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

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

“**ЗАТВЕРДЖУЮ**”

Голова НМК
_____ М.С. Зряхов
(підпис) (ініціали та прізвище)

« 30 » _____08___2019 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»

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2019 рік

Робоча програма «Системи технічного захисту інформації»
(назва навчальної дисципліни)
для студентів за спеціальністю: 125 «Кібербезпека»

Освітня програма: «Безпека інформаційних і комунікаційних систем»

«_26_» ___08___ 2019 року - 12 с.

Розробники: Плахтєєв Анатолій Павлович, доцент кафедри 503 к.т.н, доц. _____
(автор, посада, науковий ступень та вчене звання) (підпис)
Розробники: Землянко Георгій Андрійович, аспирант 503 _____
(автор, посада, науковий ступень та вчене звання) (підпис)

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

Протокол № 1 від «30» 08 2018 року

Завідувач кафедри д.т.н, професор _____ В.С.Харченко
(науковий ступень 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 – 4</td><td rowspan="12">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>Цикл загальної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2019/2020</td></tr>
<tr><td>Індивідуальне завдання: -</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 65/120</td><td>4-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="9">Кількість тижневих годин для денної форми навчання: аудиторних – 4, самостійної роботи студента – 3,5</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>1 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>55 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 65/55.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: є отримання студентами необхідних знань та навиків для застосування їх з питань з використанням інформації і захистом останньої від неправомірного використання. А також в подальшому використанню отриманих знань стосовно розробки методів і засобів систем захисту інформації (далі-ТЗІ) та при проектуванні систем технічного захисту інформації (далі-СТЗІ). Особлива увага в курсі приділяється вивченню законів, нормативних документів ТЗІ, вітчизняних та міжнародних стандартів в галузі захисту та безпеки інформації, фізичних основ каналів витоку інформації, їх виявлення та протидії, а також побудови засобів протидії несанкціонованому доступу до інформації.

Завдання:

- навчити студентів використанню нормативних документів ТЗІ, вітчизняних та міжнародних стандартів при розробці СТЗІ;
- надати студентам знання з принципів побудови засобів СТЗІ.
- надати студентам знання з оцінки якості засобів СТЗІ;
- ознайомити студентів з базовими міжнародними стандартами в галузі забезпечення інформаційної безпеки.

Міждисциплінарні зв'язки: дисципліна базується на деяких поняттях дисциплін «Операційні системи», «Теорія інформації та кодування», «Фізика». Дисципліна є базовою для окремих тем дисципліни «Комплексні системи захисту інформації: проектування впровадження, супровід».

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 2. Системи охорони (СО) об'єктів

Завдання і структура системи охорони (СО) 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 3. Датчики та прилади систем зовнішнього виявлення

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

ТЕМА 4. Оптичні засоби зовнішнього спостереження, роботизовані камери відеоспостереження

Лазерні системи. Засоби зовнішнього відеоспостереження. Види відеокамер. Р,

PT, PTZ камери. Електричні приводи камер. Інтерфейс и та протоколи управлення.

ТЕМА 5. 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.

Модуль 2

Змістовний модуль 2. Канали витоку та засоби перехоплення мовного сигналу

ТЕМА 6. Акустичні канали витоку інформації.

Акустичні канали. Вібраційні канали. Акустоелектричні канали. Оптоелектронні канали. Параметричні канали.

ТЕМА 7. 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 8. Закладні пристрої (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 9. Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони).

Структурна схема радіомікрофона (РМ). Схемотехнічна реалізація аналогових РМ (100-108 МГц, 433 МГц) і цифрових РМ (2.4 ГГц)

ТЕМА 10. 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 11. Захист від перехоплення інформації при передачі по телефонних каналах.

Методи виявлення закладних пристроїв. Демаскуючі ознаки ЗП. Технічні засоби виявлення ЗП.

ТЕМА 12. Виявлення нелінійних радіоелектронних елементів закладних пристроїв. Виявлення радіочастотного випромінення закладних пристроїв.

Принципи виявлення напівпровідникових елементів. Нелінійні радіолокатори.

Металошукачі. Класифікація засобів виявлення випромінювань закладних пристроїв. Апаратура радіоконтролю. Детектори ЗУ.

ТЕМА 13. Придушення радіоканалів витоку інформації.

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

ТЕМА 14. Паразитні електромагнітні випромінювання і наведення (ПЕМВН)

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

ТЕМА 15. Засоби запобігання витоку інформації через ПЕМВН.

Обмеження малих амплітуд. односпрямована передача сигналів. Засоби екранування електромагнітних полів.

ТЕМА 16. Висновок. Перспективи розвитку СТЗІ.

