НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра автоматики, електроніки та телекомунікацій

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної та навчальної роботи
_____ А.М. Мартиненко
«_30_» ___08_____ 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«МЕТОДИ ТА АЛГОРИТМИ ДЛЯ ЗАХИСТУ ДИСКРЕТНОЇ ІНФОРМАЦІЇ»

(назва навчальної дисципліни)

підготовки **магістра**
(назва ступеня вищої освіти)

спеціальності **172 Електронні комунікації та радіотехніка**
(код і назва спеціальності)

Полтава
2024 рік

Робоча програма навчальної дисципліни «Методи та алгоритми для захисту дискретної інформації» для студентів спеціальності 172 «Електронні комунікації та радіотехніка», другого (магістерського) рівня вищої освіти. Складена відповідно до освітньої програми «Телекомунікаційні системи та мережі», 2024 року.

Розробник: Фомін О.С., к.т.н., доцент кафедри автоматики, електроніки та телекомунікацій.

Погоджено

Гарант освітньої програми _____ Олександр ШЕФЕР

Робоча програма затверджена на засіданні кафедри автоматики, електроніки та телекомунікацій

Протокол від «19» серпня 2024 року №1

Завідувач кафедри автоматики, електроніки та телекомунікацій_____Олександр ШЕФЕР

«19» серпня 2024 року

Схвалено навчально-методичною комісією навчально-наукового інституту інформаційних технологій і робототехніки

Протокол від «19» серпня 2024 року №1

Голова навчально-методичної комісії навчально-наукового інституту інформаційних технологій і робототехніки_____Олександр ШЕФЕР

«19» серпня 2024 року

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">форма навчання</td></tr>
<tr><td>денна</td><td>дистанційна</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="2">Галузь знань
17
Електроніка, автоматизація та електронні комунікації</td><td colspan="2" rowspan="2">обов’язкова</td></tr>
<tr><td>Загальна кількість годин – 150</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="6">Спеціальність
172
Електронні комунікації та радіотехніка</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Індивідуальне завдання – курсова робота</td><td rowspan="11">Ступінь вищої освіти

магістр</td><td>28 год.</td><td>0</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>0</td><td>0</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>22 год.</td><td>0</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>70 год.</td><td>120 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота:</td></tr>
<tr><td colspan="2">30 год.</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

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

для денної форми навчання – 50/100
для дистанційної форми навчання – 0/150

2. Мета навчальної дисципліни

Мета: формування знань і вмінь студентів щодо принципів функціонування та характеристик мережевих служб дискретної інформації, принципів, методів та алгоритмів захисту дискретної інформації при побудові та експлуатації телекомунікаційної інфраструктури.

Компетентності за ОПП:

ІК – Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі електронних комунікацій та радіотехніки.
ЗК1 – Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4 – Навички використання інформаційних і комунікаційних технологій у професійній діяльності.
ЗК7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8 – Здатність приймати обґрунтовані рішення.
ФК 1 – Здатність використовувати принципи та концепції побудови телекомунікаційних систем та мереж у поєднанні з потрібними математичними інструментами вищого рівня для опису інфокомунікацій.
ФК 8 – Здатність розв'язувати задачі забезпечення надійності й інформаційної безпеки телекомунікаційних систем і мереж.
ФК 9 – Володіння принципами організації збереження даних, їх оперативної аналітичної обробки; здатність виявляти в даних раніш невідому інформацію, необхідну для прийняття рішень у різних сферах професійної діяльності.

3. Передумови для вивчення дисципліни

Попередньо опанована дисципліна: «Вища математика».

4. Очікувані результати навчання з дисципліни

ПР 2 – Використовувати принципи та концепції побудови телекомунікаційних систем та мереж у поєднанні з потребіним математичним апаратом.
ПР 4 – Застосовувати сучасні ІТ в професійній діяльності.
ПР 7 – Організовувати захист інформації в інфокомунікаційних мережах, здійснювати адміністрування інфокомунікаційних мереж, впроваджувати, налагоджувати та адмініструвати мережеве та інше системне програмне забезпечення.
ПР 12 – Застосовувати знання вимог законодавчої бази стосовно особливостей інформаційної безпеки на підприємствах інноваційної діяльності; базових моделей керування доступом; видів та механізмів контролю рівня безпеки.

5. Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом вивчення навчальної дисципліни.

