

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра програмованої електроніки, електротехніки і телекомунікацій

Код РПНД: Т72333



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

Захист інформації в суднових телекомунікаційних системах
INFORMATION SECURITY IN SHIP TELECOMMUNICATION SYSTEMS

рівень вищої освіти перший (бакалаврський)
перший (бакалаврський) / другий (магістерський)

тип дисципліни обов'язкова
обов'язкова/вибіркова

мова(и) викладання українська

Робоча програма навчальної дисципліни «Захист інформації в суднових телекомунікаційних системах» є однією із складових комплексної підготовки фахівців галузі знань 17 «Електроніка, автоматизація та електронні комунікації»

Спеціальності 172 «Електронні комунікації та радіотехніка»

освітня програма «Телекомунікації»

" 20 " травня 2023 року. – 16 с.

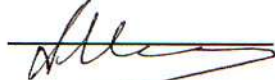
Розробник: Трибулькевич С.Л., ст. викладач кафедри ПЕЕТ



Проект робочої програми навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» узгоджено з гарантом освітньої програми.

Гарант освітньої програми «ТЕЛЕКОМУНІКАЦІЇ»

к.т.н., доц. О.К.Жук



Проект робочої програми навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» розглянуто на засіданні кафедри програмованої електроніки, електротехніки і телекомунікацій

Протокол № 11 від «06» 06 2023 р.

Завідувач кафедри ПЕЕТ  д.т.н., проф. Рябенський В.М.

Проект робочої програми навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки

Протокол № 10 від «19» 06 2023 р.

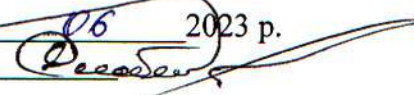
Голова  к.т.н., доцент Жук Д.О.

Проект робочої програми навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» погоджено з навчальним відділом

Начальник відділу  к.т.н., доц. Лабарткава А.В.

Робоча програма навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» затверджена Навчально-методичною радою НУК

Протокол № 5 від «28» 06 2023 р.

Голова НМР-НУК 

ЗМІСТ

ЗМІСТ	3
ВСТУП.....	4
1. Опис навчальної дисципліни.....	5
2. Мета вивчення навчальної дисципліни.....	6
3. Передумови для вивчення дисципліни	6
4. Очікувані результати навчання.....	6
5. Програма навчальної дисципліни.....	7
6. Методи навчання, засоби діагностики результатів навчання та методів їх демонстрування	12
7. Форма поточного та підсумкового контролю	12
8. Критерії оцінювання результатів навчання.....	15
9. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна	16
10. Рекомендовані джерела інформації.....	16

ВСТУП

Анотація

Вивчення основних методів та засобів захисту інформації в суднових телекомунікаційних системах, дослідження проблеми захисту інформації, які виникають у системах зв'язку і передачі даних, радіотехнічних системах, аналіз каналів витоку інформації, методів і способів несанкціонованого отримання інформації.

Програма дисципліни має на меті вивчення студентами теорії та оволодіння практичними навичками при роботі з телекомунікаційними системами у питаннях захисту інформації.

Курс захисту інформації в суднових телекомунікаційних системах носить міждисциплінарний характер з використанням технічних засобів навчання, сучасних технологій оволодіння практичними навичками експлуатації, впровадження та супроводження мереж.

Ключові слова: канал витоку, загроза, модель порушника, антивірусний захист, шифрування.

Abstract

Study of the basic methods and means of information protection in ship telecommunication systems, research of the problem of information protection arising in communication and data transmission systems, radio systems, analysis of information leakage channels, methods and ways of unauthorized receipt of information.

The discipline program aims to teach students the theory and master practical skills in working with telecommunications systems in matters of information security.

The course of information protection in ship telecommunication systems is interdisciplinary in nature with the use of technical means of training, modern technologies for mastering practical skills of operation, implementation and maintenance of networks.

