Форма № 4

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
(найменування центрального органу виконавчої влади у сфері освіти і науки)

Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Кафедра «Радіотехніка та телекомунікації»
(найменування кафедри, яка відповідає за дисципліну)

«ЗАТВЕРДЖУЮ»
Перший проректор
_____ Гугнін Е.А.
"02" 09 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ППВ 10 Захист інформації в телекомунікаційних системах
(код і назва навчальної дисципліни)

спеціальність 172 «Телекомунікації та радіотехніка»
(код і найменування спеціальності)

освітня програма (спеціалізація) Інформаційні мережі зв'язку
(назва освітньої програми (спеціалізації))

інститут Інформатики та радіоелектроніки
(найменування інституту)

факультет Радіоелектроніки та телекомунікацій
(найменування факультету)

мова навчання Українська

2020 рік

Робоча програма з дисципліни «**Захист інформації в телекомунікаційних системах**» для студентів

спеціальності 172 «Телекомунікації та радіотехніка»,

освітня програма (спеціалізація) «Інформаційні мережі зв'язку»
(назва освітньої програми (спеціалізації))

«_____» _____, 20__ року – _____ с.

Розробники: **Сметанін Ігор Миколайович**, старший викладач кафедри Радіотехніки та телекомунікацій.

Робоча програма затверджена на засіданні кафедри Радіотехніки та телекомунікацій

Протокол від « 23 » червня 2020 року № 12

Завідувач кафедри Радіотехніки та телекомунікацій
(найменування кафедри)

«23» червня 2020 року _____ (Морщавка С.В.)
(підпис) (прізвище та ініціали)

Схвалено науково-методичною комісією факультету РЕТ за спеціальністю **172 «Телекомунікації та радіотехніка»**

Протокол від « 27 » серпня 2020 року № 1

«27» серпня 2020 року Голова _____ (Кабак В.С.)
(підпис) (прізвище та ініціали)

_____ 2020 рік

1 Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3,5</td><td>Галузь знань
17 Електроніка та телекомунікації</td><td colspan="2">вибіркова</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність, освітня програма
172 Телекомунікації та радіотехніка
ОП «Інформаційні мережі зв’язку»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання _____.
(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – 105</td><td>8-й</td><td>8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 5
самостійної роботи студента – 10</td><td rowspan="10">Освітньо-кваліфікаційний рівень:
Перший (бакалаврський)</td><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>71 год.</td><td>95 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю:
іспит</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 34/71;

для заочної форми навчання – 10/95.

2 Мета та завдання навчальної дисципліни

Мета. Метою вивчення дисципліни є формування та розвиток у студентів певних загальних і професійних компетентностей з впровадження та застосування теоретичних і практичних основ знань методів і засобів захисту інформації у системах її створення та зберігання, системах зв'язку, в мережах обміну інформацією, а також у виробничих приміщеннях, які дозволять їм в подальшій професійній діяльності, або під час продовження освіти здійснювати аналіз, проектування і експлуатацію систем та мереж зв'язку з урахуванням основних вимог інформаційної безпеки.

Завдання. Основними завданнями дисципліни є вивчення:

– загальних принципів організації захисту інформації в радіотехнічних та телекомунікаційних системах і мережах на базі сучасних концепцій;

– принципів побудови та функціонування професійних пристроїв несанкціонованого знімання інформації у радіотехнічних та телекомунікаційних системах і мережах;

– принципів побудови та функціонування професійних технічних пристроїв захисту інформації в радіотехнічних та телекомунікаційних системах і мережах;

– принципів побудови та функціонування програмних засобів захисту інформації в радіотехнічних та телекомунікаційних системах і мережах;

– нормативно-правової бази захисту інформації в Україні.

За період вивчення дисципліни студенти повинні вивчити основні методи та засоби захисту інформації, а також отримати навички з вибору методик створення та обслуговування систем захисту технічних каналів витоку інформації.

У результаті вивчення навчальної дисципліни студент повинен отримати:

загальні компетентності: по вільному володінню державною мовою та спілкуванню іноземною мовою (ЗК-5), здатності працюючи в команді (ЗК-6) реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні (ЗК-11), застосовувати знання з питань захисту інформації у практичних ситуаціях (ЗК-2), приймати обґрунтовані рішення, а також здійснювати безпечну діяльність (ЗК-9);

фахові компетентності: по здатності розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства з точки зору дотримання умов захисту інформації (ПК-1); вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки (ПК-2); використовувати нормативну та правову документацію, що стосується телекомунікаційних та радіотехнічних систем для вирішення професійних завдань з питань інформаційної безпеки (ПК-5), здійснювати комп'ютерне моделювання пристроїв, систем і процесів з використанням універсальних пакетів прикладних програм для отримання більш якісного захисту інформації (ПК-4); здатність планувати та здійснювати заходи з

забезпечення захисту інформації в телекомунікаційних системах та мережах інформаційного зв’язку.

