ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра теоретичної фізики

«ЗАТВЕРДЖУЮ»
в.о. декана фізичного факультету
_____ Володимир ЛАЗУР
« _____» _____ 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ»

Рівень вищої освіти	**перший (бакалаврський)**
Галузь знань	**17 Електроніка та телекомунікації**
Спеціальність	**172 Телекомунікації та радіотехніка**
Освітня програма	**Телекомунікації та радіотехніка**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород – 2025

Робоча програма навчальної дисципліни «**Захист інформації в телекомунікаційних системах**» для здобувачів вищої освіти галузі знань **17 Електроніка та телекомунікації** спеціальності **172 Телекомунікації та радіотехніка** освітньої програми **Телекомунікації та радіотехніка**.

Розробник:
Нодь Є.А., канд. фіз.-мат. наук, доцент кафедри теоретичної фізики.

Робочу програму розглянуто та затверджено на засіданні кафедри теоретичної фізики

протокол № ____ від «_____» _____ 2025 р.

Завідувач кафедри _____ Мирослав КАРБОВАНЕЦЬ

Схвалено науково-методичною комісією фізичного факультету

протокол № ____ від «_____» _____ 2025 р.

Голова науково-методичної комісії _____ Василь РУБІШ

© Нодь Є. А., 2025 р.
© ДВНЗ «Ужгородський національний університет», 2025 р.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th>Розподіл годин за навчальним планом</th></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4,5</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 135</td><td>4-й</td></tr>
<tr><td>Кількість модулів – 2</td><td>Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин
для денної форми навчання :
аудиторних – 6
самостійної роботи студента – 6</td><td>8-й</td></tr>
<tr><td>Лекції:</td></tr>
<tr><td>36-год.</td></tr>
<tr><td>Практичні (семінарські):</td></tr>
<tr><td>30-год.</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:
залік</td><td>Лабораторні:</td></tr>
<tr><td>– -год.</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:
усна</td><td>Самостійна робота:</td></tr>
<tr><td>69-год.</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Захист інформації в телекомунікаційних системах»** є забезпечення предметної компетентності студентів спеціальності «**172 Телекомунікації та радіотехніка»** освітньої програми «**Телекомунікації та радіотехніка»** шляхом засвоєння основних знань і навиків необхідних для запобігання витоку, розголошенню, чи несанкціонованому оволодінню інформацією у телекомунікаційних системах. Даний курс дає змогу сформувати відповідний математичний та понятійний апарат необхідний для розуміння основ криптографічного захисту інформації, навчитися застосувати ці методи для розв'язання прикладних задач захищеної передачі інформації.

У результаті вивчення курсу студенти отримають відомості про сучасні математичні методи захисту (шифрування) інформації у процесі її передавання у телекомунікаційних системах та мережах.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ІК	Здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі телекомунікацій та радіотехніки, що характеризується комплексністю та невизначеністю умов
ЗК1	Здатність до абстрактного мислення, аналізу та синтезу
ЗК2	Здатність застосовувати знання у практичних ситуаціях.
ЗК4	Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК7	Здатність вчитися і оволодівати сучасними знаннями.
ФК1	Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства.
ФК2	Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки.
ФК3	Здатність використовувати базові методи, способи та засоби отримання, передавання, обробки та зберігання інформації.
ФК4	Здатність здійснювати комп'ютерне моделювання пристроїв, систем і процесів з використанням універсальних пакетів прикладних програм.
ФК8	Готовність сприяти впровадженню перспективних технологій і стандартів.
ФК14	Готовність до вивчення науково-технічної інформації, вітчизняного і закордонного досвіду з тематики інвестиційного (або іншого) проекту засобів телекомунікацій та радіотехніки.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни «**Захист інформації в телекомунікаційних системах**» є опанування таких навчальних дисциплін (НД) освітньої програми (ОП):

ОК 16 Програмування і математичне моделювання в інженерії
ОК 18 Теорія ймовірностей і математична статистика
ОК 26 Архітектура комп'ютера

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми «**Телекомунікації та радіотехніка**», вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Знання теорій та методів фундаментальних та загальноінженерних наук в об'ємі необхідному для розв'язання спеціалізованих задач та практичних проблем у галузі професійної діяльності.	ПРН1
Вміння застосовувати базові знання основних нормативно-правових актів та довідкових матеріалів, чинних стандартів і технічних умов, інструкцій та інших нормативно-розпорядчих документів у галузі електроніки та телекомунікацій.	ПРН2
Здатність брати участь у створенні прикладного програмного забезпечення для елементів (модулів, блоків, вузлів) телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення тощо.	ПРН4
Здатність брати участь у проектуванні нових (модернізації існуючих) телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення тощо.	ПРН7
Вміння застосовувати сучасні досягнення у галузі професійної діяльності з метою побудови перспективних телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення тощо.	ПРН8
Вміння адміністрування телекомунікаційних систем, інфокомунікаційних та телекомунікаційних мереж.	ПРН9

