Міністерство освіти і науки України
Національний університет кораблебудування
імені адмірала Макарова
Херсонський навчально-науковий інститут

Кафедра інформаційних технологій
та фізико-математичних дисциплін

Т7136

ЗАТВЕРДЖУЮ
Заступник директора з
навчальної роботи

_____ к.т.н., проф. Дудченко О.М.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Programming Basics

рівень вищої освіти *перший (бакалаврський)*

тип дисципліни *обов'язкова*

мова викладання *українська*

Херсон - 2023 рік

Робоча програма навчальної дисципліни “Безпека програм та даних” є однією із складових комплексної підготовки фахівців галузі знань 12 - “Інформаційні технології”
спеціальність 121 - “Інженерія програмного забезпечення”
освітня програма “Інженерія програмного забезпечення”.

“26” серпня 2023 року. – 19 с.

Розробник: Притула В.М., ст. викладач кафедри інформаційних технологій та фізико-математичних дисциплін

Проєкт робочої програми навчальної дисципліни “Безпека програм та даних” узгоджено з гарантом освітньої програми

Гарант освітньої програми “Інженерія програмного забезпечення”
д.пед.н., к.ф.-м.н., проф. _____ М.Б. Літвінова

Проєкт робочої програми навчальної дисципліни “Безпека програм та даних” розглянуто на засіданні кафедри інформаційних технологій та фізико-математичних дисциплін

Протокол № 07 від “28” серпня 2023 р.
Завідувач кафедри_____ П. Й. Гучек

Робоча програма навчальної дисципліни “Безпека програм та даних” затверджена методичною радою ХННІ НУК.

Протокол № 01 від “29” серпня 2023 р.
Голова МР ХННІ НУК _____ О.М. Дудченко

Зміст

ВСТУП

Анотація

Дисципліною “Безпека програм та даних” передбачено набуття студентами знань про типові алгоритми, структуру програмних одиниць, принципи створення програмного забезпечення, а також вмінь обирати та використовувати необхідні мові та програмні засоби та методи програмування для розв'язування конкретних задач, що виникають в процесі створення програмного забезпечення.

Програма навчальної дисципліни “Безпека програм та даних” розрахована на студентів, які вивчили математику, фізику та основи інформатики. Програма передбачає комплексне застосування набутих компетенцій для розв’язання прикладних задач. Опанування курсу надає професійні компетенції для подальшого вивчення дисциплін професійної підготовки.

Дисципліна “Безпека програм та даних” носить міждисциплінарний характер, вона забезпечує підготовку студентів до вивчення навчальних дисциплін “Моделювання програмного забезпечення”, “Архітектура та проектування програмного забезпечення”, “Організація та технології передачі даних у комп'ютерних мережах” та “Якість програмного забезпечення та тестування”.

Ключові слова: алгоритм, програмування, типи даних, структури даних, безпека.

Annotation

The discipline “Software and Data Security” provides students with knowledge of typical algorithms, structure of software units, principles of software development, as well as the ability to choose and use the necessary languages, software tools and programming methods to solve specific problems in the software development process.

The program of the discipline “Software and Data Security” is designed for students who have studied mathematics, physics and basics of computer science. The program provides a comprehensive application of the acquired competencies to solve applied problems. Mastering the course provides professional competencies for further study of disciplines.

The discipline “Software and Data Security” is interdisciplinary, it prepares students to study the disciplines “Software Modeling”, “Software Architecture and Design”, “Organization and technology of data transmission in computer networks” and “Software Quality and testing”.

Keywords: algorithm, programming, data types, data structures, security.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність (освітня програма), освітній рівень</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</td><td>Галузь знань
12 - “Інформаційні технології”</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів - 2</td><td rowspan="6">Спеціальність
121 - “Інженерія програмного забезпечення (освітня програма) “Інженерія програмного забезпечення”</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів - 2</td><td>3-й</td><td>3-й</td></tr>
<tr><td>Електронна адреса на сайті ХННІ НУК: http://kb.nuos.edu.ua/Licensing%20and%20accreditation%20specialties/b-software-ingineering.html</td><td colspan="2"></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання “Розв’язання прикладних задач на комп’ютері”</td><td colspan="2"></td></tr>
<tr><td>Загальна кількість годин - 90</td><td colspan="2">Семестри</td></tr>
<tr><td></td><td>6-й</td><td>6-й</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних:
6-й семестр – 3
самостійної роботи студента:
6-й семестр – 3</td><td rowspan="8">Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Лекції</td></tr>
<tr><td>6-й семестр – 15 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>6-й семестр – 30год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>6-й семестр – 45 год.</td><td>72 год.</td></tr>
<tr><td colspan="2">Види контролю:
6-й семестр – Екзамен</td></tr>
<tr><td colspan="2">Форма контролю: комбінована (письмовий контроль, тестовий контроль)</td></tr>
</table>