Key words: leakage channel, threat, intruder model, antivirus protection, encryption.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність (освітня програма), освітній рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 3	Галузь знань 17 Електроніка, автоматизація та електронні комунікації	Обов'язкова	Обов'язкова
Модулів – 1		Рік підготовки:	
Змістових модулів – 2		4-й	4-й
Електронний адрес РПНД на сайті Університету	Спеціальність – 172 Електронні комунікації та радіотехніка Освітня програма – Телекомунікації	Семестр	
Індивідуальне науково-дослідне завдання: –		8-й	8-й
		Лекцій	
		15 год.	6 год.
Загальна кількість годин: 90		Практичні	
		15 год.	6 год.
		Лабораторні	
Тижневих годин для денної форми навчання: аудиторних – 3; самостійної роботи студента – 5;		Освітній рівень: перший (бакалаврський)	Самостійна робота
	60 год.		78 год.
	Індивідуальні завдання: не передбачено		
	Вид контролю: 8-й сем. – екзамен		
	Форма контролю: комбінована		

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ В СУДНОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ» є базова підготовка з питань захисту інформації в телекомунікаційних і інформаційних мережах – вивчення основних методів та засобів захисту інформації в судових телекомунікаційних системах, дослідження проблеми захисту інформації, які виникають у системах зв'язку і передачі даних, радіотехнічних системах, аналіз каналів витоку інформації, методів і способів несанкціонованого отримання інформації, а також формування у студентів відповідно до освітньо-професійної програми таких компетентностей:

- ЗК7 – здатність до абстрактного мислення, аналізу та синтезу;
- ЗК8 – вміння виявляти, ставити та вирішувати проблеми;
- СК1 – здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства;
- СК2 – здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій та з урахуванням основних вимог інформаційної безпеки;
- СК5 – здатність використовувати нормативну та правову документацію, що стосується інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем (закони України, технічні регламенти, міжнародні та національні стандарти, рекомендації Міжнародного союзу електрозв'язку тощо) для вирішення професійних завдань.

3. Передумови для вивчення дисципліни

Передумовами для вивчення дисципліни є дисципліни: «Кінцеві пристрої абонентського доступу», «Системи комутації та розподілу інформації».

4. Очікувані результати навчання

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів таких результатів навчання:

- ПРН6 – адаптуватись в умовах зміни технологій інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем;
- ПРН22 – контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування.
- ПРН24 – здійснювати сервісне обслуговування, перевірку та випробування судового радіонавігаційного обладнання та систем зв'язку на відповідність вимогам нормативних документів.

5. Програма навчальної дисципліни

Змістовий модуль 1. Методи та засоби захисту від атак.

Тема 1. Основи захисту інформації в телекомунікаційних системах і мережах. Типові віддалені атаки..

Лекція 1. Основні поняття та категорії. Нормативно-правове забезпечення інформаційної безпеки. [1] с. 7-30, [7] с. 6-16.

Лекція 2. Загрози інформації. Способи несанкціонованого доступу до інформації в компютерних системах та засоби захисту від нього. [5] с. 209-236, [7] с. 25-30, [4] с. 41-57.

Тема 2. Засоби антивірусного захисту інформації.

Лекція 3. Віруси: види та класифікація. Файлові віруси. Мережеві віруси. Шкідливі програми [5] с. 382-400.

Лекція 4. Технологія зараження. Технології виявлення. Проблеми антивірусного захисту. Види моніторингу. [5] с. 432-453.

Тема 3. Програмні методи та засоби захисту інформації у телекомунікаційних системах.

Лекція 5. Стратегія захисту інформації в комп'ютерних системах. Основні принципи побудови систем захисту інформації. Програми внутрішнього захисту. Програми зовнішнього захисту. [6] с. 164-191; [7] с. 25-41.

Лекція 6. Програми ядра безпеки. Програми контролюю Програмна реалізація оцінки агресивності програмних засобів. Визначення факту інформаційного вторгнення. Використання інформаційного сліду при пошуку програмних закладок. [6] с. 190-206.

