери відеоспостереження P, PT, PTZ камери. Електричні приводи камер. Інтерфейс и та протоколи управлення.

Тема 1. Системи сигналізації та контролю доступу.

Датчики та системи сигналізації. Склад і функції системи контролю та управління доступом (далі – СКУД). СКУД на базі контролерів та терміналів доступу.

Біометричні системи контроля доступу.

Змістовний модуль 2. Канали витоку та засоби перехоплення мовного сигналу.

Тема 2. Акустичні канали витоку інформації.

Акустичні канали. Вібраційні канали. Акустоелектричні канали.

Оптоелектронні канали. Параметричні канали.

Тема 2. Технічні засоби активного захисту мовної інформації в лініях зв'язку. Спектр мовного сигналу. Спектри шумів. Зашумлення мовного сигналу. Перетворення спектра мовного сигналу (скремблювання сигналів).

Тема 2. Закладні пристрої (далі – ЗП) перехоплення мовної інформації.

Класифікація закладних пристроїв: за методом перехоплення інформації, методу обробки і передачі інформації, каналу передачі, режиму роботи і активації, способу застосування, місця установки. Принципи побудови ЗП.

Тема 2. Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони). Структурна схема радіомікрофона (далі – РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц).

Тема 2. Застосування мобільних пристроїв для перехоплення інформації.

Склад мобільних пристроїв. Підслуховуючі пристрої з мобільним зв'язком. GSM підслуховуючий пристрій на основі мобільного телефона.

Змістовний модуль 3. Запобігання витоку інформації.

Тема 3. Захист від перехоплення інформації при передачі по телефонних каналах. Методи виявлення закладних пристроїв. Демаскуючі ознаки ЗП. Технічні засоби виявлення ЗП.

Тема 3. Виявлення нелінійних радіоелектронних елементів закладних пристроїв. Принципи виявлення напівпровідникових елементів. Нелінійні радіолокатори. Металошукачі.

Тема 3. Виявлення радіочастотного випромінення закладних пристроїв. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ.

Тема 3. Придушення радіоканалів витоку інформації.

Апаратура придушення радіоканалів. Генератори загороджувальних і прицільних перешкод. Засоби порушення роботи ЗП. Руйнування ЗП.

Тема 3. Паразитні електромагнітні випромінювання і наведення (далі – ПЕМВН).

Паразитні перетворення. Паразитні зв'язку. Ланцюги витоку інформації.

Тема 3. Засоби запобігання витоку інформації через ПЕМВН. Обмеження малих амплітуд. односпрямована передача сигналів. Засоби екранування електромагнітних полів.

Тема 3. Висновок. Перспективи розвитку СТЗІ.

Модульний контроль

4. Структура навчальної дисципліни

Назви модулів і тем	Кількість годин				
	усього	у тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. ***Технічні засоби обмеження доступу до інформації***					
Тема 1. Вступ. Призначення та законодавча база технічного захисту інформації Законодавча база ТЗІ. Способи знімання інформації. Засоби виявлення.	8	1	-	4	4
Тема 1. Системи охорони об'єктів Завдання і структура системи охорони об'єкта, сучасні вимоги, що пред'являються до СО. Класифікація та призначення інженерно-технічних засобів охорони. Принципи побудови комплексу інженерно-технічних засобів охорони системи охорони об'єкта	8	1	-	-	5
Тема 1. Датчики та прилади систем зовнішнього виявлення. Інфрачервоні та радіопроменеві бар'єри. Радіохвильовий лінійний сповіщувач. Камери спостереження. Системи пропуску	8	2	-	4	5
Тема 1. Оптичні засоби зовнішнього	8	2	-	-	4

