

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ  
В.о. декана факультету комп'ютерних  
інформаційних технологій



Інформаційний технолог ЯКИМЕНКО  
2023 р.

ЗАТВЕРДЖУЮ

Директор навчально-наукового інституту новітніх  
освітніх технологій

Святослав ЦИГЕЛЬ  
2023 р.



ЗАТВЕРДЖУЮ  
В.о. проректора з  
науково-педагогічної роботи



Віктор ОСТРОВЕРХОВ  
2023 р.

## РОБОЧА ПРОГРАМА

### з дисципліни «Безпека інформаційних систем»

Ступінь вищої освіти: бакалавр  
Галузь знань – 12 «Інформаційні технології»  
Спеціальність – 126 «Інформаційні системи та технології»  
Освітньо-професійна програма – «Інформаційні системи та технології»

Кафедра комп'ютерних наук

Форма навчання	Курс	Семестр	Лекції (год.)	Лаб. (год.)	ІРС (год.)	Тренінг, КПЗ	СРС (год.)	Разом (год.)	Екзамен (сем.)
Денна	IV	7	40	30	5	20	55	150	7
Заочна	IV	7	8	4	-	-	138	150	7,8

*Святослав Цигель*

Тернопіль – ЗУНУ  
2023

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 126 «Інформаційні системи та технології», затвердженої вченою радою ЗУНУ (протокол №\_\_ від «\_\_» \_\_\_\_\_ 202\_ р.).

Робочу програму склав доцент кафедри комп'ютерних наук, к.т.н.,  
Руслан ШЕВЧУК

Робоча програма затверджена на засіданні кафедри комп'ютерних наук, протокол №1 від 28 серпня 2023р.

Завідувач кафедри



Андрій ПУКАС

Розглянуто та схвалено групою забезпечення спеціальності «Інженерія програмного забезпечення», протокол №1 від 30 серпня 2023 р.

Голова групи  
забезпечення спеціальності



Андрій МЕЛЬНИК

Гарант ОП



Андрій МЕЛЬНИК

# СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Безпека інформаційних систем»

## 1. Опис дисципліни «Безпека інформаційних систем»

Дисципліна «Безпека інформаційних систем»	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів : Денна - 5 Заочна – 5	Галузь знань - 12 «Інформаційні технології»	Статус дисципліни: обов'язкова Мова навчання: українська
Кількість залікових модулів - 4	Спеціальність: 126 «Інформаційні системи та технології»	Рік підготовки: Денна – 4, Заочна – 4. Семестр: Денна – 7 Заочна – 11.
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: Денна – 40 год, Заочна – 8 год. Лабораторні роботи: Денна – 38 год, Заочна – 4 год.
Загальна кількість годин: Денна – 150 Заочна - 150		Самостійна робота: Денна – 55 год, тренінг – 4 год. Заочна – 138 год. Індивідуальна робота: Денна – 5 год.
Тижневих годин – 12 год., з них аудиторних – 6 год		Вид підсумкового контролю – екзамен

## 2. Мета й завдання вивчення дисципліни «Безпека інформаційних систем»

### 2.1. Мета вивчення дисципліни

Метою дисципліни «Безпека інформаційних систем» є надання студентам знань щодо сучасних стандартів, підходів, методів та засобів захисту інформаційних систем. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від несанкціонованого копіювання, захисту програмних засобів від дослідження.

Ця дисципліна відноситься до дисциплін циклу професійної та практичної підготовки. Знання основ дисципліни «Безпека інформаційних систем» на даний час одним із важливих показників рівня кваліфікації фахівця з програмної інженерії.

Студенти при вивченні дисципліни повинні сформуватись вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів, захищати інформацію персонального комп'ютера та розроблене програмне забезпечення, розробляти індивідуальні системи управління доступом і захистом інформації.

Вивчення курсу "Безпека інформаційних систем" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та лабораторних роботах, самостійної роботи та виконання індивідуальних завдань.