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Захист інформації в телекомунікаційних системах**»:

Очікувані результати навчання з дисципліни	Шифр ПРН
Знати теоретичні основи методів захисту інформації у телекомунікаційних системах та основні закономірності функціонування телекомунікаційних мереж.	ПРН1
Вміти застосовувати базові знання про законодавство України щодо захисту інформації в телекомунікаційних системах. Орієнтуватися в основних нормативно-правових актах, довідкових матеріалах, чинних стандартах і технічних умовах. Використовувати інструкції та інші нормативно-розпорядчі документи у галузі електроніки та телекомунікацій.	ПРН2
Вміти створити прикладного програмного забезпечення для елементів (модулів, блоків, вузлів) телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення тощо.	ПРН4
Знати принципи проектування та модернізації телекомунікаційних, інфокомунікаційних, радіотехнічних систем, а також систем телевізійного й радіомовлення з урахуванням вимог інформаційної безпеки. Вміти застосовувати знання щодо захисту інформації при розробці та вдосконаленні телекомунікаційних мереж і систем.	ПРН7
Знати сучасні технології та інженерні рішення, що застосовуються для побудови телекомунікаційних, інфокомунікаційних, радіотехнічних систем і мереж з урахуванням вимог захисту інформації. Вміти впроваджувати засоби інформаційної безпеки на етапах проектування, модернізації та експлуатації телекомунікаційних систем.	ПРН8
Знати принципи адміністрування телекомунікаційних систем, інфокомунікаційних та телекомунікаційних мереж, а також вимоги до забезпечення їх інформаційної безпеки. Вміти здійснювати налаштування, моніторинг і підтримку телекомунікаційної інфраструктури з урахуванням заходів захисту інформації та відповідних нормативних стандартів.	ПРН9

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

– поточний контроль успішності: стандартизовані тести, презентації результатів виконаних завдань та досліджень, захист лабораторних робіт;
– модульний контроль;
– підсумковий контроль;
– залік.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю:

– вибіркове усне опитування перед початком занять;
– перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів;
– оцінювання якості та повноти виконання лабораторних робіт;
– оцінювання якості та повноти виконання завдань модульної контрольної роботи.

Форма модульного контролю: поточне оцінювання та виконання модульної контрольної роботи у письмовій формі, сумарний результати яких оцінюються за 100-бальною шкалою за кожний модуль.

Підсумковий контроль навчальної діяльності студентів здійснюється у формі заліку за результатами поточного контролю.

8 семестр

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	**60**	**100**
5	5	6	6	6	6	6		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	**60**	**100**
5	5	6	6	6	6	6		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кіль-кість	Максимальна кількість балів (сумарна)	Кіль-кість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	7	40	6	40
Модульна контрольна робота	1	60	1	60
Разом	**8**	**100**	**7**	**100**

Критерії оцінювання модульної контрольної роботи

Виконання модульних контрольних робіт здійснюється в письмовій (або електронній) формі. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

При визначенні оцінки за модуль враховуються результати модульного контрольного оцінювання та поточного контролю під час навчальних занять, результати лабораторних робіт, самостійної та індивідуальної роботи.

На виконання письмового компонента модульного контрольного оцінювання відводиться 2 академічних годин. Здобувач освіти, який не з’явився на модульний контроль, може пройти його додатково у визначений кафедрою термін.

Модульна контрольна робота містить теоретичну і практичну частини, оцінюється у 60 балів. Теоретична частина – 20 балів. Практична частина – 40 балів.

Підсумкова модульна оцінка з навчальної дисципліни визначається як середнє арифметичне результатів усіх модульних контролів та виставляється за 100-бальною шкалою, шкалою ЄКТС та національною шкалою.

Здобувач, який за результатами модульних контролів отримав від 0 до 34 балів, повинен до проведення підсумкового семестрового контролю покращити цю оцінку принаймні до показника не менше 35. Без такого покращення він до семестрового контролю не допускається.

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни «**Захист інформації в телекомунікаційних системах**» здійснюється у формі заліку. Залік проводиться в усній формі шляхом співбесіди. Результати заліку оцінюються за двобальною шкалою: "зараховано" або "незараховано". Підсумкова оцінка визначається наступними критеріями.