спостереження Лазерні системи. Засоби зовнішнього відеоспостереження. Види відеокамер					
Тема 1. Роботизовані камери відеоспостереження P, PT, PTZ камери. Електричні приводи камер. Інтерфейс и та протоколи управлення	8	2	-	-	4
Тема 1. Системи сигналізації та контролю доступу. Датчики та системи сигналізації. Склад і функції системи контролю та управління доступом (СКУД). СКУД на базі контролерів та терміналів доступу. Біометричні системи контроля доступу. **Модульний контроль**	8	2	-	4	5
Разом за змістовним модулем 1	48	10	-	12	27
Змістовний модуль 2. Канали витоку та засоби перехоплення мовного сигналу					
Тема 2. Акустичні канали витоку інформації. Акустичні канали. Вібраційні канали. Акустоелектричні канали. Оптоелектронні канали. Параметричні канали	9	2	-	-	5
Тема 2. Технічні засоби активного захисту мовної інформації в лініях зв'язку. Спектр мовного сигналу. Спектри шумів. Зашумлення мовного сигналу. Перетворення спектра мовного сигналу (скремблювання сигналів)	10	2	-	4	6
Тема 2. Закладні пристрої перехоплення мовної інформації. Класифікація закладних пристроїв: за методом перехоплення інформації, методу обробки і передачі інформації, каналу передачі, режиму роботи і активації, способу застосування, місця установки. Принципи побудови ЗП	9	2	-	-	5
Тема 2. Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони). Структурна схема радіомікрофона (далі – РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц)	8	2	-	4	5
Тема 2. Застосування мобільних пристроїв для перехоплення інформації. Склад мобільних пристроїв. Підслуховуючі пристрої з мобільним зв'язком. GSM підслуховуючий пристрій на основі мобільного телефона **Модульний контроль**	8	2	-	-	5
Разом за змістовним модулем 2	44	10	-	8	26
Змістовний модуль 3. Запобігання витоку інформації					
Тема 3. Захист від перехоплення інформації при передачі по телефонних каналах. Методи виявлення закладних пристроїв. Демаскуючі ознаки ЗП. Технічні засоби виявлення ЗП	10	2	-	4	4

Тема 3. Виявлення нелінійних радіоелектронних елементів закладних пристроїв. Принципи виявлення напівпровідникових елементів. Нелінійні радіолокатори. Металошукачі	6	2	-	-	4
Тема 3. Виявлення радіочастотного випромінення закладних пристроїв. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ	10	2	-	4	4
Тема 3. Придушення радіоканалів витоку інформації. Апаратура придушення радіоканалів. Генератори загороджувальних і прицільних перешкод. Засоби порушення роботи ЗП. Руйнування ЗП	10	2	-	4	4
Тема 3. Паразитні електромагнітні випромінювання і наведення Паразитні перетворення. Паразитні зв'язку. Ланцюги витоку інформації	5	2	-	-	3
Тема 3. Засоби запобігання витоку інформації через ПЕМВН. Обмеження малих амплітуд. односпрямована передача сигналів. Засоби екранування електромагнітних полів	5	1	-	-	4
Тема 3. Висновок. Перспективи розвитку СТЗІ. **Модульний контроль**	4.5	1	-	-	3.5
РГР	7.5	-	-	-	6.5
Разом за змістовним модулем 3	**58**	**12**	**-**	**12**	**33**
Усього годин	**150**	**32**	**-**	**32**	**86**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		денна форма навчання
1	–	0
	Разом	0