## **2.2. Завдання вивчення дисципліни**

У результаті вивчення курсу "Безпека інформаційних систем" студенти повинні знати:

- загальні відомості про захист програм та даних;
- стандарти галузі інформаційної безпеки;
- алгоритми ідентифікації та аутентифікації користувачів;
- алгоритми криптографічного захисту інформації;
- методи та засоби обмеження доступу до програм та даних
- класифікацію загроз інформації та міри протидії;
- класифікацію та особливості комп'ютерних вірусів;
- особливості захисту програм від досліджень;

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними відомостями щодо захисту інформації, потенційних загроз та проблем захисту програм та даних.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних понять захисту програм та даних;
- сформувати у студентів цілісну систему теоретичних знань з курсу "Безпека інформаційних систем".

Мета проведення лабораторних робіт полягає у тому, щоб виробити у студентів практичні навички захисту програм та даних від різного роду загроз.

Завдання проведення лабораторних робіт:

- ознайомити з методами захисту програм та даних;
- ознайомитись з сучасними засобами захисту програм та даних;
- отримання навиків програмуванні систем комплексного захисту інформації;
- глибше засвоїти та закріпити теоретичні знання, одержані на лекціях.

## **2.3 Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни «Безпека інформаційних систем»:**

- здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки;
- здатність, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

**2.4. Передумови для вивчення дисципліни** базуються на знанні таких дисциплін: «Алгоритми та структури даних», «Аналіз вимог до програмного забезпечення», «Архітектура та проектування програмного забезпечення», «Засоби програмування баз даних», «Архітектура комп'ютера», «Основи програмної інженерії».

### **2.5. Результати навчання**

У результаті вивчення курсу "Безпека інформаційних систем" студенти повинні:

- знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.
- знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

## **3. Програма навчальної дисципліни «БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»**

### **Змістовний модуль 1. Принципи безпеки та захисту інформації в ІС.**

#### **Тема 1. ОСНОВНІ ПОНЯТТЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ**

Предмет і задачі захисту ІС. Вразливість інформаційних систем. Політика безпеки в комп'ютерних системах. Оцінка та механізми захисту ІС. Стандарти захисту даних.

Література: 1-5, 7-10

#### **Тема 2. ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ**

Ідентифікація користувачів. Аутентифікація користувачів. Перевірка автентичності користувачів. Протоколи ідентифікації.

Література: 1,2,4

#### **ТЕМА 3. МОДЕЛІ РОЗПОВСЮДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

Моделі безоштовного ПЗ. Моделі умовно-безоштовного ПЗ. Моделі комерційного ПЗ. Хмарні моделі.

#### **Тема 4. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**

Основні поняття та визначання криптографічного захисту інформації. Симетричне та асиметричне шифрування. Цифрові підписи. Хеш-функції. Цифрові сертифікати. Технологія Blockchain.

Література: 1,4,7,9

### **Змістовний модуль 2. Основи побудови систем захисту інформації в ІС.**

#### **Тема 5. МЕТОДИ ТА ЗАСОБИ ОБМЕЖЕННЯ ДОСТУПУ ДО ІС**

Вразливість інформаційних систем. Способи проникнення до інформаційних систем. Спостереження за користувачами ІС. Особливості обмеження доступу до ІС.

Література: 1,4

## **Тема 6. ЗАХИСТ ПРОГРАМ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ**

Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

Література: 1,4,8

## **Тема 7. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ**

Поняття про віртуальні захищені (приватні) мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF

Література: 1,4

### **4. Структура залікового кредиту дисципліни „Безпека інформаційних систем”**

денна форма навчання \ заочна форма навчання	Кількість годин				
	Лекції	Лабораторні роботи	Самостійна робота	Індивідуальна робота	Контрольні заходи
<b>Змістовий модуль 1. Принципи безпеки та захисту інформації в ІС.</b>					
Тема 1. Основні поняття безпеки ІС	6/1	5/-	7/20	-	Усне опитування та тестування
Тема 2. Ідентифікація та аутентифікація користувачів	6/1	8/2	7/20	3/-	Усне опитування та тестування
Тема 3. Моделі розповсюдження програмного забезпечення	4/1	6/2	7/18	-	Усне опитування та тестування
Тема 4. Криптографічний захист інформації	6/2	6/-	9/20	2/-	Усне опитування та тестування
<b>Змістовий модуль 2. Основи побудови систем захисту інформації в ІС.</b>					
Тема 5. Методи та засоби обмеження доступу до ІС	6/1	5/-	7/20	-	Усне опитування та тестування
Тема 6. Захист програм та даних від несанкціонованого копіювання	6/1	5/-	9/20	-	Усне опитування та тестування
Тема 7. Віртуальні приватні мережі	6/1	5/-	9/20	-	Усне опитування та тестування
Разом	40/8	52/4	55 / 138	5/-	

## **5. Тематика лабораторних робіт**

### **Лабораторна робота №1 (5/- год.)**

Тема: Розмежування повноважень користувачів на основі парольної аутентифікації

Мета: Розробка програми розмежування повноважень користувачів на основі парольного аутентифікації.

### **Лабораторна робота №2 (8/2 год.)**

Тема: Логування дій користувачів у програмних системах.

Мета: Засвоїти методику та отримати практичні навички розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонаправленими хеш-функціями.

### **Лабораторна робота №3 (6/2 год.)**

Тема: Методи захисту програмного забезпечення.

Мета: Одержати практичні навички реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження.

### **Лабораторна робота №4 (6/- год.)**

Тема: Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA.

Мета: отримати практичні навички реалізації механізму CAPTCHA.

### **Лабораторна робота №5 (5/- год.)**

Тема: Аналіз захищеності веб-ресурсів

Мета: Отримати практичні навички аналізу захищеності веб-ресурсів, формування аналітичного звіту та рекомендацій щодо усунення виявлених вразливостей..

### **Лабораторна робота №6 (5/- год.)**

Тема: Особливості захисту даних за допомогою технології Blockchain

Мета: Формування вмінь і навиків реалізації Blockchain.

### **Лабораторна робота №7 (5/- год.)**

Тема: Створення та налаштування VPN

Мета: Формування вмінь і навиків налаштування протоколу IPSec

## **6. Комплексне практичне індивідуальне завдання**

Індивідуальні завдання з дисципліни «Безпека інформаційних систем» виконується самостійно кожним студентом. КППЗ охоплює усі основні теми дисципліни «Безпека інформаційних систем». Метою виконання КППЗ є оволодіння навичками застосування теоретичних. КППЗ оформлюється у відповідності з встановленими вимогами. Виконання КППЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Безпека інформаційних систем».

Варіанти КППЗ з дисципліни "Безпека інформаційних систем":

1. Провести критичний аналіз систем резервного копіювання та відновлення даних (не менше 5 рішень). Надати рекомендації щодо особливостей резервного копіювання та відновлення даних.

2. Провести критичний аналіз засобів створення смарт-контрактів на базі блокчейну Ethereum, NXT, Bitcoin.
3. Розробити Incident Response Plan для реагування на програми – вимагачі (Ransomware)
4. Розробити Investigation Report на фішингову атаку типу нігерійські листи.
5. Розробити політику конфіденційності IT-компанії відповідно до вимог GDPR
6. Розробити положення про обробку персональних даних користувачів відповідно до вимог GDPR для будь-якого веб-сайту.
7. Провести функціональний аналіз хмарних ресурсів (не менше 5 рішень) для забезпечення безпеки даних у відповідності до GDPR.
8. Провести функціональний аналіз DLP – систем (Data Loss Prevention) (не менше 5 рішень).
9. Провести функціональний аналіз SIEM - систем (Security information and event management) (не менше 5 рішень).
- 10.Провести функціональний аналіз IDS - систем (Intrusion Detection System). (не менше 5 рішень).
- 11.Провести функціональний аналіз IDM – систем (Identity Management System). (не менше 5 рішень).
- 12.Провести функціональний аналіз інструментів для penetration test.
- 13.Провести критичний аналіз фаєрволів для ОС Android та iOS. Сформувати рекомендації для користувачів.
- 14.Провести критичний аналіз фаєрволів для ОС Windows. Сформувати рекомендації для користувачів.
- 15.Провести критичний аналіз антивірусів для ОС Android та iOS. Сформувати рекомендації для користувачів.
- 16.Провести критичний аналіз антивірусів для ОС Windows. Сформувати рекомендації для користувачів.
- 17.Розробити рекомендації для IT-компанії щодо використання wi-fi (корпоративний, гостьовий доступ) з точки зору безпеки даних.
- 18.Проаналізувати переваги створення DMZ (demilitarized zone) для IT-компанії з точки зору безпеки даних.
- 19.Розробити рекомендації щодо впровадження VLAN (Virtual Local Area Network) для IT-компанії
- 20.Розробити рекомендації щодо використання реєстру Windows фахівцями з інформаційної безпеки. Провести критичний аналіз VPN- клієнтів для платформи Android (не менше 3 рішень). Сформувати рекомендації для користувачів



