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

_____ Д.М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2022р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи технічного захисту інформації
(назва навчальної дисципліни)

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

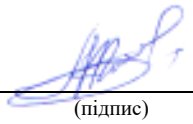
Спеціальність: 125 «Кібербезпека»
(шифр і назва галузі знань)

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

Форма навчання: денна

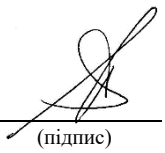
Рівень вищої освіти: перший (бакалаврський)

Харків 2022 рік

Розробник: Піскачов О.І., доцент, к.т.н., снс 
(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 2022 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 – 4</td><td rowspan="15">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
125 «Кібербезпека»
(код та найменування)

Освітня програма
«Безпека інформаційних і комунікаційних систем»,
(найменування)

«Кібербезпека індустріальних 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 – 2</td><td>2022/ 2023</td></tr>
<tr><td>Індивідуальне завдання: РГР
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 48*/120</td><td>3</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="4">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 4</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Лабораторні *</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *48/72*.

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

2. Мета та завдання навчальної дисципліни

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

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.

Компетентності, які набуваються:

- КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2. Знання та розуміння предметної області та розуміння професії.
- КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
- КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
- КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- 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.).
- КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- 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.

Очікувані результати навчання:

- ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
- ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

- ПРН 4 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.
- ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
- ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
- ПРН 17 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.
- ПРН 36 Виявляти небезпечні сигнали технічних засобів.
- ПРН 37 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.
- ПРН 38 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
- ПРН 40 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

Пререквізити – “Фізика”, “Теорія ймовірностей та математична статистика”, “Дискретна математика”, “Теорія інформації та кодування”, “Прикладна криптологія”.

Кореквізити – “Апаратні та програмні засоби захисту інформації”, “Комплексні системи захисту інформації: проектування, впровадження, супровід” (КП), “Дипломний проект (робота) бакалавра”.

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1.

Тема 1. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Напрямки захисту інформації (далі - ЗІ) в системі технічного захисту інформації (далі - СТЗІ). Технічний захист інформації (далі - ТЗІ) від несанкціонованих дій (далі - НСД) на прикладному і програмному рівні. ТЗІ від

НСД на аппаратному рівні. ТЗІ на мережевому рівні. Засоби та заходи ТЗІ. Криптографічний захист інформації. Організаційні заходи ЗІ. Нормативно-методичне забезпечення СТЗІ.

Тема 2. Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації. Концепція технічного захисту інформації в Україні. Основи побудови та функціонування систем технічного захисту інформації. Концепція технічного захисту інформації в Україні.

Тема 3. Методи вимірювань (безпосередньої оцінки, порівняння з мірою, протиставлення, диференціальний, нульовий, заміщення збіги). Види вимірювань (прямі і непрямі, сукупні і спільні, абсолютні і відносні, одноразові і багаторазові, технічні та метрологічні, равноточні і неравноточні равнорассеяні і неравнорассеяні, статичні і динамічні). Характеристики сенсорів (вимірювальних перетворювачів).

Тема 4. Технічні канали витоку інформації. Основні об'єкти захисту інформації. Загальні відомості про технічні канали витоку інформації. Структура, класифікація та основні характеристики. Технічні канали витоку інформації при передачі її по каналах зв'язку. Технічні канали витоку мовної інформації.

Тема 5. Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах. Ємнісні перетворювачі. Структура, класифікація та основні характеристики. Пристрій, принцип дії індуктивних перетворювачів. Пристрій, принцип дії індукційних перетворювачів.

Тема 6. Пристрій і принцип дії диференціального індуктивного перетворювача (сенсора). Пристрій і принцип дії індукційного перетворювача.

Тема 7. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані сенсори руху. Принципи дії інфрачервоного, ультразвукового, мікрохвильового сенсорів руху. Основні недоліки ультразвукових, інфрачервоних сенсорів руху. Переваги інфрачервоних, ультразвукових, мікрохвильових, комбінованих сенсорів руху. Ультразвуковий сенсор відстані.

Тема 8. Пристрій, принципи дій тензорезисторів. Пристрій, принципи дій магнитоупругих перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів.

Модульний контроль

Змістовний модуль 2.

Тема 9. Температура. Вимірювання і контроль температури. Методи і засоби вимірювання температури. Загальні відомості про вимірювання і контроль температури.

Тема 10. Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори).

Тема 11. Інтелектуальні сенсори. Структура інтелектуальних сенсорів. Функції, що реалізуються у інтелектуальних сенсорах (перетворення, самодіагностики, інформаційні, конфігурації, форматування, що керують).

Тема 12. Сполучення перетворювачів з вимірювальної апаратурою.