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		денна форма навчання
1	РГР "Перетворення спектру мовного сигналу"	4
	Разом	**4**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	**Тема 1.** Вступ. Призначення та законодавча база технічного захисту інформації Законодавча база ТЗІ. Способи знімання інформації. Засоби виявлення	4
2	**Тема 1.** Датчики та прилади систем зовнішнього виявлення. Інфрачервоні та радіопроменеві бар'єри. Радіохвильовий лінійний сповіщувач. Камери спостереження. Системи пропуску	4
3	**Тема 1.** Системи сигналізації та контролю доступу. Датчики та системи сигналізації. Склад і функції системи контролю та управління доступом (СКУД). СКУД на базі контролерів та терміналів доступу. Біометричні системи контроля доступу. **Модульний контроль**	4
4	**Тема 2.** Технічні засоби активного захисту мовної інформації в лініях зв'язку. Спектр мовного сигналу. Спектри шумів. Зашумлення мовного сигналу. Перетворення спектра мовного сигналу (скремблювання сигналів)	4
5	**Тема 2.** Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони). Структурна схема радіомікрофона (далі – РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц)	4
6	**Тема 3.** Захист від перехоплення інформації при передачі по телефонних каналах. Методи виявлення закладних пристроїв. Демаскуючі ознаки ЗП. Технічні засоби виявлення ЗП	4
7	**Тема 3.** Виявлення радіочастотного випромінення закладних пристроїв. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ	4
8	**Тема 3.** Придушення радіоканалів витоку інформації. Апаратура придушення радіоканалів. Генератори загороджувальних і прицільних перешкод. Засоби порушення роботи ЗП. Руйнування ЗП	4
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	**Тема 1.** Вступ. Призначення та законодавча база технічного захисту інформації Законодавча база ТЗІ. Способи знімання інформації. Засоби виявлення.	2
2	**Тема 1.** Системи охорони об'єктів Завдання і структура системи охорони об'єкта, сучасні вимоги, що пред'являються до СО. Класифікація та призначення інженерно-технічних засобів охорони. Принципи побудови комплексу інженерно-технічних засобів охорони системи охорони об'єкта	2
3	**Тема 1.** Датчики та прилади систем зовнішнього виявлення. Інфрачервоні та радіопроменеві бар'єри. Радіохвильовий лінійний сповіщувач. Камери спостереження. Системи пропуску	2
4	**Тема 1**. Оптичні засоби зовнішнього спостереження Лазерні системи. Засоби зовнішнього відеоспостереження. Види відеокамер	2
5	**Тема 1.** Роботизовані камери відеоспостереження P, PT, PTZ камери. Електричні приводи камер. Інтерфейс и та протоколи управлення	2
6	**Тема 1.** Системи сигналізації та контролю доступу. Датчики та системи сигналізації. Склад і функції системи контролю та управління доступом (СКУД). СКУД на базі контролерів та терміналів доступу. Біометричні системи контроля доступу. **Модульний контроль**	2
7	**Тема 2.** Акустичні канали витоку інформації. Акустичні канали. Вібраційні канали. Акустоелектричні канали. Оптоелектронні канали. Параметричні канали	2
8	**Тема 2.** Технічні засоби активного захисту мовної інформації в лініях зв'язку. Спектр мовного сигналу. Спектри шумів. Зашумлення мовного сигналу. Перетворення спектра мовного сигналу (скремблювання сигналів)	2
9	**Тема 2.** Закладні пристрої перехоплення мовної інформації. Класифікація закладних пристроїв: за методом перехоплення інформації, методу обробки і передачі інформації, каналу передачі, режиму роботи і активації, способу застосування, місця установки. Принципи побудови ЗП	2
10	**Тема 2.** Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони). Структурна схема радіомікрофона (далі – РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц)	2
11	**Тема 2.** Застосування мобільних пристроїв для перехоплення інформації. Склад мобільних пристроїв. Підслуховуючі пристрої з мобільним	2