Модульний контроль.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. *Технічні засоби обмеження доступу до інформації*					
Тема 1. Вступ. Призначення та законодавча база технічного захисту інформації	**7**	**2**		**4**	**1**
ТЕМА 2. Системи охорони (СО) об'єктів	**3**	**2**			**1**
ТЕМА 3. Датчики та прилади систем зовнішнього виявлення	**8**	**2**		**4**	**2**
ТЕМА 4. Оптичні засоби зовнішнього спостереження, роботизовані камери відеоспостереження	**4**	**2**			**2**
ТЕМА 5. Системи сигналізації та контролю Доступу	**7**	**1**		**4**	**2**
Модульний контроль	**3**	**1**	**-**	**-**	**2**
Разом за змістовим модулем 1	**32**	**10**		**12**	**10**
Разом за модулем 1	**32**	**10**		**12**	**10**
Модуль 2					
Змістовий модуль 2. *Канали витоку та засоби перехоплення мовного сигналу*					
ТЕМА 6. Акустичні канали витоку інформації.	**4**	**2**			**2**
Тема 7. Технічні засоби активного захисту	**9**	**2**		**5**	**2**

1	2	3	4	5	6
мовної інформації в лініях зв'язку.					
Тема 8. Закладні пристрої (ЗП) перехоплення мовної інформації.	**5**	**2**			**3**
Тема 9. Радіочастотні ЗП перехоплення мовної інформації (радіомікрофони).	**11**	**2**		**5**	**4**
Тема 10. Застосування мобільних пристроїв для перехоплення інформації.	**6**	**2**			**4**
Разом за змістовим модулем 2	**35**	**10**		**10**	**15**
Змістовий модуль 3. *Запобігання витоку інформації*					
Тема 11. Захист від перехоплення інформації при передачі по телефонних каналах.	**5**	**2**			**3**
Тема 12. Виявлення нелінійних радіоелектронних елементів закладних пристроїв. Виявлення радіочастотного випромінення закладних пристроїв.	**12**	**2**		**5**	**5,5**
Тема 13. Придушення радіоканалів витоку інформації.	**12**	**2**		**5**	**5**
Тема 14. Паразитні електромагнітні випромінювання і наведення (ПЕМВН)	**5**	**2**			**3**
Тема 15. Засоби запобігання витоку інформації через ПЕМВН.	**5**	**2**			**3**
Тема 16. Висновок. Перспективи розвитку СТЗІ.	**4**	**1**			**3**
РГР	**6,5**		**1**		**5,5**
Модульний контроль	**3**	**1**	**-**	**-**	**2**
Разом за змістовим модулем 3	**53**	**12**	**1**	**10**	**30**
Разом за модулем 2	**88**	**22**	**1**	**20**	**45**
Усього годин	**120**	**32**	**1**	**32**	**55**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	РГР	1
	Разом	1

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
1	Канали витоку інформації	4
2	Засоби охорони периметра. інфрачервоні бар'єри	4
3	Датчики систем сигналізації	5
4	Електронні замки систем контролю і управління доступом	5
5	Перетворення мовного сигналу	5
6	Генератори шуму	5
7	Засоби виявлення закладних пристроїв	4
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Законодавча база технічного захисту інформації	**2**
2	Структура системи охорони (СО) об'єктів	**2**
3	Серійні радіочастотні датчики та прилади систем зовнішнього виявлення.	**2**
4	Лазерні засоби зовнішнього спостереження	**2**
5	Роботизовані камери відеоспостереження. Протокол Pelco.	**2**
6	Шлейфи систем сигналізації. Серійні засоби контролю доступу.	**2**
7	Акустичні канали витоку інформації.	**2**
8	Технічні засоби активного захисту мовної інформації в лініях зв'язку.	**4**
9	Закладні пристрої (ЗП) перехоплення мовної інформації.	**4**
10	Схемна реалізація радіочастотних ЗП перехоплення мовної інформації (радіомікрофони).	**2**
11	Застосування мобільних пристроїв для перехоплення інформації.	**2,5**
12	Захист від перехоплення інформації при передачі по телефонних каналах.	**3**
13	Апаратура виявлення нелінійних радіоелектронних елементів закладних пристроїв.	**4**
14	Апаратура виявлення радіочастотного випромінення закладних пристроїв.	**3**
15	Апаратура придушення радіоканалів витоку інформації.	**3**
16	Паразитні електромагнітні випромінювання і наведення (ПЕМВН)	**3**
17	Екранування для запобігання витоку інформації через	**3**

	ПЕМВН.	
18	Перспективи розвитку СТЗІ.	**3**
19	РГР	**6,5**
	Разом	**55**

9. Індивідуальні завдання

Розрахункова робота. *Перетворення спектру мовного сигналу*.

