

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
 НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
 імені адмірала Макарова
 Навчально-науковий інститут автоматики та електротехніки
 Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП
 ПП21



ЗАТВЕРДЖЕНО

Проректор
 з науково-педагогічної роботи
 Слободян С. О.
 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

ЗАХИСТ ПРОГРАМНОГО ПРОДУКТУ
SOFTWARE PRODUCT SECURITY

Рівень вищої освіти перший (бакалаврський)
 Тип дисципліни обов'язкова
 Мова викладання українська

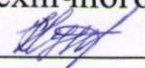
Галузь знань 12 Інформаційні технології
 Спеціальність 125 Кібербезпека
 Освітньо-професійна програма Системи технічного захисту інформації, автоматизації її обробки

Робоча програма навчальної дисципліни «Захист програмного продукту» є однією зі складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» за освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки»

«___»_____ 2022 р. – 15 с.

Розробник: к.т.н., доц. Козирев С. С., доцент кафедри комп'ютерних технологій та інформаційної безпеки (КТІБ).

Проект робочої програми навчальної дисципліни «Захист програмного продукту» узгоджено з гарантом освітньої програми.

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки», к.т.н., доцент  С. М. Нужний

Проект робочої програми навчальної дисципліни «Захист програмного продукту» розглянуто на засіданні кафедри КТІБ.

Протокол від «18» 04 2022 р. № 9.

Завідувач кафедри КТІБ, к.т.н., доцент  С. М. Нужний

Проект робочої програми навчальної дисципліни «Захист програмного продукту» розглянуто методичною радою Навчально-наукового інституту автоматики і електротехніки.

Протокол від «21» 04 2022 р. № 9.

/Голова, к.т.н., доцент  В. А. Скороходов

Проект робочої програми навчальної дисципліни «Захист програмного продукту» погоджено з навчальним відділом.

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

Робочу програму навчальної дисципліни «Захист програмного продукту» затверджено Навчально-методичною радою НУК.

Протокол від «27» 04 2022 р. № 3.

Голова НМР НУК, к.т.н., доцент  С.О. Слободян

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета вивчення навчальної дисципліни.....	6
3. Передумови для вивчення навчальної дисципліни	6
4. Очікувані результати навчання.....	6
5. Програма навчальної дисципліни.....	6
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	11
7. Форми поточного та підсумкового контролю.....	12
8. Критерії оцінювання результатів навчання.....	13
9. Засоби навчання	14
10. Рекомендовані джерела інформації.....	14

ВСТУП

Анотація

Навчальна дисципліна «Захист програмного продукту» є дисципліною професійної підготовки бакалаврів зі спеціальності 125 «Кібербезпека». Вона забезпечує формування вміння створення захищених, алгоритмічно безпечних програмних продуктів для використання в критичних інформаційних системах.

Основним завданням навчальної дисципліни є вивчення теоретичних та прикладних аспектів захисту програмних продуктів різного призначення. Засвоєння оптимальних методів керування розробкою й механізмів контролю якості програмних продуктів на кожному етапі життєвого циклу, починаючи з постановки завдання й закінчуючи авторським супроводом. Основна увага приділяється здобуттю практичних навичок розробки захищених, алгоритмічно безпечних програмних продуктів з використанням методів технологічного та експлуатаційного захисту для використання в критичних інформаційних системах.

Ключові слова: програмний продукт, технологічний та експлуатаційний захист, життєвий цикл програмного продукту, критичні інформаційні системи.

Abstract

The course "Software Product Security" is the discipline of the bachelor degree of the specialties 125 "Cybersecurity". It provides the formation of the ability to create secure, algorithmically safe software products for use in critical information systems.

The main task of the course is the study of theoretical and applied aspects of security of software products of various purposes. Acquiring the knowledge of optimal methods for managing the development and mechanisms of quality assurance of software products at each life cycle stage, starting from problem definition and ending with product support. The focus is on obtaining practical skills for the development of secure, algorithmically safe software products using technological and operational protection techniques for use in critical information systems.