№ з/п	Назва теми	Кількість годин
	зв'язком. GSM підслуховуючий пристрій на основі мобільного телефона	
12	**Тема 3.** Захист від перехоплення інформації при передачі по телефонних каналах. Методи виявлення закладних пристроїв. Демаскуючі ознаки ЗП. Технічні засоби виявлення ЗП	4
13	**Тема 3.** Виявлення нелінійних радіоелектронних елементів закладних пристроїв. Принципи виявлення напівпровідникових елементів. Нелінійні радіолокатори. Металошукачі	4
14	**Тема 3.** Виявлення радіочастотного випромінення закладних пристроїв. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ	4
15	**Тема 3.** Придушення радіоканалів витоку інформації. Апаратура придушення радіоканалів. Генератори загороджувальних і прицільних перешкод. Засоби порушення роботи ЗП. Руйнування ЗП	4
16	**Тема 3.** Паразитні електромагнітні випромінювання і наведення Паразитні перетворення. Паразитні зв'язку. Ланцюги витоку інформації	3
17	**Тема 3.** Засоби запобігання витоку інформації через ПЕМВН. Обмеження малих амплітуд. односпрямована передача сигналів. Засоби екранування електромагнітних полів	4
18	**Тема 3.** Висновок. Перспективи розвитку СТЗІ	3.5
19	**Розрахункова робота**	6.5
	Разом	**55**

9. Індивідуальні завдання

Виконання Рахункової роботи (Перетворення спектру мовного сигналу. Створення фрагменту мовного сигналу та визначення його спектральних характеристик. Скремблювання фрагмента переставленням частин спектру за заданим варіантом. Відновлення скрембльованого фрагменту мовного сигналу за заданим варіантом).

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами (п.4, 8).

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді заліку.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист лабораторних (практичних) робіт	0...1	16	0...16
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Виконання і захист лабораторних (практичних) робіт	0...2	8	0... 16
Модульний контроль	0…18	1	0…18
Змістовний модуль 3			
Виконання і захист лабораторних (практичних) робіт	0...1	16	0...16
Модульний контроль	0…16	1	0…16
Усього за семестр			**0…100**

Семестровий контроль у вигляді заліку за наявності допуску до заліку. Під час складання семестрового заліку студент має можливість отримати максимум 100 балів.

Білет для заліку складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

– знати правові та нормативні основи побудови системи технічного захисту інформації в Україні;

– знати основи функціонування системи технічного захисту інформації, охоронних і пожежних сенсорних пристроїв;

– знати системи ідентифікації, основні типи пристроїв ідентифікації (в тому числі біометричні), а також пристрої систем відеоспостереження.

Необхідний обсяг вмінь для одержання позитивної оцінки:

– уміти використовувати нормативні документи, вітчизняних та міжнародних стандартів при удосконаленні СТЗІ;

– уміти проводити вибір та використання вимірювальних перетворювачів (сенсори) для СТЗІ;

– мати навички підключення вимірювальних перетворювачів в вимірювальну мережу.

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Захистити не менше 85% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування СТЗІ.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 95% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо розвитку та підтримки функціонування СТЗІ. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати інформаційне забезпечення СТЗІ.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Перепелицин А.Є. Лабораторні роботи (в електронному вигляді).
2. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https:// elearn.csn.khai.edu/xsl-portal/site/24650914-259c-4c0f-8198-5ac8f37d67db.
3. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1633.

14. Рекомендована література

1. Закон України «Про державну таємницю» від 21 січня 1994, Документ 3855-XII, чинний, поточна редакція — Редакція від 05.08.2018, підстава - 2509-VIII, https://zakon.rada.gov.ua/laws/show/3855-12.
2. Закон України «Про інформацію», від 02.10.92, 1992, Документ 2657-XII, чинний, поточна редакція — Редакція від 16.07.2019, підстава - 2704-VIII, https://zakon.rada.gov.ua/laws/main/2657-12.
3. Закон України «Про науково-технічну інформацію» від 25.06.1993, Документ 3322-XII, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/3322-12.

4. Закон України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах"», Документ 2594-IV, чинний, поточна редакція – Прийняття від 31.05.2005, https://zakon.rada.gov.ua/laws/main/2594-15.

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», 1994, Документ 80/94-ВР, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80.

5. Закон України «Про Національну систему конфіденційного зв'язку», 2002, Документ 2919-III, чинний, поточна редакція — Редакція від 19.04.2014, https://zakon.rada.gov.ua/laws/main/2919-14.