Тема 13. Аналогові та цифрові системи перетворення.
Тема 14. Технічні засоби охоронних систем. Технічні засоби охоронної сигналізації. Електроконтактні, магнітоконтактні та удароконтактні засоби виявлення порушень. Пасивні й активні інфрачервоні сенсорні пристрої. Радіохвильові сенсорні пристрої. Сенсорні пристрої реєстрації механічного впливу.
Тема 15. Сенсорні пристрої та пристрої протипожежних систем. Характеристики пожежі та способи її виявлення. Класифікація та принципи функціонування пожежних сенсорних пристроїв. Теплові сенсорні пристрої. Оптичні сенсорні пристрої диму. Сенсорні пристрої відкритого полум'я**.** Ручні пожежні сповіщувачі.
Тема 16. Системи ідентифікації. Основні типи пристроїв ідентифікації. Біометричні пристрої ідентифікації. Пристрої систем відеоспостереження.
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.					
Тема 1. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення	6	2	-	-	4
Тема 2. Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації	12	2	4	-	6
Тема 3. Методи вимірювань	10	2	2	-	6
Тема 4. Технічні канали витоку інформації	6	2	-	-	4
Тема 5. Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах	6	2	-	-	4
Тема 6. Пристрій і принцип дії диференціального індуктивного перетворювача (сенсора). Пристрій і принцип дії індукційного перетворювача	6	2	-	-	4
Тема 7. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку.	12	2	4	-	6

Ультразвукові, мікрохвильові, інфрачервоні, комбіновані сенсори руху					
Тема 8. Пристрій, принципи дій тензорезисторів. Пристрій, принципи дій магнитоупругих перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів **Модульний контроль**	8	2	-	-	6
Разом за змістовним модулем 1	**66**	**16**	**10**	**-**	**40**
Змістовний модуль 2					
Тема 9. Температура. Вимірювання і контроль температури об'єктів	8	2	2	-	4
Тема 10. Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	8	2	2	-	4
Тема 11. Інтелектуальні сенсори	6	2	-	-	4
Тема 12. Сполучення перетворювачів з вимірювальної апаратурою	6	2	-	-	4
Тема 13. Аналогові та цифрові системи перетворення	6	2	-	-	4
Тема 14. Технічні засоби охоронних систем.	5	2	-	-	3
Тема 15. Сенсорні пристрої та пристрої протипожежних систем	8	2	2	-	4
Тема 16. Системи ідентифікації. Основні типи пристроїв ідентифікації. Біометричні пристрої ідентифікації. Пристрої систем відеоспостереження **Модульний контроль**	7	2	-	-	5
Разом за змістовним модулем 2	**54**	**16**	**6**	**-**	**32**
Усього годин	**120**	**32**	**16**	**-**	**72**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	**Тема 2.** Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації	4
	Разом	4

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	**Тема 3.** Методи вимірювань	2
2	**Тема** 7. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані сенсори руху	4
3	**Тема 9**. Температура. Вимірювання і контроль температури об'єктів	2
4	**Тема 10**. Пристрої, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	2
5	**Тема 15.** Сенсорні пристрої та пристрої протипожежних систем	2
	Разом	**12**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1		
	Разом	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	**Тема 1**. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення	4
2	**Тема 2.** Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації	6
3	**Тема 3.** Методи вимірювань	6
4	**Тема 4**. Технічні канали витоку інформації	4
5	**Тема 5.** Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах	4
6	**Тема 6**. Пристрій і принцип дії диференціального індуктивного перетворювача (сенсора). Пристрій і принцип дії індукційного перетворювача	4
7	**Тема 7**. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані сенсори руху	6
8	**Тема 8.** Пристрій, принципи дій тензорезисторів.	4

№ з/п	Назва теми	Кількість годин
	Пристрій, принципи дій магнитоупругих перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів	
9	**Тема 9**. Температура. Вимірювання і контроль температури об'єктів	4
10	**Тема 10**. Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	4
11	**Тема 11.** Інтелектуальні сенсори	4
12	**Тема 12.** Сполучення перетворювачів з вимірювальної апаратурою	4
13	**Тема 13**. Аналогові та цифрові системи перетворення	4
14	**Тема 14**. Технічні засоби охоронних систем	3
15	**Тема 15.** Сенсорні пристрої та пристрої протипожежних систем	4
16	**Тема 16.** Системи ідентифікації. Основні типи пристроїв ідентифікації. Біометричні пристрої ідентифікації. Пристрої систем відеоспостереження	5
	Разом	**72**

9. Індивідуальні завдання

Виконання РГР (Обробка прямих багаторазових вимірювань)

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

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних (практичних) робіт	0...4	4	0...16
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних (практичних) робіт	0...4	4	0... 16
Модульний контроль	0…18	1	0…18
Усього за семестр			**60…100**

Контроль знань при проведенні занять оцінюється за такими шкалами: активність на лекції під час відповідей на питання:

- повна відповідь на питання - 2 бали;
- неповна відповідь - 1 бал;
- відсутність на лекції - 0 балів,

<u>виконання і захист практичних робіт:</u>

при виконанні всіх вимог завдань методик на роботи - 4 бали;
- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1балл;
- якщо робота не виконана і не захищена - 0 балів.

<u>На модульний контроль</u> (всього 18 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 3 питання (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 6.

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.

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. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.

2. Дистанційний курс в системі дистанційного навчання Ментор, розташований за адресою: https://mentor.khai.edu/course/view.php?id=4835.

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: Справочное пособие / Под общ. ред. В.М. Шарапова, Е.С. Полищука 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. с. 104.
18. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. с. 608.
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. с. 544.
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. 380 с.
27. 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.
28. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. - 608 с. ISBN 966-522-167-5.