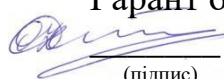


Міністерство освіти і науки України  
Національний аерокосмічний університет ім. М. Є. Жуковського  
«Харківський авіаційний інститут»

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

**ЗАТВЕРДЖУЮ**

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

" 31" 08 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: Піскачов О.І., доцент, к.т.н., снс

(прізвище та ініціали, посада, науковий ступінь та вчене звання)



(підпис)

Робочу програму розглянуто на засіданні кафедри \_\_\_\_\_

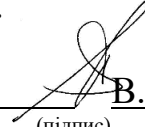
«Комп'ютерних систем, мереж і кібербезпеки»

(назва кафедри)

Протокол № 1 від «31» 08 2023 р.

Завідувач кафедри д.т.н., професор

(науковий ступінь та вчене звання)



В. С. Харченко

(підпис)

(ініціали та прізвище)

## 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни (денна форма навчання)
Кількість кредитів – 4	<p><b>Галузь знань</b> <u>12 «Інформаційні технології»</u> (шифр та найменування)</p> <p><b>Спеціальність</b> <u>125 «Кібербезпека»</u> (код та найменування)</p> <p><b>Освітня програма</b> <u>«Безпека інформаційних і комунікаційних систем»<sub>2</sub></u> (найменування)</p> <p><u>«Кібербезпека індустриальних систем»</u> (найменування)</p> <p><b>Рівень вищої освіти:</b> перший (бакалаврський)</p>	Обов'язкова
Кількість модулів – 1		<b>Навчальний рік</b>
Кількість змістових модулів – 2		2023/ 2024
<u>Індивідуальне завдання: РР</u> (назва)		<b>Семестр</b>
Загальна кількість годин – 48*/120		<b>3</b>
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи студента – 4.5		<b>Лекції*</b>
		<u>32</u> годин
		<b>Практичні, семінарські*</b>
		<u>16</u> годин
		<b>Лабораторні *</b>
	<u>0</u> годин	
	<b>Самостійна робота</b>	
<u>72</u> годин		
<b>Вид контролю</b>		
Модульний контроль, залік		

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

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

## **2. Мета та завдання навчальної дисципліни**

**Мета:** навчити діяльності на основі застосування системи теоретичних знань, отримати практичні навички обґрунтування, вибору та аналізу систем технічного захисту інформації.

### **Компетентності, які набуваються.**

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості 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. Організувати 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 8. Готувати пропозиції до нормативних актів щодо забезпечення 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 заводових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами 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”.

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

### **3. Програма навчальної дисципліни**

#### **Модуль 1.**

##### **Змістовий 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 на прикладному і програмному рівні. ТЗІ від несанкціонованих дій на апаратному рівні. ТЗІ на мережевому рівні. Засоби та заходи ТЗІ. 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, рівноточні і нерівноточні

равно розсіяні і не равно розсіяні, статичні і динамічні). Характеристики датчиків (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 датчики руху. Принципи дії інфрачервоного, ультразвукового, мікрохвильового датчиків руху. Основні недоліки ультразвукових, інфрачервоних датчиків руху. Переваги інфрачервоних, ультразвукових, мікрохвильових, комбінованих датчиків руху. Ультразвуковий датчик відстані.

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

## **Модульний контроль**

### **Змістовий 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 датчики. Структура інтелектуальних датчиків. Функції, що реалізуються у інтелектуальних датчиках (перетворення, самодіагностики, інформаційні, конфігурації, форматування, що керують).

**Тема 12.** Сполучення перетворювачів з вимірювальною 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 датчики. Радіохвильові датчики. Датчики реєстрації механічного впливу.

**Тема 15.** Датчики та пристрої протипожежних систем. Характеристики пожежі та способи її виявлення. Класифікація та принципи функціонування пожежних сенсорних пристроїв. Теплові сенсорні пристрої. Оптичні датчики диму. Датчики та пристрої визначення 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
<b>Модуль 1</b>					
<b>Змістовий модуль 1.</b>					
<b>Тема 1.</b> Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення	6	2	-	-	4
<b>Тема 2.</b> Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації	12	2	4	-	6
<b>Тема 3.</b> Методи вимірювань	10	2	2	-	6
<b>Тема 4.</b> Технічні канали витоку інформації	6	2	-	-	4
<b>Тема 5.</b> Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах	6	2	-	-	4
<b>Тема 6.</b> Пристрій і принцип дії диференціального індуктивного перетворювача (датчика). Пристрій і принцип дії індукційного перетворювача	6	2	-	-	4
<b>Тема 7.</b> Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані датчики руху	12	2	4	-	6
<b>Тема 8.</b> Пристрій, принципи дій тензорезисторів. Пристрій, принципи дій магнітоупругих перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів	8	2	-	-	6
<b>Модульний контроль</b>					
<b>Разом за змістовим модулем 1</b>	<b>66</b>	<b>16</b>	<b>10</b>	<b>-</b>	<b>40</b>