Key words: software product, technological and operational security, software life cycle, critical information systems.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 3,0	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека Освітня програма: Системи технічного захисту інформації, автоматизація її обробки	Обов’язкова	
Модулів – 1		Рік підготовки	
Змістових модулів – 3		4-й	4-й
Електронна адреса РПНД на сайті Університету: http://education.nuos.edu.ua/		Семестр	
Загальна кількість годин – 90		8-й	8-й
		Лекції	
Тижневих годин для денної форми навчання: аудиторних – 3 год.; самостійної роботи студента – 3 год.		15 год.	4 год.
		Практичні, семінарські	
		–	–
		Лабораторні роботи	
		30 год.	6 год.
		Самостійна робота	
		45 год.	80 год.
		Індивідуальне завдання не передбачено	
Освітній рівень: перший (бакалаврський)		Вид контролю: залік	
	Форма контролю: тестування		

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Захист програмного продукту» є формування у студентів відповідно до освітньо-професійної програми таких компетентностей:

Загальні компетентності:

ЗК 2 Знання та розуміння предметної області та розуміння професії.

Фахові компетентності:

ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

3. Передумови для вивчення навчальної дисципліни

Передумовами для вивчення навчальної дисципліни є наступні дисципліни:

- Теорія інформації, кодування та цифрова обробка інформації;
- Криптографія та стеганографія;
- Методи і засоби захисту інформації.

4. Очікувані результати навчання

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

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Загрози безпеці програмних продуктів (ПП) та принципи забезпечення надійного захисту

Тема 1 (Лекція 1). Аналіз і класифікація загроз безпеці програмних продуктів. Базові етапи життєвого циклу програмних продуктів. [1], С. 6-26; [5, 7, 8, 9, 10].

Перелік питань, що виносяться на вивчення за темою:

Рівень безпечності програмних продуктів. Причини функціональної непридатності програмних продуктів. Критичні інформаційні системи. Способи деструктивного впливу на програмний продукт. Класифікація загроз безпеці програмних продуктів. Тактичні й стратегічні загрози. Руйнівні програмні засоби (РПЗ). Алгоритмічні та програмні закладки. Комп'ютерні віруси. Поліморфні програмні загрози. Базові етапи життєвого циклу (ЖЦ) програмних продуктів (ПП). Каскадна та ітераційна моделі життєвого циклу програмних продуктів. Стандартизація життєвих циклів програмних продуктів. Технологічна частина ЖЦ: системний аналіз, проектування, розробка, тестування та випробування ПП. Експлуатаційна частина ЖЦ.

Тема 2. Модель загроз і принципи забезпечення надійного захисту. Технологічні етапи розробки систем захисту ПП. [1], С. 27-45; [5, 6, 8, 10].

Лекція 2.1. Модель загроз і принципи забезпечення надійного захисту.

Перелік питань, що виносяться на вивчення:

Схема загроз технологічній безпеці ПП. Модель експлуатаційної безпеки ПП. Неформалізований опис моделі загроз ПП. Принципи забезпечення технологічної безпеки при плануванні. Принципи забезпечення технологічної безпеки в процесі розробки. Принципи забезпечення безпеки при стендових випробуваннях та експлуатації програмних продуктів.

Лекція 2.2. Технологічні етапи розробки систем захисту ПП.

Перелік питань, що виносяться на вивчення:

Етапи процесу проектування й розробки систем захисту ПП: виявлення цілей і завдань, визначення відповідного рівня захисту, аналіз можливих і ймовірних загроз безпеці ПП, визначення стратегії захисту, вибір оптимального захисту, розробка й оптимізація алгоритму захисту, програмна реалізація системи захисту ПП і її тестування.

Змістовий модуль 2. Забезпечення технологічного захисту програмних продуктів в процесі розробки

Тема 3 (Лекція 3). Механізми захисту програмних продуктів в процесі розробки. Методи створення алгоритмічно безпечних програмних продуктів. Види і алгоритми обфускації (obfuscation – заплутування). [1], С. 46-68; [6, 7, 8, 12].

Перелік питань, що виносяться на вивчення за темою:

Механізми захисту: використання складних логічних процедур; шифрування коду ПП; комбіновані системи. Алгоритми захисту: заплутування; мутації, компресії; шифрування. Протистояння технічних методів і засобів розробників систем захисту і зловмисників. Основні вимоги до сучасних систем

захисту ПП. Обфускація як метод створення алгоритмічно безпечних програмних продуктів, що дозволяє ускладнити процес реверсивної інженерії коду ПП. Аналітичні та емпіричні методи оцінки ефективності обфускації. Класифікація видів обфускації, залежно від способу модифікації коду програми: лексична, обфускація даних, обфускація керування, превентивна. Процес деобфускації.