2. Мета навчальної дисципліни

2.1 Метою вивчення навчальної дисципліни “Безпека програм та даних” є формування у студентів згідно зі Стандартом вищої освіти України, затвердженим Наказом Міністерства освіти і науки України від 29.10.2018 №1166 таких компетентностей:

Інтегральна компетентність

– здатність розв’язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення для розв’язання на ЕОМ задач, пов’язаних з програмуванням різних структур даних і їх організації у пам’яті та зовнішніх носіях у ЕОМ.

Загальні компетентності

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення.

К23. Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.

К24. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

К25. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

3. Передумови для вивчення дисципліни

Передумовами для вивчення даної дисципліни є дисципліни: математика, фізика та основи інформатики в курсі середньої школи.

4. Очікувані результати навчання

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

ПР03. Знати основні процеси, фази та ітерації життєвого циклу програмного забезпечення..

ПР04. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.

ПР09. Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.

ПР10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування.

ПР11. Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання.

ПР12. Застосовувати на практиці ефективні підходи щодо проектування програмного забезпечення.

ПР14. Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.

ПР15. Мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення.

ПР19. Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.

ПР22. Знати та вміти застосовувати методи та засоби управління проектами.

5. Програма навчальної дисципліни

6-й семестр

Модуль 1.
Захист інформації, криптографія і криптоаналіз.

Змістовий модуль 1.1 Введення у захист інформації.

Тема 1. Основні концепції захисту інформації.
Джерела інформації: [4] – стор. 36-52.

Тема 2. Криптографія і криптоаналіз, потокові і блокові шифри.
Джерела інформації: [4] – стор. 203-213.

Змістовий модуль 1.2 Шифри. Алгоритми.

Тема 3. Сучасні алгоритми симетричного шифрування.
Джерела інформації: [2] – стор. 313-322.

Тема 4. Принципи побудови криптосистем з відкритим ключем.
Джерела інформації: [3] – стор. 153-212; [5] – стор. 87 -116.

Модуль 2.

Коди та протоколи і програмування систем безпеки.

Змістовий модуль 2.1 Коди. Цифрові підписи та протоколи.

Тема 5. Коди автентичності повідомлень та функції хешування.
Джерела інформації: [4] – стор. 316-332.

Тема 6. Цифрові підписи та протоколи автентифікації.
Джерела інформації: [4] – стор. 343-354.

Змістовий модуль 2.2 Програмна реалізація ПЗ та аналіз безпеки.

Тема 7. Програмна реалізація криптографічних алгоритмів, безпека прикладних програм.
Джерела інформації: [4] – стор. 333-341.

Тема 8. Моделювання загроз ПЗ, методи безпечної реалізації ПЗ.
Джерела інформації: [5] – стор. 410-422.

Тема 9. Методи і засоби аналізу безпеки ПЗ.
Джерела інформації: [5] – стор. 425-436.

5.1 Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
1	2	3	4	6	5	6	7	8
6-й семестр								
Модуль 1								
Змістовний модуль1. Захист інформації, криптографія і криптоаналіз								
Тема 1. Основні концепції захисту інформації.	9	1	2	6				9
Тема 2. Криптографія і криптоаналіз, потокові і блокові шифри.	12	2	4	6				9
Тема 3. Сучасні алгоритми симетричного шифрування.	12	2	4	6				9
Тема 4. Принципи побудови криптосистем з відкритим ключем.	12	2	4	6				9
Разом за змістовим модулем 1	**45**	**7**	**14**	**24**	**45**	**4**	**5**	**36**
Модуль 2								
Змістовний модуль 2. Коди та протоколи і програмування систем безпеки.								
Тема 5. Коди автентичності повідомлень та функції хешування.	9	1	4	4				7
Тема 6. Цифрові підписи та протоколи автентифікації.	9	1	4	4				7
Тема 7. Програмна реалізація криптографічних алгоритмів, безпека прикладних програм.	10	2	4	4				7
Тема 8. Моделювання загроз ПЗ, методи безпечної реалізації ПЗ.	10	2	4	4				7
Тема 9. Методи і засоби аналізу безпеки ПЗ.	7	2	-	5				8
Разом за змістовим модулем 2	**45**	**8**	**16**	**21**	**45**	**4**	**5**	**36**

Примітка. Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до таблиці (розд. 4).