Тема 4. Апаратні та апаратно-програмні методи та засоби захисту інформації у телекомунікаційних системах.

Лекція 7. Класифікація засобів технічного захисту інформації в каналах загального користування. Пристрої захисту інформації в телекомунікаційних системах. Методи захисту факсимільних та телефонних апаратів. [4] с. 107-134; [6] с. 120-128.

Лекція 8. Захист ліній зв'язку. Виявлення факту та визначення місця зйому інформації. Методи і засоби захисту телефонних ліній. Захист волоконно-оптичних ліній. Екранування приміщень. [6] с. 75-120, 128-164.

Змістовий модуль 2. Захист інформації у мережах.

Тема 5. Технічний захист інформації в спеціальних ІТС.

Лекція 9. Призначення та склад автоматизованих систем управління технологічними процесами. Потенційна небезпека АСУ ТП. Найбільш часті уразливості. [5] с. 236-272.

Лекція 10. Реалізація системи інформаційної безпеки. Інтеграція з промисловою безпекою. Етапи робіт із забезпечення кібербезпеки АСУ ТП. [5] с. 451-460; [6] с. 10-22.

Тема 6. Криптографічні методи захисту інформації при її передаванні у телекомунікаційних мережах.

Лекція 11. Основні принципи криптографії. Класифікація шифрів. [4] с. 191-196; [6] с. 206-227

Лекція 12. Криптографічні алгоритми. Симетричні шифри. Асиметричні шифри. Електронний цифровий підпис. [1] с. 196-229; [6] с. 227-295.

Тема 7. Стеганографічні методи захисту інформації при її передаванні у телекомунікаційних мережах.

Лекція 13. Стеганографічні технології. Класифікація стеганографічних методів. Класифікація стегосистем. [6] с. 311-317.

Лекція 14. Класифікація методів приховування інформації. Текстові стенографи. Приховування інформації у зображенні та відео. Приховування інформації у звуковій середі. [6] с. 318-338; [7] с. 154-164.

Тема 8. Захист в мережах. Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій.

Лекція 15. Керування доступом до об'єктів в комп'ютерних системах. Захист інформації від несанкціонованого доступу в операційних системах Windows. [7] с. 60-69.

Лекція 16. Підсистема безпеки операційних систем. Аудит безпеки [7] с. 73-122.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	У тому числі				усього	у тому числі			
		лек	пр	лаб	с.р.		лек	пр	лаб	с.р.
1	2	3	4	5	6	7	8	9	10	11
Модуль 1										
Змістовий модуль 1. Основи побудови телекомунікаційних мереж										
Тема 1. Основи захисту інформації в телекомунікаційних системах і мережах. Типові віддалені атаки	8	1	0		7	10	1	0		9
Тема 2. Засоби антивірусного захисту інформації	13	2	3		8	11	0	1		10
Тема 3. Програмні методи та засоби захисту інформації у телекомунікаційних системах	12	2	2		8	12	1	1		10
Тема 4. Апаратні та апаратно-програмні методи та засоби захисту інформації у телекомунікаційних системах	12	2	2		8	12	1	1		10
Разом за змістовим модулем 1	45	7	7		31	45	3	3		39
Змістовий модуль 2. Сучасні телекомунікаційні мережі										
Тема 5. Технічний захист інформації в спеціальних ІТС	9	2	0		7	9	0	0		9
Тема 6. Криптографічні методи захисту інформації при її передаванні у телекомунікаційних мережах	13	2	3		8	12	1	1		10
Тема 7. Стеганографічні методи захисту інформації при її передаванні у телекомунікаційних мережах	11	2	2		7	12	1	1		10
Тема 8. Захист в мережах. Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій	12	2	3		7	12	1	1		10
Разом за змістовим модулем 2	45	8	8		29	45	3	3		39
Усього годин за модуль 1	90	15	15	0	60	90	6	6	0	78
Усього годин	90	15	15	0	60	90	6	6	0	78

Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	2	3	4
Змістовий модуль 1			
1	Антивірусний захист	3	1
2	Міжмережеві екрани	2	1
3	Настроювання дозволів доступу до файлів і папок NTFS	2	1
Змістовий модуль 2			
5	Аудит доступу до ресурсів	3	1
6	Аналіз стійкості паролей Windows	2	1
8	IP-безпека	3	1
	<i>Разом</i>	15	6

Самостійна робота

Самостійна робота студента має на меті поглиблення знань студента з дисципліни і передбачає проробку лекційного матеріалу, підготовку до лабораторних занять, опрацювання окремих питань тем змістових модулів з використанням рекомендованої та додаткової літератури, підготовку до поточного (модульного) контролю знань, вивчення розділів літературних джерел, які не увійшли до курсу.

Розподіл годин самостійної роботи для студентів денної форми навчання:

- підготовка до лекційних занять – **1 год. / 1 лекцію;**
- підготовка до практичних занять – **2-3 год. / 1 робота;**
- підготовка до семінарських занять – **2-4 год/1 заняття**
- підготовка до тестування – **5-6 год. / 1 тест;**
- підготовка до екзамену – **15 год.**

Завдання для самостійної роботи

№ з/п	Вид роботи	Кількість годин	
		Денна форма	Заочна форма
1	2	3	4
Змістовий модуль 1			
1	Підготовка до лекційних занять	5	7
2	Підготовка до лабораторних робіт	10	10
3	Написання реферату	10	16
4	Підготовка до тестування	6	6
		31	39
Змістовий модуль 2			
5	Підготовка до лекційних занять	4	7
6	Підготовка до лабораторних робіт	5	12
7	Підготовка до тестування	5	5
8	Підготовка до екзамену	15	15
		29	39
	Разом	60	78

Індивідуальне науково дослідне завдання

Не передбачено.

6. Методи навчання, засоби діагностики результатів навчання та методів їх демонстрування

Методи навчання:

- лекції;
- практичні роботи;
- робота з літературою;
- інструктаж з техніки безпеки та пожежної безпеки (проводиться одноразово на першому занятті в лабораторії).

Засоби оцінювання та методи демонстрування результатів навчання з дисципліни:

- стандартизовані тести;
- модульні контрольні роботи;
- презентації результатів виконаних практичних робіт;
- презентації результатів виконаних досліджень;
- підсумкова семестрова контрольна робота;
- екзамен.

7. Форма поточного та підсумкового контролю

Рівень засвоєння матеріалу дисципліни здійснюється шляхом проведення поточного контролю у вигляді тестових завдань різної складності, результатів роботи на практичних заняттях та підсумкового контролю у формі екзамену. Питома вага заключного екзамену в загальній системі оцінок – 40 балів.

Поточний контроль проводиться на кожному практичному занятті та за результатами самостійної роботи. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми шляхом тестування (у тому числі, самостійно опрацьованого матеріалу) та набутих практичних навичок під час виконання завдань практичних робіт. Підсумкова оцінка з дисципліни складається з оцінок, отриманих за поточний модульний контроль у формі тестування – до 20 балів, результатів роботи на практичних заняттях – до 40 балів та екзамену – до 40 балів.

За всі контрольні заходи (КЗ) протягом семестру студент може отримати від 0 до 100 балів. Умовою допуску студента до КЗ є мінімальна сума балів, яку студент повинен набрати у разі виконання всіх елементів модулів. Якщо студент не набрав мінімальну суму балів, то він не допускається до КЗ і йому рекомендується набрати цю кількість за рахунок написання реферату на одну із зазначених вище тем.