Оцінка "зараховано" – якщо студент достатньо чітко і грамотно відповідає на питання в межах матеріалу, викладеного у рамках лекційних занять, може показати та обґрунтувати взаємозв'язок різних частин матеріалу,

пройденого у межах матеріалу навчальної дисципліни; демонструє здатність до мислення, при відповіді на питання розмірковує, спираючись на отримані у рамках курсу знання, не допускає істотних неточностей у відповіді, правильно вибудовує логіку вирішення типових завдань;

Оцінка "незараховано" – якщо студент викладає основні питання недостатньо чітко або допускає істотні помилки при їх викладі, не може пояснити зв'язків у рамках викладеного матеріалу, не знає значної частини програмного матеріалу, не може дати точних визначень понять, пройдених у рамках курсу, дає розпливчасті формулювання і не володіє в належній мірі термінологією, плутається при відповіді на додаткові питання, не володіє прийомами вирішення типових завдань.

За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Шкала оцінювання: національна та ECTS

Шкала ЄКТС	Диференційована шкала	Недиференційована шкала	Мін.бал-макс.бал
A	Відмінно	Зараховано	90-100
B	Добре		82-89
C			74-81
D	Задовільно		64-73
E			60-63
Fx	Незадовільно	Не зараховано	35-59
F			0-34

Здобувач, який отримав за результатами підсумкового контролю оцінку "незараховано" (0-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни і скласти залік.

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

СЕМЕСТР 8

Модуль 1

Тема 1. *Законодавство України про захист інформації в телекомунікаційних системах***.**

Вступ, загальні положення та нормативно-правова база захисту інформації. Законодавство України про захист інформації. Організація захисту інформації на підприємстві.

Тема 2. *Загальні поняття про кодування інформації.*

Загальні поняття про кодування інформації, "наївні" методи кодування, формальна криптографія, роторні криптосистеми, сучасні криптографічні методи кодування. Поняття про інформаційний канал (канал передачі інформації), обчислення пропускної здатності інформаційного каналу. Проблема узгодження коду з пропускною здатністю каналу передачі інформації.

Тема 3. *Необхідні відомості з розділів дискретної математики та теорії чисел.*

Оцінка складності виконання арифметичних операцій. Подільність цілих чисел. Алгоритм подільності Евкліда. Знаходження найбільшого спільного дільника (НСД) за допомогою алгоритму Евкліда.

Тема 4. *Математичні основи криптографії.*

Модульна арифметика. Порівняння за модулем. Дискретний логарифм цілого числа за модулем. Квадрат числа за модулем.

Тема 5. *Основи криптології, криптографії та криптографічного аналізу.*

Роль криптографічних протоколів у загальній задачі забезпечення інформаційної безпеки. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз. Класифікація методів шифрування повідомлень. Криптографічний аналіз.

Тема 6. *Традіційні історичні шифри.*

Шифри підстановки. Моноалфавітні шифри підстановки. Багатоалфавітні шифри підстановки. Шифри перестановки. Шифри перестановки без використання ключа. Шифри перестановки з використанням ключа.

Тема 7. *Принципи побудови сучасних симетричних криптографічних систем.*

Сучасні блокові шифри. Шифри підстановки та транспозиції. Блокові шифри як групові математичні перестановки. Компоненти сучасного блокового шифру. Складені шифри. Розсіювання й перемішування. Раунди. Два класи складених шифрів. Атаки на блокові шифри. Диференціальний криптографічний аналіз. Лінійний криптографічний аналіз.

Модуль 2

Тема 1. *Потокові шифри й генератори псевдовипадкових чисел.*

Загальні відомості про потокові шифри. Принципи використання генераторів псевдовипадкових чисел під час потокового шифрування. Класифікація потокових шифрів. Потоковий шифр *A5*. Потоковий шифр *RC4*.

Тема 2. *Стандарт симетричного алгоритму блокового шифрування даних.*

Принципи побудови алгоритму. Структура алгоритму шифрування даних. Генерація раундових ключів. Видалення бітів перевірки ключової послідовності. Циклічний зсув уліво послідовностей *Ci* і *Di*.. Об'єднання послідовностей *Ci* і *Di*, їх перестановка та стиснення. Функція *DES*.

Тема 3. *Режими виконання алгоритмів блокового симетричного шифрування даних.*

Режим виконання "Електронна кодова книга". Режим виконання "Зчеплення блоків зашифрованих даних". Режими виконання "Зворотний зв'язок".

Тема 4. *Симетричний алгоритм блокового шифрування даних.*

Структура алгоритму шифрування даних. Генерація раундових ключів. Процес шифрування даних. . Аналіз шифру *IDEA*. Уразливість ключа шифру.

Тема 5. *Асиметричні криптографічні системи шифрування.*

Перша криптографічна система з відкритим ключем – система Діффі–Хеллмана. Криптографічна система Шаміра. Криптографічна система Ель-Гамаля. Криптографічна система *RSA*. Криптографічна система Рабіна. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні

Тема 6. *Квантові алгоритми захисту інформації.*

Необхідні відомості з квантової механіки. Квантова суперпозиція станів, кубіти, однокубітні перетворення. Заплутаність станів, нерівність Белла. Поняття про квантові вентилі (квантові гейти). Контрольований NOT гейт.