5.2 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
6-й семестр		
1	Програмування процедур роботи зі стеками. Джерела інформації: [1-3] , робота 1.	7
2	Програмування процедур роботи з чергами. Джерела інформації: [1-4] , робота 2.	7
3	Програмування процедур роботи зі списками. Джерела інформації: [1-4] робота 3.	8
4	Програмування процедур роботи з деревами. Джерела інформації: [1-4], робота 4.	8
Разом		30

5.3 Самостійна робота та індивідуальні завдання

№ з/п	Назва теми	Кількість годин
6-й семестр		
1	Моделі загроз безпеки програмного забезпечення	4
2	Формальні методи доказу правильності програм і їх специфікації	4
3	Конфіденційні обчислення	4
4	Самотестуючи і само корегуючи програми	4
5	Захист програм і забуванне моделювання на RAM-машинах	4
6	Кріптопрограмування за допомогою використання інкрементальних алгоритмів	4
7	Захист програм від автоматічної генерації інструментальними засобами програмних закладок	4
8	Методи ідентифікації програм	4
9	Методи і засоби захисту програм від комп'ютерних вірусів	4
10	Методи захисту програмного забезпечення від дослідження коду	3
11	Методи і засоби забезпечення цілісності та достовірності використовуваного програмного коду	3
12	Підходи до захисту програм від несанкціонованого копіювання	3
Разом		45

Під час виконання індивідуальних завдань студент повинен закріпити теоретичний лекційний та практичний матеріал, навчитися самостійно працювати з літературою, складати програми виходячи з поставленої задачі.

Кожне завдання з лабораторної роботи виконується студентом індивідуально за консультативною допомогою викладача. Усі лабораторні роботи виконуються з використанням персонального комп'ютера.

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

Методи навчання:

для всіх видів занять:

- робота з літературою - опрацювання різних видів джерел, спрямоване на формування нових знань, їх закріплення, вироблення вмінь і навичок та реалізацію контрольно-корекційної функції в умовах формальної освіти;

для лекційних занять:

- лекція - усний виклад навчального матеріалу, який характеризується великим обсягом, складністю логічних побудов, сконцентрованістю розумових образів, доведень і узагальнень;
- відеометод - використання відеоматеріалів для активізації наочно-чуттєвого сприймання; забезпечує більш легке і міцне засвоєння знань в їх образно-понятійній цілісності та емоційній забарвленості;

для лабораторних занять:

- лабораторна робота - метод поглиблення і закріплення теоретичних знань шляхом створення програм і отримання результатів роботи програми з використанням комп'ютерів;
- інструктаж - ознайомлення зі способами виконання завдань, інструментами, матеріалами, технікою безпеки та організацію робочого місця.

Засобами оцінювання та методами демонстрування результатів навчання є:

- звіти з виконання лабораторної роботи та презентації результатів виконаних лабораторних робіт на комп'ютері (або письмовий контроль результатів);
- усні відповіді на лабораторних заняттях;
- поточні модульні контрольні роботи у формі тестування (тестовий контроль);
- екзамен.

7. Методи контролю

При вивченні дисципліни студентам рекомендується використовувати основну та додаткову літературу, конспект лекцій, а також джерела з мережі Internet.

Навчальний процес вивчення дисципліни складається з 2 модулів. При вивченні дисципліни проводиться поточний та підсумковий модульний контроль.

7.1 Поточний контроль

Поточний контроль охоплює:

- якість виконання та захисту лабораторних робіт;
- терміни захисту лабораторних робіт;
- пропуски лекційних та лабораторних занять.

Кількість залікових балів за виконання лабораторних робіт встановлюється відповідно складності і складає від 15 до 25 балів. Максимальна кількість балів відповідає виконанню лабораторних робіт та їх захисту без помилок у встановлений термін, мінімальна – з допустимими помилками із захистом пізніше встановленого терміну.

8. Форми поточного та підсумкового контролю

Досягнення студента оцінюються за 100-бальною системою Університету.

Підсумкова оцінка навчального курсу включає в себе оцінки з поточного контролю і оцінки заключного іспиту.

Питома вага заключного іспиту в загальній системі оцінок – ***40 балів***. Право здавати заключний іспит дається студенту, якій з урахуванням максимальних балів проміжних оцінок і заключного іспиту набирає не менше ***60 балів***. Підсумкова оцінка навчального курсу є сумою проміжних оцінок і оцінки іспиту.

Поточний контроль проводиться на кожному лабораторному занятті та за результатами виконання завдань самостійної роботи. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) під час виконання завдань лабораторних робіт.