- 21.Провести критичний аналіз VPN - сервісів для платформи Windows (не менше 3 рішень). Сформувати рекомендації для користувачів.
- 22.Провести критичний аналіз засобів дешифрування результатів роботи програм-вимагачів (не менше 3 рішень). Сформувати рекомендації для користувачів.
- 23.Розробити рекомендації для користувачів, що заразились adware.
- 24.Розробити рекомендації для користувачів що заразились троянськими вірусами.
- 25.Розробити рекомендації для запобігання телефонному та email – фішингу.
- 26.Розробити рекомендації для користувачів для безпечної роботи в мережі Інтернет.
- 27.Розробити рекомендації для користувачів для безпечного користування мобільними телефонами.
- 28.Безпека систем, що використовують NCSA HTTPD і Apache HTTPD
- 29.Безпека систем, що використовують скрипти в CGI-BIN
- 30.Класифікація систем виявлення мережевих атак
- 31.Класифікація систем контролю цілісності
- 32.Аналіз проблем безпеки Інтернету – речей
- 33.Аналіз проблем безпеки кіберфізичних систем
- 34.Аналіз проблем безпеки в хмарі
- 35.Аналіз проблем безпеки в NFC
- 36.Аналіз атак на Microsoft AD.
- 37.Аналіз задач SOC центру (Security operation center)
- 38.TOP-10 фінансових втрат українських підприємств від зловмисних атак за 2019 рік.
- 39.Актуальні тренди кібербезпеки 2019
40. Аналіз засобів захисту кінцевих терміналів

### 7. Самостійна робота

№ п/п	Тематика	К-сть годин (денна)	К-сть годин (заочна)
1	Сервіси і механізми захисту VPN	5	13
2	Принципи побудови блочних шифрів та криптосистем з відкритим ключем	5	13
3	Сучасні алгоритми симетричного та асиметричного шифрування	5	13
4	Сучасні алгоритми хешування	5	13
5	Основні методи безпечного написання коду програм	5	13
6	Методи і засоби аналізу безпеки програмних	5	13

	засобів		
7	Використовувати функції Microsoft CryptoAPI для розробки прикладного ПЗ	5	11
8	Оцінка та аналіз безпеки ПЗ	5	13
9	Протоколи автентифікації	5	10
10	Програмна реалізація криптографічних алгоритмів	5	13
11	Методи безпечної реалізації ПЗ	5	13
<b>Разом:</b>		<b>55</b>	<b>138</b>

## 8. Тренінг з дисципліни

Тематика тренінгу: Захист інформаційних систем від несанкціонованого копіювання

Завдання та структура тренінгу:

1. На базі розробленого програмного забезпечення на лабораторних роботах, реалізувати метод захисту від несанкціонованого копіювання відповідно до варіанту, поданого нижче.
2. Варіанти завдання