Мінімальний порогів рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати в мінімальну позитивну оцінку числової (рейтингової) шкали.

Сума балів	Значення ЄКТС	Оцінка за національною шкалою	Критерій оцінювання	Рівень компетентності
90 – 100	**A**	**Відмінно**	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дис-	**Високий**, що повністю забезпечує

			ципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін.	вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82 – 89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній**, що забезпечує здобувачу самостійне вирішення основних практичних задач.
74 - 81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.
64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.
60 – 63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень і володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використанням	**Середній,** що є мінімально допустимим у всіх складових навчальної дисципліни.

			основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	
35 - 59	**FX**	**Незадовільно** з можливістю повторного складання екзамену/ диф.заліку	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних і лабораторних робіт в більшості є неправильними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький**, не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни.
0 – 34	**F**	**Незадовільно** з обов'язковим повторним вивченням дисципліни	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний**, здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є:
- екзамен;
- виконання завдань на лабораторних заняттях;
- курсова робота.

7. Програма навчальної дисципліни

Змістовий модуль 1. Основи теорії інформації та криптографії.

Тема 1. Основи поняття теорії інформації та криптографії.

Модель системи з криптозахистом. Класифікація криптосистем. Методи криптоаналіза і типи атак. Мінімальні довжини ключів.

Лабораторне заняття №1.

Тема 2. Історія розвитку криптографічних методів захисту дискретної інформації.

Способи приховування інформації у стародавні часи. Криптографія середньовіччя. Становлення криптографії як науки у XX столітті.

Лабораторне заняття №2.

Змістовий модуль 2. Методи та алгоритми захисту дискретної інформації.

Тема 3. Класичні шифри.

Моноалфавітні шифри. Біграмні шифри заміни. Поліграмний шифр заміни Хіл-Ла. Шифр гамування Віженера. Криптоаналіз поліалфавітних шифрів.

Лабораторне заняття №3.

Тема 4. Досконала криптостійкість інформаційних систем.

Визначення та умови досконалої криптостійкості. Криптосистема Вернама. Відстань єдиності.

Лабораторне заняття №4.

Тема 5. Блокові шифри.

Вступ та класифікація. SP-мережі. Проект «Люцифер». Комірка Фейстеля. Шифр DES. Стандарт шифрування США AES.

Лабораторне заняття №5.

Тема 6. Генератори псевдовипадкових чисел.

Лінійний конгруентний генератор. Регістр зсуву з лінійним зворотним зв'язком. Криптографічно стійкі генератори псевдовипадкових чисел.

Лабораторне заняття №6.

Тема 7. Потокові шифри.

Визначення потокового шифру та способи реалізації. Шифр RC4.

Лабораторне заняття №7.

Тема 8. Криптографічні хеш-функції.

Імітовставлення. Колізії у хеш-функціях. Ймовірність колізії. Комбінації хеш-функцій.

Лабораторне заняття №8.

Тема 9. Асиметричні криптосистеми.

Криптосистема RSA. Криптосистема Ель-Гамаля. Еліптичні криві. Довжини ключів. Інфраструктура відкритих ключів.

Лабораторне заняття №9.

Тема 10. Розповсюдження ключів. Поділ секрету.

Триетапний протокол Шаміра на комутативних шифрах. Симетричні протоколи. Асиметричні протоколи. Порогові схеми. Розподіл секрета по коаліціях.

Лабораторне заняття №10.

Тема 11. Стеганографія.

Основні терміни та визначення. Історичні приклади стеганосистем Математична модель та структурна схема стеганографічної системи. Класифікація контейнерів.

Тема 12. Реалізація систем захисту дискретної інформації.

Система Kerberos для локальної мережі. Pretty Good Privacy. Протокол SSL/TLS. Захист IPsec на мережному рівні.

Лабораторне заняття №11.

Тема 13. Автентифікація користувачів.

Багатофакторна автентифікація. Ентропія та криптостійкість паролів. Аутентифікація за паролем. Зберігання паролів та автентифікація в ОС. Аутентифікація у веб-сервісах.

Тема 14. Програмні вразливості.

Контроль доступу до інформаційних систем. Контроль доступу в ОС. Види програмних уразливостей. Міжсайтовий скриптинг. SQL-ін'єкції з виконанням коду базою даних інтернет-сервісу.