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8.1 Форми контролю результатів навчальної діяльності студентів та їх оцінювання

Критерії оцінювання лабораторних робіт

Бал	Критерії оцінювання
5	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані цілі, завдання та гіпотеза досліджень. Застосовувалися коректні методи обробки отриманих результатів. У висновках проведена коректна інтерпретація результатів.
4	Робота виконана у встановлений термін. Студент виконує лабораторну роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; в цілому правильно складає звіт та робить висновки.
3	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; складає звіт, що містить неточності у висновках та помилки.
2	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну згідно з інструкцією; складений звіт містить неточності у висновках та помилки.
1	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну під керівництвом викладача; складений звіт містить неточності у висновках та помилки.
0	Робота не виконувалася

8.2 Підсумковий модульний контроль

Підсумковий модульний контроль проводиться по завершенні вивчення усіх модулів поточного семестру. До підсумкового модульного контролю студент допускається при умові виконання усіх елементів відповідних модулів та одержання не менше ніж 50 балів поточного контролю.

Якщо за результатами поточного контролю студент набрав не менше 60 балів, він може бути звільненим від складання підсумкового семестрового контролю.

Якщо студент бажає підвищити підсумкову оцінку, він має можливість виконати додаткові завдання, або скласти семестровий екзамен.

Підсумковий модульний контроль складається з теоретичних та практичних питань. За відповідь на теоретичні питання без помилок, або з одною незначною помилкою студент отримує максимальну оцінку. За неповні відповіді або відповіді з помилками, знижується кількість отриманих балів. При неправильній відповіді або при відсутності відповіді бали не нараховуються.

За всі контрольні заходи протягом семестру студент може отримати від 0 до 100 балів.

8.3 Розподіл балів, які отримують студенти

Можливі поточні бали за виконання кожної лабораторної роботи та необхідна кількість балів для зарахування модуля наведені в наступній таблиці.

При виконанні роботи з декількома незначними помилками оцінка знижується на 1-3 бали. При допущені грубих помилок робота повинна бути виконана повторно.

При виконанні і поданні лабораторної роботи до захисту пізніше встановленого терміну без поважних причин оцінка знижується на 1 бал за кожний тиждень після терміну захисту.

За кожне пропущене лекційне або лабораторне заняття без поважних причин нараховується по 1 штрафному балу.

Модуль	Змістовний модуль	Сума залікових балів	Тема	№ ЛР	Поточні бали за виконання ЛР	Необхідна кількість балів для зарахування модуля
6-й семестр						
1	1	30 - 50	Т1	1	15 – 25	30
			Т2			
			Т3	2	15 – 25	
			Т4			
2	2	30 - 50	Т5	3	15 – 25	30
			Т6			
			Т7	4	15 – 25	
			Т8			
			Т9			

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

Оцінка знань студентів в залежності від набраної суми балів формується у відповідності до наступної шкали, в якій представлено відповідність між набраними балами, оцінкою ECTS та традиційною системою:

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
82-89	**B**	добре
74-81	**C**	
64-73	**D**	задовільно
60-63	**E**	
35-59	**FX**	незадовільно з можливістю повторного складання

0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни

Критерії оцінювання поточного модульного контролю знань у формі тестування

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
6-й семестр										
Бал	20	18	16	14	12	10	8	6	4	2

Критерії оцінювання контрольної роботи (для заочної форми)

Бал	Критерії оцінювання
20	Робота виконана у встановлений термін. Матеріал викладено у достатньому обсязі, аргументовано і у правильній послідовності. Під час захисту роботи студент вільно орієнтується в матеріалах.
15	Робота виконана у встановлений термін. Матеріал викладено у достатньому обсязі, але частка програм наведена без результатів розрахунків. Під час захисту роботи студент вільно орієнтується в матеріалах.
10	Робота виконана з порушенням встановлених термінів. Матеріал викладено у правильній послідовності, але недостатньо повно, більша частка програм наведена без результатів розрахунків. Під час захисту роботи студент слабо орієнтується в матеріалах.
0	Роботу не виконано.