Тема 7. *Недоліки класичної криптографії і поява квантової криптографії.*

Квантові ключі, розподіл квантових ключів. Квантова аутентифікація. Теорема про неможливість абсолютного копіювання (клонування) довільного невідомого квантового стану (No-Cloning theorem).

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Форма навчання					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
8-й семестр						
Модуль 1						
Тема 1. Законодавство України про захист інформації в телекомунікаційних системах.	6	2				4
Тема 2. Загальні поняття про кодування інформації.	8	2	2			4
Тема 3. Необхідні відомості з розділів дискретної математики та теорії чисел.	8	2	2			4
Тема 4. Математичні основи криптографії.	10	2	2			6
Тема 5. Основи криптології, криптографії та криптографічного аналізу.	10	2	2			6
Тема 6. Традиційні історичні шифри.	12	4	2			6
Тема 7. Принципи побудови сучасних симетричних криптографічних систем.	10	2	4			4
Модульна контрольна робота	2	2				
Разом за модуль 1	66	18	14			34
Модуль 2						
Тема 1. Потокові шифри й генератори псевдовипадкових чисел.	14	4	4			6
Тема 2. Стандарт симетричного алгоритму блокового шифрування даних.	8	2	2			4
Тема 3. Режими виконання алгоритмів блокового симетричного шифрування даних.	8	2	2			4
Тема 4. Симетричний алгоритм блокового шифрування даних.	9	2	2			5
Тема 5. Асиметричні криптографічні системи шифрування.	10	2	2			6
Тема 6. Квантові алгоритми захисту	10	2	2			6

інформації.						
Тема 7. Недоліки класичної криптографії і поява квантової криптографії.	8	2	2			4
Модульна контрольна робота	2	2				
Разом за модуль 2	69	18	16			35
Разом	**135**	**36**	**30**			**69**

6.3. Теми практичних занять

№ з/п	Назва теми	Кіль-кість годин
1	Законодавство України про захист інформації в телекомунікаційних системах.	_
2	Загальні поняття про кодування інформації.	2
3	Необхідні відомості з розділів дискретної математики та теорії чисел.	2
4	Математичні основи криптографії.	2
5	Основи криптології, криптографії та криптографічного аналізу.	2
6	Традіційні історичні шифри.	2
7	Принципи побудови сучасних симетричних криптографічних систем.	4
8	Потокові шифри й генератори псевдовипадкових чисел.	4
9	Стандарт симетричного алгоритму блокового шифрування даних.	2
10	Режими виконання алгоритмів блокового симетричного шифрування даних.	2
11	Симетричний алгоритм блокового шифрування даних.	2
12	Асиметричні криптографічні системи шифрування.	2
13	Квантові алгоритми захисту інформації.	2
14	Недоліки класичної криптографії і поява квантової криптографії.	2
	Разом	**30**

6.4. Самостійна робота

№ з/п	Назва теми	Кіль-кість годин
1	Законодавство України про захист інформації в телекомунікаційних системах.	4
2	Загальні поняття про кодування інформації.	4
3	Необхідні відомості з розділів дискретної математики та теорії чисел.	4
4	Математичні основи криптографії.	6
5	Основи криптології, криптографії та криптографічного аналізу.	6
6	Традіційні історичні шифри.	6
7	Принципи побудови сучасних симетричних криптографічних систем.	4
8	Потокові шифри й генератори псевдовипадкових чисел.	6
9	Стандарт симетричного алгоритму блокового шифрування даних.	4
10	Режими виконання алгоритмів блокового симетричного шифрування даних.	4
11	Симетричний алгоритм блокового шифрування даних.	5
12	Асиметричні криптографічні системи шифрування.	6
13	Квантові алгоритми захисту інформації.	6
14	Недоліки класичної криптографії і поява квантової криптографії.	4
	Разом	**69**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби та обладнання: мультимедійний проектор, комп‘ютер.

Обладнання: персональні комп’ютери, ноутбуки, планшети, веб-камери.

Програмне забезпечення: MS Power Point, MS Excel, Python, математичні пакети прикладних програм Mathcad, Matlab.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с
2. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
3. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп’ютерних системах: підручник. – Ніжин: ФОП Лук’яненко В.В., ТПК «Орхідея», 2020. – 236с.
4. Інформаційна безпека в комп’ютерних мережах: навч. посіб. / О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов [та ін.]; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. – Кропивницький: Лисенко В.Ф., 2020. – 295 с.
5. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації : Навчальний посібник. – Л.: Новий світ-2000, 2021. – 678 с.
6. Захист інформації в комп’ютерних системах : підручник / уклад. О. М. Гапак, С. І. Балога; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.
7. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
8. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

Допоміжна література

1. Державні стандарти України: ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
2. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в КС від НСД
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в КС від НСД
4. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.