8. Структура навчальної дисципліни

а) для денної форми навчання

Назви змістових модулів і тем	Кількість годин					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1. Основи теорії інформації та криптографії						
Тема 1. Основи поняття теорії інформації та криптографії.	8	2		2		4
Тема 2. Історія розвитку криптографічних методів захисту дискретної інформації.	8	2		2		4
Разом за змістовим модулем 1	**16**	**4**		**4**		**8**
Змістовий модуль 2. Методи та алгоритми захисту дискретної інформації						
Тема 3. Класичні шифри.	10	2		2		6
Тема 4. Досконала криптостійкість інформаційних систем.	10	2		2		6
Тема 5. Блокові шифри.	10	2		2		6
Тема 6. Генератори псевдовипадкових чисел.	8	2		2		4
Тема 7. Потокові шифри.	8	2		2		4
Тема 8. Криптографічні хеш-функції.	8	2		2		4
Тема 9. Асиметричні криптосистеми.	8	2		2		4
Тема 10. Розповсюдження ключів. Поділ секрету.	10	2		2		6
Тема 11. Стеганографія.	36	2			30	4
Тема 12. Реалізація систем захисту дискретної інформації.	10	2		2		6
Тема 13. Автентифікація користувачів.	8	2				6
Тема 14. Програмні вразливості	8	2				6
Разом за змістовим модулем 2	**134**	**24**		**18**	**30**	**62**
Усього годин	**150**	**28**		**22**	**30**	**70**

б) для дистанційної форми навчання

Назви змістових модулів і тем	Кількість годин					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1. Основи теорії інформації та криптографії						
Тема 1. Основи поняття теорії інформації та криптографії.	8	-	-			8
Тема 2. Історія розвитку криптографічних методів захисту дискретної інформації.	8	-	-			8
Разом за змістовим модулем 1	**16**	-	-			**16**
Змістовий модуль 2. Методи та алгоритми захисту дискретної інформації						
Тема 3. Класичні шифри.	10	-	-			10
Тема 4. Досконала криптостійкість інформаційних систем.	10	-	-			10
Тема 5. Блокові шифри.	10	-	-			10
Тема 6. Генератори псевдовипадкових чисел.	10	-	-			10
Тема 7. Потокові шифри.	10	-	-			10
Тема 8. Криптографічні хеш-функції.	8	-	-			8
Тема 9. Асиметричні криптосистеми.	8	-	-			8
Тема 10. Розповсюдження ключів. Поділ секрету.	8	-	-			8
Тема 11. Стеганографія.	36	-	-		30	6
Тема 12. Реалізація систем захисту дискретної інформації.	8	-	-			8
Тема 13. Автентифікація користувачів.	8	-	-			8
Тема 14. Програмні вразливості	8	-	-			8
Разом за змістовим модулем 2	**134**	-	-		**30**	**104**
Усього годин	**150**	-	-		**30**	**120**

9. Перелік питань для семінарських занять

№ заняття	Назва питань	Кількість годин	
		для денної форми	для дистанційної форми
	Семінарські заняття не передбачені		

10. Перелік питань для практичних занять

№ заняття	Назва питань	Кількість годин	
		для денної форми	для дистанційної форми
	Практичні заняття не передбачені		

11. Перелік питань для лабораторних занять

№ заняття	Назва питань	Кількість годин	
		для денної форми	для дистанційної форми
1	Дослідження шифру простої заміни та його криптоаналіз	2	-
2	Дослідження шифру заміни і перестановки	2	-
3	Дослідження блокового шифру	2	-
4	Дослідження асиметричного шифру	2	-
5	Дослідження шифру Віжинера	2	-
6	Дослідження криптографічних хеш-функцій	2	-
7	Дослідження гасло-шифру	2	-
8	Дослідження RSA шифрування	2	-
9	Дослідження алгоритму SHA256	2	-
10	Дослідження алгоритмів генерації і верифікації електронного цифрового підпису	2	-
11	Дослідження криптографічного алгоритму на основі еліптичних кривих	2	-
	Разом	**22**	-

12. Самостійна робота

Метою самостійної роботи студентів є додаткове вивчення принципів, методів та алгоритмів захисту мережевих служб дискретної інформації, що не охоплені лекційним курсом та лабораторними заняттями. Студент повинен уміти користуватись науково-технічною літературою, державними та міжнародними стандартами, іншими джерелами, а також самостійно використовувати навики та вміння, одержані при вивченні дисципліни.