Семестровий підсумковий контроль здійснюється у формі екзамену, що проводиться у письмовій формі в екзаменаційну сесію). Студент, який набрав за всі КЗ менше 60 балів, пише підсумкову семестрову залікову роботу (проводиться у письмовій формі у вигляді тестів), до якої він допускається, якщо має за виконання всіх передбачених елементів модулів необхідну мінімальну суму 50 балів. Максимальна кількість балів за підсумкову залікову роботу становить 40 балів. Результуюча оцінка виставляються відповідно до шкали оцінювання ECTS.

Форми контролю результатів навчальної діяльності студентів та їх оцінювання

Практичні заняття	Критерії оцінювання
5	Студент виконував всі завдання самостійно, чітко сформулював цілі, завдання та гіпотезу досліджень. Застосовувалися коректні методи обробки отриманих результатів, проведена коректна інтерпретація результатів.
4	Студент виконує роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; в цілому правильно робить висновки.
3	Студент виконує роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; відповіді частково правильні, містить неточності, недостатньо обґрунтовані.

2	Студент виконує роботу згідно з інструкцією; відповіді мають суттєві помилки, аргументи несформульовані, використовуються невірна термінологія.
1	Студент виконує роботу під керівництвом викладача; відповіді містять значну кількість суттєвих помилок та не обґрунтовані.
0	Робота не виконувалася
	Максимальна оцінка студента за даний компонент програми 40 балів (8 робіт по 5 балів).

Поточний модульний контроль у формі тестування

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

Форма контролю	Максимальна кількість балів	
	Денна форма	Заочна форма
Робота на практичних заняттях	8x5 балів = 40 бали	8x5 балів = 40 бали
Поточний модульний контроль у формі тестування	2x10 бали = 20 балів	2x10 бали = 20 балів
Всього	60	60

Критерії оцінювання знань з дисципліни на екзамені

Екзамен (8-й семестр) проводиться в письмовій формі та складається з трьох завдань – двох теоретичних запитань та тесту. Максимальна оцінка студента за даний компонент програми 40 балів

Виконання першого завдання потребує повної аналітичної і змістовної відповіді (оцінюється від 0 до 15 балів).

13-15 балів отримують студенти, які повно та ґрунтовно розкрили теоретичне питання, використавши при цьому не лише обов'язкову, а й додаткову літературу, в повному обсязі володіють навчальним матеріалом, вільно, самостійно й аргументовано його викладають під час письмової відповіді.

10-12 балів отримують студенти, які достатньо повно володіють навчальним матеріалом, в цілому розкрили теоретичне питання, однак не повно, і допустили деякі несуттєві неточності та незначні помилки, не вистачає достатньої глибини та аргументації. При цьому не було використано на достатньому рівні обов'язкову літературу.

8-9 балів отримують студенти, які в цілому володіють навчальним матеріалом, правильно визначили сутність питання, але розкрили його не повністю, без глибокого всебічного аналізу, обґрунтування та аргументації, допустивши деякі незначні помилки.

6-7 балів отримують студенти, які в цілому володіють навчальним матеріалом, правильно визначили сутність питання але без використання необхідної літератури, розкривши його частково і допустивши при цьому окремі суттєві неточності і помилки, котрі частково впливають на загальне розуміння питання.

3-5 балів отримують студенти, які не в повному обсязі володіють матеріалом, загалом правильно визначили сутність питання, однак недостатньо або поверхнево розкривши більшість його окремих положень і допустивши при цьому окремі помилки, які частково вплинули на загальне розуміння проблеми.

0-2 бали отримують студенти, які частково володіють навчальним матеріалом, фрагментарно та поверхнево розкрили лише окремі положення питання і допустили при цьому певні суттєві помилки, котрі значно вплинули на загальне розуміння питання.

Друге питання потребує короткої відповіді, котра розкриває сутність того чи іншого поняття або теоретичного положення (оцінюється від 0 до 15 балів).

12-15 балів отримують студенти, які повністю розкрили сутність поняття, дали його чітке визначення або проаналізували і зробили висновок з конкретного теоретичного положення.

7-11 балів отримують студенти, які правильно, але не повністю дали визначення поняття, або поверхнево проаналізували і зробили висновок з теоретичного положення.