Тема 4 (Лекція 4). Криптопрограмування на основі інкрементальних алгоритмів. Методологія самотестування та самокорекції ПП. Методи ідентифікації та аналізу безпечності ПП. [1], С. 68-88; [2, 4, 7, 9, 11].

Перелік питань, що виносяться на вивчення за темою:

Мета та ідея інкрементальної криптографії. Криптографічні алгоритми. Основні елементи інкрементальної криптографії. Оператори модифікації. Інкрементальні алгоритми. Методологія самотестування. Програми самотестування. Програми самокорекції. Застосування програм з самотестуванням та самокорекцією. Ідентифікація програм за внутрішніми характеристиками. Контрольно-випробні й логіко-аналітичні методи аналізу безпечності ПП. Моделі ПП та РПЗ. Види аналізу ПП: лексичний верифікаційний, синтаксичний верифікаційний, семантичний аналіз.

Змістовий модуль 3. Забезпечення експлуатаційного захисту програмних продуктів

Тема 5 (Лекція 5). Методи і засоби захисту від комп'ютерних вірусів та програмних закладок. [1], С. 89-107; [3, 5, 8, 10].

Перелік питань, що виносяться на вивчення за темою:

Загальна характеристика комп'ютерних вірусів. Властивості комп'ютерних вірусів. Структура комп'ютерного вірусу. Класифікація комп'ютерних вірусів за режимом функціонування, за об'єктом вторгнення, за ступенем і способом маскування. Способи інфікування. Ефекти, викликані вірусами в процесі реалізації ними цільових функцій. Наслідки дії вірусів. Загальна характеристика засобів нейтралізації комп'ютерних вірусів. Групи антивірусних програм: детектори, фаги, вакцини, щеплення, ревізори, монітори. Класифікація методів захисту від комп'ютерних вірусів. Проактивні технології боротьби з комп'ютерними вірусами.

Тема 6 (Лекція 6). Методи захисту програмних продуктів від злому та несанкціонованого копіювання. [1], С. 107-126; [5, 8, 10].

Перелік питань, що виносяться на вивчення за темою:

Забезпечення цілісності й достовірності ПП. Методи захисту програм від несанкціонованих змін: використання надлишкових даних, криптографічні методи, метод віртуального процесора. Криптографічні засоби контролю цілісності й вірогідності програм. Базові поняття й визначення криптології. Електронний (цифровий) підпис. Хеш-функції. Криптографічні протоколи. Апаратні засоби захисту від копіювання. Електронні ключі (HASP). Енергонезалежна пам'ять (EEPROM). Основні методи програмного захисту від копіювання. Криптографічні методи захисту від копіювання. Метод прив'язки до ідентифікатора. Методи, засновані на роботі з переходами й стеком. Методи протидії динамічним способам зняття захисту програм від копіювання.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усьо- го	у тому числі				усього	у тому числі			
		л	п	лаб	с.р.		л	п	лаб	с.р.
Модуль 1 (М1)										
Змістовий модуль 1. Загрози безпеці програмних продуктів (ПП) та принципи забезпечення надійного захисту										
Тема 1. Аналіз і класифікація загроз безпеці програмних продуктів. Базові етапи життєвого циклу програмних продуктів.	10	2	-	2	6	15	1	-	1	13
Тема 2. Модель загроз і принципи забезпечення надійного захисту. Технологічні етапи розробки систем захисту ПП.	20	4	-	4	12	15	1	-	1	13
Разом за змістовим модулем 1	30	6	-	6	18	30	2	-	2	26
Змістовий модуль 2. Забезпечення технологічного захисту програмних продуктів в процесі розробки										
Тема 3. Механізми захисту програмних продуктів в процесі розробки. Методи створення алгоритмічно безпечних програмних продуктів. Види і алгоритми обфускації (obfuscation – заплутвання).	14	2	-	4	6	15	1	-	-	14
Тема 4. Крипто-програмування на основі інкрементальних алгоритмів. Методологія самотестування та самокорекції ПП. Методи ідентифікації та аналізу безпечності ПП.	16	2	-	8	8	15	1	-	2	12
Разом за змістовим модулем 2	30	4	-	12	14	30	2	-	2	26
Змістовий модуль 3. Забезпечення експлуатаційного захисту програмних продуктів										
Тема 5. Методи і засоби захисту від комп’ютерних вірусів та програмних закладок.	11	2	-	4	5	15	-	-	1	14
Тема 6. Методи захисту програмних продуктів від злому та несанкціонованого копіювання.	19	3	-	8	8	15	-	-	1	14
Разом за змістовим модулем 3	30	5	-	12	13	30	-	-	2	28
Разом за курсом	90	15	-	30	45	90	4	-	6	80

Примітка 1. Для студентів заочної форми навчання проводяться оглядові лекції, лабораторні заняття за темами змістових модулів в обсягах відповідно до таблиці (розд. 5).