6. Закон України «Про національну безпеку України» Документ 2469- VIII, чинний, поточна редакція – Прийняття від 21.06.2018, https://zakon.rada.gov.ua/laws/main/2469-19.

7. Закон України «Про основні засади забезпечення кібербезпеки України», 2017, Документ 2163-VIII, чинний, поточна редакція — Редакція від 08.07.2018, https://zakon.rada.gov.ua/laws/main/2163-19.

8. Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» від 10.04.2000, Документ 582/2000, поточна редакція — Прийняття від 10.04.2000, https://zakon.rada.gov.ua/laws/show/582/2000.

9. Указ президента україни «Про Положення про технічний захист інформації в Україні», Документ 1229/99, поточна редакція — Редакція від 04.05.2008, https://zakon.rada.gov.ua/laws/show/1229/99.

10. Постанова Кабінету Міністрів України від 8 жовтня 1997 р. N 1126 «Про затвердження Концепції технічного захисту інформації в Україні». Документ 1126-97-п, поточна редакція — Редакція від 13.10.2011, підстава - 938-2011-п. https://zakon.rada.gov.ua/laws/main/1126-97-%D0%BF.

11. Ловейкін В.С., Ромасевич Ю.О., Човнюк Ю.В. Мехатроніка. Навчальний посібник. – К., 2012. - 357 с.

12. Датчики: Довідковий посібник / За заг. ред. В.М. Шарапова, Є.С. Поліщука Москва: Техносфера, 2012. – 624 с.

13. Барило Г.І., Вісьтак М.В., Готра З.Ю., Лесінський В.В., Політанський Л.Ф. Електронні елементи та пристрої систем безпеки й охорони: Навчальний посібник .- За ред. Готри З.Ю. – Чернівці: Рута, 2017. – 216 с. ISBN 978-966-423-419-8.

14. ГСТУ 78.11.001-98 «Укріпленість об’єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони».

15. Технічні канали витоку інформації. Порядок створення комплексів ехнічного захисту інформації. Навчальний посібник /Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ "КПІ", 2016. - 104 с.

16. Комплексні системи захисту інформації [Текст]: навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.]; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018. - 118 с. - Бібліогр.: с. 116-117.

17. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України/ Рибальський О.В., Хахановський В.Г., Кудінов В.А. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

18. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

19.- ДСТУ 3396.0-96 ТЗІ. Основні положення.

20.- ДСТУ 3396.1-96 ТЗІ. Порядок проведення робіт.

21. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Загальні положення. (НД ТЗІ 1.1-002-99).

22. Методи та засоби вимірювань: підручник / Раннев Г.Г. та інші. - 4-те видання. М: Вид.центр «Академія», 2008.

23. Підручник / Є.С. Поліщук, М.М. Дорожовець, В.О. Яцук, В.М. Ванько, Т.Г. Бойко. Друге видання, доповнене та перероблене. Львів: Видавництво Львівської політехніки, 2012, - 544 с.

24. Електронні методи і засоби біомедичних вимірювань: навчальний посібник /С.К. Мещанінов, В.М. Співак, А.Т. Орлов . – К.; Кафедра, 2015. – 211 с.: іл..ISBN 966-8934-17-2.

25. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

26. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. Захист інформації в телекомунікаційних системах: Навчальний посібник.(лист МОНУ №1.4/18 – Г – 183 від 02.06.2009р.). – К.: НАУ,2009. – 380с.

27. Мішин Є.Т., Соколов Є.Є. Побудова систем фізичного захисту потенційно небезпечних об'єктів. М.: "Радіо і зв'язок", 2005 - с.200, іл. 44.

ISBN 5-94101-122-9.

28. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

29. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. - 608 с. ISBN 966-522-167-5.

15. Інформаційні ресурси

1. eLearning Portal – [Ел. ресурс]. – Режим доступу: https://elearn.csn.khai.edu