Очікувані програмні результати навчання: відповідно до визначених компетентностей студент повинен **знати** порядок оцінювання, інтерпретації, синтезу та захисту інформації і даних (РН-5); основні властивості компонентної бази для забезпечення якості, надійності функціонування та захисту інформації в телекомунікаційних, радіотехнічних системах і пристроях (РН-14); як знаходити, оцінювати і використовувати інформацію з різних джерел, необхідну для розв’язання професійних завдань з точки зору безпеки, включаючи відтворення інформації через електронний пошук (РН-18); методики стандартних випробувань інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів по боротьбі з інформаційною злочинністю (РН-19), а також **уміти** спілкуватись з професійних питань із інформаційної безпеки, включаючи усну та письмову комунікацію державною мовою та однією з поширених європейських мов (РН-10); аналізувати, аргументувати, приймати рішення при розв’язанні спеціалізованих задач та практичних проблем по захисту інформації, які характеризуються комплексністю та неповною визначеністю умов (РН-1); пояснювати результати, отримані в результаті проведення специфічних вимірювань, в термінах їх значущості та пов’язувати їх з відповідною теорією (РН-4); контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування системи захисту чи її відмови, та систематично фіксувати всі відхилення в її роботі шляхом документування (РН-22); планувати та здійснювати заходи, спрямовані на забезпечення заданого рівня інформаційної безпеки в інформаційних мережах зв’язку.

3 Програма навчальної дисципліни

Змістовий модуль 1. Основи інформаційної безпеки і захисту інформації.

Тема 1. Вступ. Основні концептуальні положення системи захисту інформації.

Сучасна постановка проблеми захисту інформації. Поняття «Інформаційна безпека». Місце, цілі і завдання інформаційної безпеки.

Концептуальна модель інформаційної безпеки. Цілі переслідувані джерелами загроз. Прояв загроз інформації. Класифікація загроз.

Дії, що призводять до неправомірного оволодіння конфіденційною інформацією і їх класифікація. Розголошування. Витік. Несанкціонований доступ. Формальні та неформальні канали поширення інформації.

Забезпечення інформаційної безпеки. Основні принципи забезпечення інформаційної безпеки. Рівні (напрями) захисту інформації.

Правові основи захисту інформації. Структура законодавства України в області захисту інформації.

Організаційні заходи захисту інформації. Організаційно-правові форми захисту інформації.

Інженерно-технічний захист. Класифікація інженерно-технічний захисту.

Тема 2. Об'єкти захисту, відомості, що охороняються, і демаскуючі ознаки.

Об'єкти захисту. Основні об'єкти захисту. Перелік об'єктів, які підлягають захисту в технічних засобах передачі, зберігання і обробки інформації. Перелік об'єктів, які підлягають захисту в допоміжних технічних засобах і системах.

Відомості, що охороняються. Відомості у військовій області. Відомості в області економіки, науки і техніки. Відомості в сфері зовнішньої політики і економіки. Відомості в області розвідувальній, контррозвідувальній і оперативно-пошуковій діяльності.

Демаскуючі ознаки. Первинні демаскуючі ознаки. Вторинні демаскуючі ознаки. Формування переліку демаскуючих ознак методом експертних оцінок.

Тема 3. Класифікація і основні характеристики технічних каналів просочування інформації.

Поняття і структура технічного каналу просочування інформації (ТКПІ). Класифікація видів ТКПІ.

Канали просочування інформації, що обробляється технічними засобами прийому, обробки, зберігання і передачі інформації.

Канали просочування мовної інформації. Акустичні, вібраційні, акустоелектричні, оптоелектронні (лазерні) і параметричні канали.

Канали просочування інформації при її передачі по каналах зв'язку. Електромагнітні, електричні та індукційні канали.

Технічні канали витоку відеоінформації. Спостереження за об'єктами. Зйомка об'єктів. Зняття копій документів.

Несанкціонований доступ до інформації, що обробляється засобами обчислювальної техніки. Спроби злому засобів обчислювальної техніки

Технічні канали просочування інформації, що виникає при роботі обчислювальної техніки за рахунок ПЕМВН. Класифікація каналів по середовищу поширення, за способом створення, по фізичній природі.