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
Змістовий модуль 1			
1	Вступне заняття. Інструктаж з техніки безпеки. Доведення плану робіт, вимог до звітів, принципів оцінювання. Ознайомлення з обладнанням та програмним забезпеченням лабораторії.	2	-
2	Побудова моделі загроз експлуатаційній безпеці ПП інформаційної комп'ютерної системи (ІКС) навчальної лабораторії.	2	1
3	Визначення необхідних методів і засобів надійного захисту. Розробка системи захисту ІКС.	2	1
Змістовий модуль 2			
4	Захист програмних продуктів (ПП) з використанням алгоритмів обфускації (obfuscation – заплутування) за допомогою спеціалізованого програмного забезпечення.	4	-
5	Криптографічний захист. Створення відкритого зашифрованого тому за допомогою програми VeraCrypt.	2	1
6	Криптографічний захист. Створення прихованого зашифрованого тому за допомогою програми VeraCrypt.	2	-
7	Криптографічний захист. Перевірка роботи зашифрованих томів VeraCrypt в режимі захисту прихованого тому і без.	4	1
Змістовий модуль 3			
8	Аналіз і порівняльна характеристика функціональних можливостей антивірусних програм.	4	1
9	Розробка програмного коду для заборони несанкціонованого копіювання прикладної програми з використанням перевірки серійного номера або обсягу накопичувача.	4	1
10	Захист програмного продукту від несанкціонованого використання за допомогою програми AsProtect.	2	-
11	Злам захисту програмного продукту за допомогою програми Trial Reset.	2	-
Разом		30	6

Самостійна робота

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год./1 год. занять;
- підготовка до лабораторних робіт – 2-3 год./1 робота;
- підготовка до контрольних заходів – 15-30 год. на 1 захід.

Завдання для самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
Модуль 1			
1	Підготовка до лекцій	7,5	30
3	Підготовка до лабораторних робіт	22	35
5	Підготовка до модульних контрольних робіт та заліку	15,5	15
Разом		45	80

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

Методи навчання:

- лекція - усний виклад навчального матеріалу з використанням слайдів, інтернет-ресурсів, рекламних матеріалів виробників програмних продуктів, базових програмних засобів;
- робота з літературою - опрацювання різних видів джерел, спрямоване на формування нових знань у сфері захисту програмних продуктів, їх закріплення;
- лабораторна робота - вивчення в спеціалізованих лабораторіях методів і засобів захисту програмних продуктів з використанням спеціального програмного забезпечення.

Засоби оцінювання результатів навчання:

- звіти з лабораторних робіт;
- модульні контрольні роботи;
- поточне та підсумкове тестування;

Методи демонстрування результатів навчання:

- усні відповіді;
- виконання завдань на лабораторному комп'ютерному комплексі, пов'язаних із здобуттям навичок стосовно принципів, методів і засобів технологічного та експлуатаційного захисту програмних продуктів;
- проходження поточного та підсумкового тестування.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету. Підсумкова оцінка навчального курсу включає в себе оцінки з поточного та підсумкового контролю.

Форми поточного контролю:

- захист звітів з лабораторних робіт;
- модульні контрольні роботи у формі тестування;
- перевірка конспектів лекційного матеріалу.

Форми підсумкового контролю:

- залік у формі підсумкового тестування.

Форми контролю результатів навчальної діяльності студентів та їх оцінювання

Лабораторна робота	
Кількість балів	Критерії оцінювання
5	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках проведена коректна інтерпретація результатів.
4	Робота виконана у встановлений термін. Виконана самостійно згідно з інструкцією, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках при інтерпретації результатів допущено неточності.
3	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну згідно з інструкцією; складений звіт містить неточності у висновках.
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 з порушенням інструкції; складений звіт містить неточності у висновках та помилки.
0	Робота не виконувалася.
	<i>Максимальна кількість балів за даний компонент програми 55 балів (11 робіт по 5 балів).</i>

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

Підсумковий контроль (залік у формі тестування)

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

Форма контролю	Максимальна кількість балів
Виконання лабораторних робіт	11 x 5 балів = 55 балів
Поточний модульних контроль	2 x 10 балів = 20 балів
Перевірка конспектів лекційного матеріалу	5 балів
Залік у формі тестування	20 балів
Всього	100