Види самостійної роботи студента:

- опрацювання лекційного матеріалу;
- підготовка до лабораторних занять;
- опрацювання тем курсу, які виносяться на самостійне вивчення, за списками літератури, рекомендованими в робочій навчальній програмі дисципліни, та іншими джерелами;
- підготовка до тестування;
- відвідування консультацій;
- курсова робота;
- підготовка до складання екзамену.

Питання
для самостійного вивчення студентами

№ з/п	Назва питань	Кількість годин	
		для денної форми	для дистанційної форми
1	Основи поняття теорії інформації та криптографії	4	8
2	Історія розвитку криптографічних методів захисту дискретної інформації	4	8
3	Класичні шифри	6	10
4	Досконала криптостійкість інформаційних систем	6	10
5	Блокові шифри	6	10
6	Генератори псевдовипадкових чисел	6	10
7	Потокові шифри	6	10
8	Криптографічні хеш-функції	4	8
9	Асиметричні криптосистеми	4	10
10	Розповсюдження ключів. Поділ секрету	6	10
11	Реалізація систем захисту дискретної інформації.	6	10
12	Автентифікація користувачів	6	8
13	Програмні вразливості	4	8
	Разом	**70**	**120**

13. Індивідуальні завдання

Загальний обсяг часу на виконання курсової роботи складає 30 годин. За цей час студент виконує самостійну роботу за темою «Дослідження алгоритмів захисту дискретної інформації на основі стеганографії», яка має за мету навчити студентів застосовувати здобуті знання при розв’язуванні конкретної технічної задачі у галузі захисту дискретної інформації.

Під час виконання роботи рекомендується користуватися методичними рекомендаціями для курсової роботи з дисципліни «Методи та алгоритми для захисту дискретної інформації» для студентів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіотехніка» Національного університету «Полтавська політехніка імені Юрія Кондратюка».

14. Методи навчання

При викладанні дисципліни застосовуються словесні, наочні та практичні методи навчання.

Словесні і наочні використовуються під час лекцій та інструктажів, практичні – при проведенні лабораторних занять.

Під час проведення лекцій використовуються такі словесні методи як розповідь, пояснення та наочні методи; ілюстрація, демонстрація.

Перед проведенням лабораторних занять викладачами проводяться інструктажі: вступні, поточні, підсумкові.

Під час проведення лабораторних занять застосовуються наочні спостереження та словесні бесіди: вступні, поточні, репродуктивні, евристичні, підсумкові; студентами виконуються вправи; тренувальні, творчі, усні, практичні, технічні.

15. Методи контролю

Поточний контроль успішності засвоєння студентами навчального матеріалу може здійснюватися шляхом опитування й оцінювання знань студентів під час лабораторних занять, оцінювання виконання студентами самостійної роботи та індивідуальних завдань, проведення і перевірки письмових контрольних робіт, тестування або в ході індивідуальних співбесід зі студентами під час консультацій. Вибір конкретних форм і методів поточного контролю знань студентів залежить від викладача і доводиться до їхнього відома на першому лабораторному занятті. Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння студентом певної сукупності знань та вмінь, що формують відповідний модуль. Він реалізується шляхом проведення спеціальних контрольних заходів (у формі тестування чи написання студентами контрольних робіт), проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять або самостійної роботи для дистанційної форми навчання, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу студентів. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація).

Підсумковий контроль здійснюється у формі семестрового екзамену.

16. Розподіл балів, які отримують студенти

Поточне оцінювання, тестування, самостійна та індивідуальна робота															**Семестровий екзамен**	**Сума**
Змістовий модуль 1		***Змістовий модуль 2***												Індиві-дуальні завдання		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14			
3	3	3	3	3	3	4	4	4	4	4	4	4	4	0	50	100

Курсова робота оцінюється за окремою 100-бальною шкалою.

Пояснювальна записка	**Захист роботи**	**Сума**
50	50	100

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою для екзамену, диференційованого заліку, курсового проекту (роботи), практики
90 – 100	**A** – відмінно	**5** – відмінно
82 – 89	**B** – дуже добре	**4** – добре
74 – 81	**C** – добре	
64 – 73	**D** – задовільно	**3** – задовільно
60 – 63	**E** – достатньо	
35 – 59	**FX** – незадовільно з можливістю повторного складання	**2 –** незадовільно
0 – 34	**F** – незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них:

– при підсумковому контролі у вигляді екзамену 50 балів відведено на поточний контроль, а 50 балів – на підсумковий (для допуску до екзамену необхідно мати не менше 25 балів поточної успішності).