Створення фрагменту мовного сигналу та визначення його спектральних характеристик. Скремблювання фрагмента перестановкою частин спектру за заданим варіантом. Відновлення скрембльованого фрагменту мовного сигналу за заданим варіантом.

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді екзамену.

12. 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
Модуль 1			
Змістовий модуль 1			
Лекції	0…1	5	0…5
Лабораторні роботи	0...5	3	0…15
Модульний контроль	0…20	1	0..20
Модуль 2			
Змістовий модуль 2			
Лекції	0…1	5	0…5
Лабораторні роботи	0…5	2	0…10
Змістовий модуль 3			
Лекції	0…1	6	0…6
Лабораторні роботи	0…5	2	0…10
Модульний контроль	0…20	1	0…20
РГР	0…9	1	0…9
Усього за семестр			**0…100**

12.3. Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань

лабораторних занять.

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

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

14. Рекомендована література

1. Конституція України. https://zakon.rada.gov.ua/laws/show/254/96-вр.
2. Цивільний кодекс України. https://zakon.rada.gov.ua/laws/show/435-15.
3. Технічний захист інформації. URL: http://www.znanius.com/3853.html (станом на 26.08.2018р)
4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
5. Титов А.А. Технические средства защиты информации: Учебное пособие для студентов специальностей ≪Организация и технология защиты информации≪ и ≪Комплексная защита объектов информатизации≪. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 194 с.
5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

1. Закон України

1. Закон України «Про державну таємницю». https://zakon.rada.gov.ua/laws /show/3855-12
2. Закон України «Про захист інформації в автоматизованих системах». https://zakon.rada.gov.ua/laws/show/2594-15.
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». https://zakon.rada.gov.ua/laws/show/3475-15.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». https://zakon.rada.gov.ua/laws/show/80/94-вр.

2. Укази Президента України.

1. № 891 від 24.09.2001 року «Про деякі заходи щодо захисту державних ін формаційних ресурсів у мережах передачі даних».
2. №582 від 10.04 2000 року «Про заходи щодо захисту інформаційних ресурсів держави».
3. № 1229 від 27.09.1999 року «Про Положення про технічний захист ін формації в Україні».

3. Постанови КМУ

1. Постанова КМ від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

6. КМ України Постанова КМ, від 16.11.2002 р. N 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах».

7. КМ України Постанова КМ, від 04.02. 1998, N 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних».

8. КМ України Постанова КМ, від 08.10.1997, № 1126 «Про затвердження Концепції технічного захисту інформації в Україні».

9. КМ України Постанова КМ, від 16.02.1997, №180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

4. Нормативні документи.

1. НД ТЗІ 2.7-008-08 «Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки».

2. НД ТЗІ 2.3-017-08 «Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами».

3. НД ТЗІ 2.2-006-08 «Захист інформації на об'єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку мовної інформації».

4. НД ТЗІ 2.2-003-06 «Протидія технічним розвідкам. Норми з протидії засобам радіолокаційної розвідки».

5. НД ТЗІ 2.3-010-06 «Протидія технічним розвідкам. Методика контролю ефективності протидії засобам радіолокаційної розвідки».

6. НД ТЗІ 2.4-003-06 «Протидія технічним розвідкам. Рекомендації щодо протидії засобам радіолокаційної розвідки».

7. НД ТЗІ 2.3-011-06 «Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок».

8. НД ТЗІ 2.4-004-06 «Протидія технічним розвідкам. Рекомендації з протидії засобам фотографічної та оптико-електронної розвідок».

10. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

11. НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2"

12. НД ТЗІ 4.7-002-01 "Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні вказівки».

13. НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу».

15. НД ТЗІ Р-001-2000 «Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та

загальні технічні вимоги. Рекомендації».

16. НД ТЗІ 1.5-001-2000 «Радіовиявлювачі. Класифікація. Загальні технічні вимоги».

17. НД ТЗІ 1.1-001–99 «Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення».

18. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

19. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

20. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

21. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

5. Стандарти

1. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96

2. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

3. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97

4. ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96

15. Інформаційні ресурси

1. Офіційний портал Верховної Ради України [Электрон. ресурс]. – Режим доступа: http://www.rada.gov.ua

2. Законодавство України [Электрон. ресурс]. – Режим доступа: http://zakon3.rada.gov.ua/laws

6. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. – Режим доступа: http://dstszi.kmu.gov.ua/dstszi/control/uk/index