№	Тип ПЗ	Обмеження	Шифр ключа
1	Demoware	Розмір файлів для відкриття не більший 100 КБ	Цезаря
2	Demoware	Відкриття файлів тільки формату BMP	Віженера
3	Demoware	Відкриття файлів тільки текстових форматів	Цезаря
4	Demoware	Відсутня функція збереження файлів	Віженера
5	Demoware	Файли відкриваються тільки з однієї директорії	Віженера
6	Demoware	Недоступна функція друку	Цезаря
7	Demoware	Недоступна функція перегляду параметрів файлу	Цезаря
8	Trialware	Блокування виконання програми після 30 днів після її встановлення	Віженера
9	Trialware	Блокування виконання програми після 10 запусків після її встановлення	Цезаря
10	Trialware	Блокування виконання програми після її відкриття 10 раз	Віженера
11	Trialware	Блокування виконання програми після 30 днів після її встановлення або 20 запусків	Віженера
12	Trialware	Блокування функцій програми після 10 днів після її встановлення	Цезаря
13	Trialware	Блокування функцій програми в останній день поточного року	Цезаря
14	Trialware	Блокування функцій програми в кінці поточно місяця	Віженера
15	Nagware	Діалогове вікно нагадування про реєстрацію програми через кожні 5 хвилин роботи з нею	Цезаря

16	Nagware	Діалогове вікно нагадування про реєстрацію програми після кожного запуску програми	Віженера
17	Nagware	Діалогове вікно нагадування про реєстрацію програми після кожного завершення програми	Віженера

Література: 1,2,4,9,10

### 9. Засоби оцінювання та методи демонстрування результатів навчання

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіа проектора та інших ТЗН; лабораторні роботи, в у комп'ютерному класі; індивідуальні заняття; виконання КППЗ, тренінг.

У процесі вивчення дисципліни «Безпека інформаційних систем» використовуються наступні методи оцінювання навчальної роботи студентів:

- поточне тестування та опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання КППЗ;
- ректорська контрольна робота;
- тренінг;
- підсумковий письмовий екзамен;
- інше.

### 10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Безпека інформаційних систем» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КППЗ, враховуючи поточне опитування)	Заліковий модуль 4 (екзамен)	Разом
20%	20 %	20 %	40%	100%
1) Усне або письмове опитування під час заняття (4 теми по 10 балів – 40 балів) 2) Лабораторні роботи – 60 балів	1) Усне або письмове опитування під час заняття (4 теми по 10 балів – 40 балів) 2) Лабораторні роботи – 60 балів	1) Написання та захист КППЗ – 80 балів 2) Виконання завдань під час тренінгу – 80 балів	1) Тестові завдання (25 тестів по 2 бали за тест) – макс. 50 балів 2) Завдання 1 – макс. 25 балів 3) Завдання 2 – макс. 25 балів	100

За шкалою Університету	За національною шкалою	За шкалою ECTS
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)

75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

### **11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна**

№	Найменування	Номер теми
1.	Електронний варіант лекцій	1-7
2.	Вихідні дані для виконання лабораторних робіт	1-7
3.	Visual Studio 2019	1-4
4	Deep packet inspection	5

### **РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ**

1. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.
2. Поляков А. О., Євсєєв С. П., Огурцов В. В. Лабораторний практикум з навчальної дисципліни "Захист інформації в інформаційних системах" : навч.-практ. посіб. - Х. : ХНЕУ, 2017. – 208 с.
3. Терейковський, І. А. Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавр за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 Комп'ютерна інженерія / І. А. Терейковський, А. О. Корченко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,16 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 176 с. – Назва з екрана.
4. Гуз А.М., Довгань О.Д., Марущак А.І. Організація захисту інформації з обмеженим доступом. - К. : Наук.-вид. відділ НА СБ України, 2015. - 378 с.
5. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2018. – С. 10 – 14.
6. Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.
7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТТСЗІ СБ України, Київ, 1998.

8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.2-001-98, ДСТТСЗІ СБ України, Київ, 1998.
9. Класифікація автоматизованих систем і стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.2-002-98, ДСТТСЗІ СБ України, Київ, 1998.
10. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТТСЗІ СБ України, Київ, 1998.