1. Поточний контроль. Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином:

- робота на лабораторних заняттях (усні відповіді, виконання практичних завдань, захист лабораторних робіт, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять) – до 50 балів.

Присутність на лекціях не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів. При тривалій відсутності студента на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

Студент, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (не менше 25 балів), допускається до підсумкового контролю з дисципліни.

2. Підсумковий контроль Підсумковим контролем є екзамен. Він здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті імені Юрія Кондратюка».

17. Методичне забезпечення

1. Фомін О.С. Курс лекцій з дисципліни «Методи та алгоритми для захисту дискретної інформації» для студентів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіотехніка» Національного університету «Полтавська політехніка імені Юрія Кондратюка», 2024 р. – 250 с.
2. Фомін О.С. Методичні рекомендації для лабораторних занять з дисципліни «Методи та алгоритми для захисту дискретної інформації» для студентів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіотехніка» Національного університету «Полтавська політехніка імені Юрія Кондратюка», 2024 р. – 85 с.
3. Фомін О.С. Методичні рекомендації для курсової роботи з дисципліни «Методи та алгоритми для захисту дискретної інформації» для студентів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіотехніка» Національного університету «Полтавська політехніка імені Юрія Кондратюка», 2024 р. – 20 с.

18. Рекомендована література

Базова

1. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. - Київ: Ліра-К, 2023. - 483 с.
2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту - Київ : Ліра-К, 2024. - 554 с.
3. Присяжнюк М.М., Рідей Н.М., Титова Н.М. Інформаційна безпека та кібербезпека держави. Навчальний посібник - Ліра-К, 2024. - 224 с.

Допоміжна

1. Мельник І., Лунтовський А. Проектування та дослідження комп'ютерних мереж. – Київ: Університет «Україна», 2010. – 362 с.
2. Мельник І., Лунтовський А. Комп'ютерні мережі та телекомунікації. – Київ: Університет «Україна», 2007. – 274 с.

3. Blum R., Bresnahan C. Linux command line and shell scripting bible. – Wiley, 2021. – 832 p.

4. Шульга В. П.,Іванченко Є. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 2024 р., 3(59) - 6-19 с.

5. Гаврилова А. А., Король О. Г., Воропай Н. І., Севрюкова Є. О., Бондаренко К. О. Аналіз методів криптографічної автентифікації та виявлення маніпуляцій для великих даних. Сучасний захист інформації, 2024 р., 1(57) - 97-102 с.

6. Laptiev, O., Tkachev, V., Maystrov, O., Krasikov, O., Open'ko, P., Khoroshko, V., Parkhuts, L.The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). Vol 13, No 2, August 2021 P.271-277. ISSN: 2073-607X (Online). DOI:10.54039/ijcnis.v13i2.5008 https://www.ijcnis.org/index.php/ijcnis/article/view/5008.

7. Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. The Cyber Defense Review, 87–102. https://www.jstor.org/stable/26846122.

8. Florian Klaus Kaisera, Tobias Budiga, Elisabeth Goebela, Tessa Fischera, Jurek Muffa, Marcus Wiensa and Frank Schultmanna. Attack Forecast and Prediction. C&ESAR'21: Computer Electronics Security Application Rendezvous, November 16-17, 2021, Rennes, France.

9. Jones, M., Kotsalis, G., Shamma, J.S. (2013). Cyber Attack Forecast Modeling and Complexity Reduction Using a Game-Theoretic Framework. In: Tarraf, D. (eds) Control of Cyber-Physical Systems. Lecture Notes in Control and Information Sciences, vol 449. Springer, Heidelberg. https://doi.org/10.1007/978-3-319-01159-2_4.

10. Ganjali, A., Marwat, S. S., & Sifalakis, M. (2012). Critical infrastructure protection: A mathematical modeling perspective. Journal of Network and Systems Management, 20(1), 128-144.

19. Інформаційні ресурси

1. Сторінка курсу на платформі Moodle: https://dist.nupp.edu.ua/course/view.php?id=6145