3-6 балів отримують студенти, які правильно, але лише частково визначили те чи інше поняття, або частково проаналізували і зробили висновок з теоретичного положення.

0-2 бали отримують студенти, які частково і поверхнево визначили те чи інше поняття або сформулювали висновок з теоретичного положення, допустивши неточності та помилки.

Третє завдання підсумкового екзамену представляє собою тест, що містить 10 запитань і оцінюється від 0 до 10 балів. Кожна вірна відповідь на запитання тесту оцінюється в 1 бал.

8. Критерії оцінювання результатів навчання

8-й семестр

		Денне відділення 8-й семестр		Заочне відділення 8-й семестр	
		Вид роботи	Кіл.	Вид роботи	Кіл.
ЗМ 1	T1	Практичне заняття №1	5	Практичне заняття №1	5
	T2	Практичне заняття №2	5	Практичне заняття №1	5
	T3	Практичне заняття №3	5	Практичне заняття №2	5
	T4	Практичне заняття №4	5	Практичне заняття №3	5

ПМК		Тест	10	Тест	10
ЗМ 2	T5	Практичне заняття №5	5	Практичне заняття	5
	T6	Практичне заняття №6	5	Практичне заняття №4	5
	T7	Практичне заняття №7	5	Практичне заняття №5	5
	T8	Практичне заняття №8	5	Практичне заняття №6	5
ПМК		Тест	10	Тест	10
Підсумко		Екзамен	40	Екзамен	40
Сума			100		100

9. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

На лекційних заняттях використовуються технічні засоби, а саме: комп'ютер, мультимедійний проектор або інтерактивна дошка. Якщо є можливість використання інтерактивної дошки або проектора, то наочні пояснення можна організувати таким чином: теоретичні відомості будуть наочно супроводжуватися демонстрацією на інтерактивній дошці (за наявності), або мультимедійному проекторі. Це дає можливість студенту не тільки почути, а й побачити, що сприяє більш ефективному засвоєнню нового матеріалу. Такі лекції є найдоступнішою і найцікавішою формою викладання нового матеріалу з навчальної дисципліни.

На практичних заняттях студенти використовують комп'ютери разом зі спеціалізованими стендами та тренажерами, та отримують навички ефективного використання сучасних апаратно-програмних засобів, що має забезпечити формування у студентів практичних навичок з вирішення завдань. Також комп'ютери використовуються для проведення поточного модульного контролю у формі тестування.

Навчально-методичні матеріали та технічні засоби навчання

1. Персональні комп'ютери.
2. Мережеве обладнання.
3. Навчально-методична література, рекомендована з дисципліни.

10. Рекомендовані джерела інформації

Основна література

1. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.

2. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. / В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМІТ», 2006. – 238 с. [1]. – 292 с. [2].

3. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / О.В. Рибальський, В.Г. Хахановський, В.В. Шорошев, О.І. Грищенко, С.В. Сторожев, М.В. Кобець. – К.: НАВСУ, 2003. – 160 с.

4. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.: “МК–Пресс”, 2005. – 288 с.

5. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.

6. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 2. Информационная безопасность. – 344 с.

Допоміжна література

8. Конституція України // Урядовий кур’єр, 13 липня 1996 р.

9. Закон України “Про основи національної безпеки України” // Урядовий кур’єр, 30 липня 2003 р.

10. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

11. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

12. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

13. Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.

14. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.

15. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.

16. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

17. Наказ МВС України від 14.07.1998 р. “Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”. – К., 1998.

Інформаційні ресурси в Інтернет

18. Threatpost. Режим доступу: <https://threatpos.com>

19. Geektimes. Режим доступу: <https://geektimes.com/hub/infosecurity>

Розробник:

Ст. викладач кафедри ПЕЕТ

A handwritten signature in black ink, appearing to be 'S.L. Tribulkevich', written over a horizontal line.

Трибулькевич С.Л.