Тема 4. Акустичні і віброакустичні канали просочування мовної інформації з об'ємів виділених приміщень.

Основні поняття, визначення і одиниці виміру в акустиці.

Основні акустичні параметри мовних сигналів. Основні статистичні параметри: частотний діапазон, рівень мовних сигналів, динамічний діапазон, сприйняття мови, розбірливість і зрозумілість мови.

Поширення акустичних сигналів в приміщеннях і будівельних конструкціях. Основні поняття в будівельній акустиці. Коефіцієнти поглинання, відображення, звукопроникності та звукоізоляція.

Канали просочування мовної інформації. Акустичні та віброакустичні канали.

Акустичне підслуховування — пасивний спосіб добування інформації. Види об'єктів, які визначають вибір каналу прослуховування і тактику дій зловмисника

Тема 5. Знімання інформації з використанням закладних пристроїв. Загальні характеристики і побудова закладних пристроїв.

Класифікація і загальні характеристики заставних пристроїв.

Радіозакладні пристрої.

Радіозакладні пристрої, що перевипромінюють.

Закладні облаштування типу «довге вухо».

Мережеві закладні пристрої.

Змістовий модуль 2. Методи і способи захисту інформації.

Тема 6. Виявлення каналів просочування інформації.

Заходи по виявленню і протидії роботі закладних пристроїв.

Засоби виявлення каналів просочування інформації. Засоби виявлення облаштувань знімання інформації з радіоканалом. Автоматизовані пошукові комплекси. Нелінійні локатори. Досмотрова техніка. Засоби радіаційного контролю.

Тема 7. Захист мовної інформації.

Методи, які застосовуються для захисту мови від несанкціонованого прослуховування. Активні і пасивні методи. Основна ідея пасивних засобів захисту інформації. Пасивні засоби захисту виділених приміщень.

Звукоізоляція приміщень. Коефіцієнти поглинання звуку різними середовищами.

Способи активного захисту приміщень. Вібродатчики систем віброакустичного зашумления.

Оптимальні параметри перешкод і апаратура для їх постановки.

Особливості постановки активних перешкод.

Тема 8. Основи сучасної криптографії і питання шифрування. Криптографія і криптосистеми.

Історія криптографії, основні терміни і вимоги, що пред'являються до криптосистем. Історія криптографії. Термінологія. Криптографічна система. Основні вимоги, що пред'являються до криптосистем.

Симетричні криптосистеми і системи шифрування. Перестановки.

Системи підстановок. Підстановка Цезаря. Гамування. Блокові шифри. Шифри Хилла і Плейфера. Системи шифрування Вижинера.

Датчики ПВЧ. Багатоалфавітні системи. Системи одноразового використання. Датчики М-послідовностей.

Стандарт шифрування даних ДОСТ 28147-89.

Тема 9. Огляд сучасних криптосистем. Засоби аутентифікації даних і управління ключами шифрування.

Системи з відкритим ключем. Безповоротні або односторонні функції. Засоби для розподілу ключів.

Алгоритм RSA. Гарантована оцінка захищеності алгоритму RSA. Математичні результати. Практична реалізація RSA.

Криптосистема Ель-Гамаля.

Криптосистеми на основі еліптичних рівнянь.

Електронний підпис. Можливі порушення захисту повідомлень. Засоби аутентифікації користувачів. Електронний підпис на основі алгоритму RSA.

Цифрова сигнатура. Хэш-функції

Управління ключами. Генерація ключів. Накопичення ключів. Розподіл ключів. Механізм запиту-відповіді. Механізм відмітки часу ("часовий штемпель").