Критерії оцінювання підсумкового контролю та екзамену

Бал	Критерії оцінювання
40	Студент склав програму самостійно без помилок та відповідає на теоретичні питання без помилок
30	Студент склав програму самостійно без помилок, але відповіді на теоретичні питання не повні
20	Студент розуміє алгоритм, але склав програму, яка працює не правильно, проте відповідає на теоретичні питання без помилок
10	Студент не розуміє алгоритм, не склав програму, але відповідає на теоретичні питання без помилок
0	Студент не розуміє алгоритм, не склав програму і не відповідає на теоретичні питання без помилок

Узагальнюючі результати поточного контролю знань

Форма контролю	Максимальна кількість балів	
	Денна форма	Заочна форма
6-й семестр		
Виконання лабораторних робіт	4 роб. × 10 балів = 40 балів	4 роб. × 10 балів = 40 балів
Поточний модульний контроль	1 МКР × 20 балів = 20 балів	-
Виконання контрольних робіт	-	1 роб. × 20 балів = 20 балів
Всього	**60**	**60**

10. Критерії оцінювання результатів навчання

Змістовий модуль	Тема	Денна форма		Заочна форма	
		Вид роботи	Бали	Вид роботи	Бали
1	**2**	**3**	**4**	**5**	**6**
6-й семестр					
ЗМ 1	Т1-Т2	Лабораторна робота № 1	10	Лабораторна робота № 1	10
	Т3-Т4	Лабораторна робота № 2	10	Лабораторна робота № 2	10
ЗМ 2	Т5-Т6	Лабораторна робота № 2	10	Лабораторна робота № 2	10
	Т7-Т9	Лабораторна робота № 3	10	Лабораторна робота № 3	10
	Т1-Т9	Поточний модульний контроль	20	-	-
	Т1-Т9	-	-	Контрольна робота	20
Підсумковий контроль		Екзамен	40	Екзамен	40
Сума			**100**		**100**

11. Засоби навчання

Технічні засоби навчання: мультимедійний проектор, персональні комп'ютери з підключенням до мережі Інтернет.

При проведенні занять за дистанційною формою навчання (у період карантину) використовуються дистанційні платформи й інформаційно-комунікаційні технологій (Moodle, Google Classroom, DingTalk, ZOOM Cloud Meetings, Skype, Viber, WeChat, Telegram, соціальні мережі тощо).

12. Рекомендовані джерела інформації

Основна література

1. Stallings B. Cryptography And Network Security, 7Th Edition.: Publisher PEARSON INDIA, Publication Date January 1, 2017. – 672 с.
2. Сенів М. М., Яковина В. С. Безпека програм та даних Навчальний посібник. Львів : Видавництво Львівської політехніки, 2015. Код: 978-617-607-836-4 256 с.
3. Вишня В. Б. В 55 Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. ISBN 978-617-7665-08-2 128 с.
4. Кавун С. В. К12 Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 200. УДК 004.056(075.8) ББК 32.973я73 — 352 с.
5. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». Запоріжжя : ЗНУ, 2022. 72 с.

Допоміжна література

5. Кібербезпека: криптографія з PYTHON. / Євсеєв С.П. , Король О.Г. , Шматко О.В. Видавництво: Новий світ-2000 Рік видання: 2021 . — 120 с.
6. Лагун А.Е. Криптографічні системи та протоколи. — Видавництво: Львівська політехніка. Рік видання: 2013 — 96 с.
7. Молдован А.А, Молдован Н.А., Советов Б.Я. Криптография. — СПб.: «Лань», 2000. — 224 с.
8. Остапов С.Е., Євсеєв С.П., Король О.Г.. Кібербезпека: сучасні технології захисту. — Видавництво: Новий світ-2000, 2020. — 678 с.
9. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення. — Видавництво: Гельветика, 2017. — 548 с.

10. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 с.

Інформаційні ресурси в інтернет

Сайт ХННІ НУК: http://kb.nuos.edu.ua

Розробник
ст. викладач  Притула В.М.

Додаток

Питання для модульного контролю

6-й семестр

Контрольні питання до 1-го модуля

1. Які основні концепції захисту інформації?
2. Що таке криптографія?
3. Що таке стеганографія?
4. Яке бувають шифри?
5. Який алгоритм симетричного шифрування?
6. Який алгоритм несиметричного шифрування?
7. Що таке системи з відкритим ключем?
8. Що таке системи симетричного шифрування?
9. Які принципи побудови криптосистем вважаються сучасними?
10. Які використовують шифри?
11. Що таке криптоаналіз?

Контрольні питання до 2-го модуля

1. Що таке коди?
2. Які методи автентифікації ви знаете?
3. Що таке функції хешування?
4. Що таке цифрові підписи?
5. Що таке протоколи автентифікації?
6. Опишіть криптографічний алгоритм?
7. Як програмно реалізуються криптографічні алгоритми?
8. Що таке безпека прикладних програм?
9. Що таке моделювання загроз ПЗ?
10. Де використовують методи безпечної реалізації ПЗ?
11. Яки методи аналізу безпеки ПЗ ви знаєте?
12. Яки засоби аналізу безпеки ПЗ ви знаєте?

.