<b>Змістовий модуль 2</b>					
<b>Тема 9.</b> Температура. Вимірювання і контроль температури об'єктів	8	2	2	-	4
<b>Тема 10.</b> Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	8	2	2	-	4
<b>Тема 11.</b> Інтелектуальні датчики	6	2	-	-	4
<b>Тема 12.</b> Сполучення перетворювачів з вимірювальною апаратурою	6	2	-	-	4
<b>Тема 13.</b> Аналогові та цифрові системи перетворення	6	2	-	-	4
<b>Тема 14.</b> Технічні засоби охоронних систем. Системи доступу на об'єкт інформаційної діяльності. Підбір пароля.	5	2	-	-	3
<b>Тема 15.</b> Датчики та пристрої протипожежних систем	8	2	2	-	4
<b>Тема 16.</b> Системи ідентифікації. Основні типи пристроїв ідентифікації. Біометричні пристрої ідентифікації. Пристрої систем відеоспостереження	7	2	-	-	5
<b>Модульний контроль</b>					
<b>Разом за змістовим модулем 2</b>	<b>54</b>	<b>16</b>	<b>6</b>	-	<b>32</b>
<b>Усього годин</b>	<b>120</b>	<b>32</b>	<b>16</b>	-	<b>72</b>

### 5. Теми семінарських занять

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

### 6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	<b>Тема 3.</b> Методи вимірювань	2
2	<b>Тема 7.</b> Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані	4



	датчики руху	
3	<b>Тема 9.</b> Температура. Вимірювання і контроль температури об'єктів	2
4	<b>Тема 10.</b> Пристрої, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	2
5	<b>Тема 14.</b> Системи доступу на об'єкт інформаційної діяльності. Підбір пароля.	2
	<b>Разом</b>	<b>12</b>

### 7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	<i>Не передбачено</i>	
	<b>Разом</b>	

### 8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	<b>Тема 1.</b> Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення	5
2	<b>Тема 2.</b> Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації	6
3	<b>Тема 3.</b> Методи вимірювань	6
4	<b>Тема 4.</b> Технічні канали витоку інформації	4
5	<b>Тема 5.</b> Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах	4
6	<b>Тема 6.</b> Пристрій і принцип дії диференціального індуктивного перетворювача (датчика). Пристрій і принцип дії індукційного перетворювача	4
7	<b>Тема 7.</b> Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані датчики руху	6
8	<b>Тема 8.</b> Пристрій, принципи дій тензорезисторів. Пристрій, принципи дій магнітоупругих перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів	4
9	<b>Тема 9.</b> Температура. Вимірювання і контроль температури об'єктів	4
10	<b>Тема 10.</b> Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори)	4

№ з/п	Назва теми	Кількість годин
11	<b>Тема 11.</b> Інтелектуальні датчики	4
12	<b>Тема 12.</b> Сполучення перетворювачів з вимірювальною апаратурою	4
13	<b>Тема 13.</b> Аналогові та цифрові системи перетворення	4
14	<b>Тема 14.</b> Технічні засоби охоронних систем	4
15	<b>Тема 15.</b> Датчики та пристрої протипожежних систем	4
16	<b>Тема 16.</b> Системи ідентифікації. Основні типи пристроїв ідентифікації. Біометричні пристрої ідентифікації. Пристрої систем відеоспостереження	5
	<b>Разом</b>	<b>72</b>

### 9. Індивідуальні завдання

Виконання РГР (Обробка 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
<b>Змістовий модуль 1</b>			
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
<b>Змістовий модуль 2</b>			
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
<b>Усього за семестр</b>			<b>60...100</b>

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,

### виконання і захист практичних робіт:

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 - 1 бал;

- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 18 балів) виносяться всі пройдені за контрольований період теми, які входять до варіантів 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 умінь для одержання позитивної оцінки.

**Відмінно (90-100).** Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти 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. 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 Документ 3855-ХІІ, чинний, поточна редакція — Редакція від 31.03.2023, підстава - [2849-ІХ](#), <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.

2. Закон України Про інформацію Документ 2657-ХІІ, чинний, поточна редакція — Редакція від 27.07.2023, підстава - 3005-ІХ <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

3. Закон України «Про науково-технічну інформацію» від 25.06.1993, Документ 3322-ХІІ, чинний, поточна редакція — Редакція від 19.04.2014, <https://zakon.rada.gov.ua/laws/show/3322-12#Text>.

4. Закон України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах"». Документ 2594-ІV, чинний, поточна редакція — Прийняття від 31.05.2005, <https://zakon.rada.gov.ua/laws/show/2594-15#Text>.

5. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Документ 80/94-ВР, чинний, поточна редакція — Редакція від 01.07.2022, підстава - 2130-ІХ», <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

5. Закон України «Про Національну систему конфіденційного зв'язку». Документ 2919-ІІІ, чинний, поточна редакція — Редакція від 01.01.2022, підстава - 1089-ІХ, <https://zakon.rada.gov.ua/laws/show/2919-14#Text>.

6. Закон України «Про національну безпеку України». Документ 2469-ВІІІ, чинний, поточна редакція — Редакція від 31.03.2023, підстава - 2849-ІХ, <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

7. Закон України «Про основні засади забезпечення кібербезпеки України», Документ 2163-ВІІІ, чинний, поточна редакція — Редакція від 17.08.2022, підстава - 2470-ІХ, <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

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#Text>.

9. Указ Президента України «Про Положення про технічний захист інформації в Україні», Документ 1229/99, поточна редакція — Редакція від 04.05.2008, підстава - 333/2008, <https://zakon.rada.gov.ua/laws/show/1229/99#Text>.

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/show/1126-97-%D0%BF#Text>.

11. 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.

12. ГСТУ 78.11.001-98 Укріпленість об'єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони. Загальні технічні вимоги.

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

14. 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.

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

16. ДСТУ 3396.0-96 ТЗІ. Основні положення.

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

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

19. 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.

20. 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.