8. Критерії оцінювання результатів навчання

		Вид роботи	Кількість балів
Змістовий модуль 1	Тема 1	Лабораторна робота № 1	5
	Тема 2	Лабораторна робота № 2, № 3	10
Поточний контроль		Тестування	10
Змістовий модуль 2	Тема 3	Лабораторна робота № 4	5
	Тема 4	Лабораторна робота № 5, № 6, № 7	15
Поточний контроль		Тестування	10
Змістовий модуль 3	Тема 5	Лабораторна робота № 8	5
	Тема 6	Лабораторна робота № 9, № 10, № 11	15
Перевірка конспектів лекційного матеріалу		Лекції за темами №1 ... №6	5
Підсумковий контроль		Залік у формі тестування	20
Сума			100

Шкала оцінювання: національна та ECTS

Сума балів за результатом підсумкового контролю	Оцінка ECTS	Оцінка за національною шкалою
90 – 100	A	Відмінно
82 – 89	B	Дуже добре
74 – 81	C	Добре
64 – 73	D	Посередньо
60 – 63	E	Достатньо
35 – 59	FX	Незадовільно з можливістю повторного складання
0 – 34	F	Незадовільно з обов'язковим повторним вивченням дисципліни

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер або ноутбук, підключені до локальної комп'ютерної мережі.

Прикладне програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає: ASProtect; Trial Reset; Vera Crypt; Kaspersky Anti-Virus; ESET Internet Security; Dr. Web Security Space; Bitdefender Internet Security; Avira Antivirus; Avast Antivirus; Symantec Norton 360, Mangle-It C++, Stunnix.

Використовуються апаратні та програмні можливості лабораторій №130, №129 кафедри КТІБ ННІАЕ НУК.

10. Рекомендовані джерела інформації

Основні джерела інформації

1. Блінцов В.С., Козирев С.С. Захист програмних продуктів // Навч. посібник (Лист МОН № 1/11-10917 від 30.11.2010 р.). – Миколаїв: НУК, 2010. – 146 с.
2. Блінцов В.С., Гальчевський Ю.Л. Практикум з криптології // Навч. посібник. – Миколаїв: НУК, 2005. – 172 с.
3. Безруков Н.Н. Компьютерные вирусы. – М.: Наука, 2001. – 159 с.
4. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології. – Миколаїв: НУК, 2006. – 232 с.
5. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу – К.: Вид-во Європ. ун-ту, 2001. – 321 с.
6. Гарбарчук В., Минович З., Свиц А. Кибернетический поход к проектированию систем защиты информации. – Киев – Луцк – Люблин, 2003. – 659 с.

7. Жоголев Е.А. Технология программирования. - М.: Научный мир, 2004. – 216 с.
8. Зегжда Д. П., Ивашко А. М. Основы безпеки інформаційних систем. – М.: Гаряча лінія Телекому, 2000. – 452 с.
9. Казарин О.В., Шубинский И.Б. Надёжность и безопасность программного обеспечения: Учеб. пособие для бакалаврата и магистратуры. – М.: Издательство Юрайт, 2018. – 342 с.
10. Казарин О.В. Безопасность программного обеспечения компьютерных систем. - Москва, МГУЛ, 2003. – 212 с.
11. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

Додаткові джерела інформації

12. Глушаков С.В., Хачиров Т.С., Соболев Р.О. Секреты хакера. Защита и атака. Харьков: Фолио, 2005. – 414с.
13. Горбенко І.Д., Гріненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах / Навч. Посібник, Ч.1 Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 368 с.
14. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО “ТИД ДС”, 2001.– 688 с.
15. Середа С. А. Процедура разработки систем программно-технической защиты программного обеспечения // Сборник научных трудов Академического Совета МЭСИ. - М. 2004, С. 160-173.

Інформаційні ресурси мережі Інтернет

1. VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. <https://veracrypt.fr/>
2. AsProtect 32 - packer for 32bit software with protection functions. <http://aspack.com/asprotect32.html>
3. Avast. <https://www.avast.ua/>
4. Kaspersky Cyber Security Solutions for Home & Business. <https://www.kaspersky.com/>
5. Stunnix C++ Obfuscator. <http://stunnix.com/>

Доцент кафедри КТІБ,
К.Т.Н., доц.

_____ С.С. Козирев