4 Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1. Основи інформаційної безпеки і захисту інформації.												
Тема 1. Вступ. Основні концептуальні положення системи захисту інформації.	7	2	–	–	–	5	7	–	–	–	–	7
Тема 2. Об'єкти захисту, відомості, що охороняються, і демаскуючі ознаки.	12	2	–	2	–	8	12	1	–	–	–	11
Тема 3. Класифікація і основні характеристики технічних каналів просочування інформації.	11	2	–	–	–	9	11	1	–	–	–	10
Тема 4. Акустичні і віброакустичні канали просочування мовної інформації з об'ємів виділених приміщень.	12	2	–	3	–	7	12	–	–	1	–	11
Тема 5. Знімання інформації з використанням закладних пристроїв. Загальні характеристики і побудова закладних пристроїв.	10	2	–	2	–	6	10	1	–	1	–	8
Разом за змістовим модулем 1	52	10	–	7	–	35	52	3	–	2	–	47
Змістовий модуль 2. Методи і способи захисту інформації.												
Тема 6. Виявлення каналів просочування інформації.	9	2	–	2	–	5	9	1	–	–	–	8
Тема 7. Захист мовної інформації.	14	2	–	3	–	9	14			1	–	13
Тема 8. Основи сучасної криптографії і питання шифрування. Криптографія і криптосистеми.	16	3	–	2	–	11	16	1	–	1	–	14
Тема 9. Огляд сучасних криптосистем. Засоби аутентифікації даних і управління ключами шифрування..	14	3	–	–	–	11	14	1	–	–	–	13
Разом за змістовим модулем 2	53	10	–	7	–	36	53	3	–	2	–	48
Усього годин	**105**	**20**	**–**	**14**	**–**	**71**	**105**	**6**	**–**	**4**	**–**	**95**
Модуль 2												
ІНДЗ			–	–		–			–	–	–	
Усього годин												

5 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження регламенту радіочастотного діапазону від 30 МГц до 1ГГц м.Запоріжжя	2
2	Дослідження спрямованих мікрофонів	3
3	Контактне зняття мовної інформації з телефонної лінії з використанням програмно-апаратного комплексу	2
4	Вивчення характеристик та будови пристрою СРМ-700 («Акула»)	2
5	Дослідження генератору акустичного зашумлення ANG-2200	3
6	Дослідження маскувача мовних сигналів	2
	Разом	14

6 Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Підготовка до лабораторних та лекційних занять	51
2	Підготовка до поточного контролю та іспиту	20
	Разом	71

7 Індивідуальні завдання

Реферат за темою однієї з лабораторних робіт.

8 Методи навчання

Поєднання (різною мірою) пасивного, активного і інтерактивного методів на лекційних і лабораторних заняттях, на консультаціях по темам занять.

9. Очікувані результати навчання з дисципліни

В процесі опанування дисципліни, здобувач вищої освіти за першим (бакалаврським) рівнем має бути ознайомленим з вимогами законодавчої бази України щодо особливостей інформаційної безпеки у галузі; базовими моделями керування доступом та видами і механізмами контролю цілісності даних, будувати стандартизовані або використовувати стандартні профілі захисту інформації від несанкціонованого доступу, виявляти канали витоку інформації в

радіотехнічних та телекомунікаційних системах, вживати методи протидії навмисним спробам порушити цілісність інформації. Це дозволить йому в майбутній професійній діяльності або навчанні вирішувати ряд важливих завдань з питань інформаційної безпеки.

10. Засоби оцінювання

Оцінювання ступені засвоєння студентом теоретичного та практичного матеріалу за результатами навчання здійснюється під час семестрового контролю, шляхом проведення семестрового екзамену, який виконується в формі електронного тестування в Системі дистанційного навчання НУ «Запорізька політехніка» (moodle.zp.edu.ua). Крім того, проводитися поточний контроль у формі усного опитування на лабораторних заняттях та лекціях, а рубіжний (модульний) контроль проводитися у формі електронного тестування.

Це дозволяє об'єктивно встановити рівень знань та умінь, що набули студенти під час вивчення цієї дисципліни, оцінити якість підготовки спеціалістів за фахом.

11. Критерії оцінювання

Поточне тестування та самостійна робота									Підсумковий тест (екзамен)	Сума
Змістовий модуль №1					Змістовий модуль № 2					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9		
10	10	15	15	10	10	10	10	10	100	100

Т1, Т2 ... Т9 – теми змістових модулів.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену, курсового проекту (роботи), практики
90 – 100	**A**	відмінно
85-89	**B**	добре
75-84	**C**	
70-74	**D**	задовільно
60-69	**E**	
35-59	**FX**	незадовільно з можливістю повторного складання
1-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни

12. Методичне забезпечення

1. Методичні вказівки до виконання лабораторних робіт з дисципліни “Захист інформації в телекомунікаційних системах” для студентів спеціальності 172 «Телекомунікації та радіотехніка», які навчаються за освітньою програмою «Інформаційні мережі зв’язку» всіх форм навчання. Частина 1 / Укл. Сметанін І.М. –Запоріжжя: НУ"Запорізька політехніка", 2019. – 79 с.

2. Методичні вказівки до виконання лабораторних робіт з дисципліни “Захист інформації в телекомунікаційних системах” для студентів спеціальності 172 «Телекомунікації та радіотехніка», які навчаються за освітньою програмою «Інформаційні мережі зв’язку» всіх форм навчання. Частина 2 / Укл. Сметанін І.М. – Запоріжжя: НУ"Запорізька політехніка", 2019. – 66 с.

3. Методичні вказівки до самостійного вивчення дисципліни “Захист інформації в телекомунікаційних системах” для студентів спеціальності 172 «Телекомунікації та радіотехніка», які навчаються за освітньою програмою «Інформаційні мережі зв’язку» заочної форми навчання /Укл.: І.М. Сметанін. – Запоріжжя: НУ"Запорізька політехніка", 2019. – 91 с.

4. Електронний конспект лекцій.

5. Електронні презентації лекцій в Microsoft PowerPoint. / Розр. І.М. Сметанін.

6. Курс "Захист інформації в телекомунікаційних системах" в Системі дистанційного навчання НУ «Запорізька політехніка» на платформі Moodle. / Розр. І.М. Сметанін.

13 Рекомендована література

Базова

1. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации: учеб. пособие для студ. выш. учеб заведений. – М.: Издательский центр “Академия”, 2006. – 256 с.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М: Горячая линия-Телеком, 2004. – 280с.
3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия-Телеком, 2005. – 416с.
4. Бурячок В.Л., Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. – К.:ДУТ, 2015. – 345 с.
5. Железняк В. К. Защита информации от утечки по техническим каналам: учебное пособие / В. К. Железняк; ГУАП. – СПб., 2006. – 188 с.
6. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.

Допоміжна

7. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности –М.: Гелиос АРВ, 2005. – 960 с.:.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 с.
9. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд.– 2004. – 544 с.
10. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации: – К.: изд. Юниор, 2003. – 504 с.
11. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. М.: Гротек, 1997 г. - 248 с.
12. Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и способы защиты информации. – СПб.: Полигон, 2000. – 320 с.
13. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник./ В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.
14. Соколов А.В. Шпионские штучки. Новое и лучшее. – СПб.: ООО «Издательство Полигон», 2000.– 256 с.
15. Мельников В. П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб.

заведений /под. ред. С.А.Клейменова. — 3-е изд., — М.: Издательский центр «Академия», 2008. — 336 с.
16. Петраков А.В. Основы практической защиты информации: Учеб. пособие. - М.: Радио и связь, 1999. – 368 с.
17. Организация и современные методы защиты информации. / под общей редакцией Диева С. А. И Шаваева А. Г./. – М.: Концерн "Банковский Деловой Центр", 1998, – 472 с.
18. Барсуков В.С. Обеспечение информационной безопасности. – М: ТЭК, 1996. – 268 с.
19. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. — М.: Гелиос АРВ, 2005. – 192 с.
20. Хорев А.А Способы и средства защиты информации. М.: МО РФ, 2000 г. - 316 с.
21. Богуш В.М., Юдін О.К. Інформаційна безпека держави. [Текст] / В.М. Богуш, О.К. Юдін. – К.: "МК-Прес", 2005. – 432 с.
22. Энциклопедия промышленного шпионажа/ Ю.Ф.Каторин, Е.В.Куренков, А.В.Лысов, А.Н.Остапенко / под общ. Ред. Е.В.Куренкова. - С. Петербург: ООО «Изд-во Полигон», 1999.-512 с.
23. Архипов О.Є., Луценко В.М., Худяков В.О. Захист інформації в телекомунікаційних мережах та системах зв'язку: Навч.-метод. посіб. – К.: Політехніка, 2003. – 40 с.
24. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. – М.: изд. "Ось", 1995. – 54 с.
25. Гайкович В.Ю. Першин А.М. Безопасность электронных банковских систем. – М.: Компания Единая Европа, 1994. – 384 с.
26. Волхонский В. В. Устройства охранной сигнализации. – СПб.: Экономпис и культура, 1999. – 272 с.
27. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: Учеб. пособие. – СПб.: СПбГУТ.-СПб, 2000. – 134 с.

Періодичні видання:

28. "Системы безопасности связи и телекоммуникаций" - издатель компания «Гротек», Москва;
29. "Защита информации. Конфидент" - издатель ООО «Конфидент», С.-Петербург;
30. "Специальная техника" - учредитель ОАО ХК «Электрозавод», Москва;
31. "БДИ" (Безопасность, Достоверность, Информация), С.-Петербург.

14. Інформаційні ресурси

1. www.zntu.edu.ua
2. www.rtt.zntu.edu.ua
3. www.moodle.zp.edu.ua