МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування
імені адмірала Макарова

**М. В. ТУРТИ, О. О. ЩЕЛКОНОГОВ,
А. В. ЄРМАКОВА**

МЕТОДИЧНІ ВКАЗІВКИ
до самостійної роботи студентів з дисципліни "АВТОМАТИЗАЦІЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ"

Рекомендовано Методичною радою НУК

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
КОРАБЛЕБУДУВАННЯ
ІМ. АДМІРАЛА МАКАРОВА
2021

УДК 004.05(076)
Т86

Автори: М. В. Турти, канд. техн. наук, доцент;
О. О. Щелконогов, старший викладач;
А. В. Єрмакова, магістр

Рецензент В. С. Блінцов, д-р техн. наук, професор

Рекомендовано Методичною радою НУК

Турти М. В.

Т86 Методичні вказівки до самостійної роботи студентів з дисципліни "Автоматизація обробки інформації з обмеженим доступом" / М. В. Турти, О. О. Щелконогов, А. В. Єрмакова. – Миколаїв : НУК, 2021. – 44 с.

Методичні вказівки до самостійної роботи призначені для впорядкування процесу самостійної підготовки студентів, що спеціалізуються з технічного захисту інформації в галузі електричної інженерії. Самостійна робота передбачає опрацювання лекційного матеріалу, підготовку до лабораторних робіт, модульних контрольних робіт та підготовку до іспиту.

УДК 004.05(076)

1. ЗАГАЛЬНІ ВІДОМОСТІ

Більша кількість сучасних електротехнічних систем є автоматизованими системами, в яких циркулює інформація, спотворення якої може привести до виходу системи в аварійний режим, а в окремих системах – інформація щодо параметрів технологічних процесів, конструктивних особливостей, складу об'єктів обробки, що є комерційною таємницею. Автоматизовані системи є також основою бізнесу, наукової і політичної діяльності, засобами спілкування і часто пов'язані з фінансовими оборудками чи іншими операціями з інформацією обмеженого доступу. У зв'язку з цим професіонали з технічного захисту інформації повинні мати теоретичні знання і практичні навички автоматизації обробки інформації з обмеженим доступом в різноманітних предметних галузях.

Дисципліна "Автоматизація обробки інформації з обмеженим доступом" є однією з останніх дисциплін циклу професійної підготовки магістрів за освітньо-професійною програмою "Системи технічного захисту інформації, автоматизація її обробки" спеціальності 141 "Електроенергетика, електротехніка та електромеханіка" галузі знань 14 "Електрична інженерія".

Дисципліна "Автоматизація обробки інформації з обмеженим доступом" базується на дисциплінах загальної і професійної підготовки бакалаврів ("Інформаційні технології в системах захисту інформації", "Безпека інформаційних та комунікаційних систем", "Засоби передавання інформації в системах технічного захисту інформації", "Засоби приймання та обробки інформації в системах технічного захисту інформації", "Електроніка та компонентна база засобів технічного захисту інформації", "Методи та засоби захисту інформації", "Організаційне забезпечення технічного захисту інформації",

"Основи теорії кіл, сигналів та процесів в системах захисту інформації", "Поля і хвилі в системах технічного захисту інформації", "Проектування систем кібербезпеки", "Схемотехніка пристроїв технічного захисту інформації", "Теорія інформації та кодування", "Технічні засоби охорони об'єктів", "Бази даних", "Захист програмного продукту", "Мікропроцесорні засоби обробки даних в системах технічного захисту інформації", "Моделювання об'єктів і процесів інформаційної безпеки", "Системи і мережі передачі даних", "Технології програмування систем кібербезпеки", "Цифрова обробка сигналів", "Захист аудіо- та відеоінформації в засобах її обробки", "Комплексні системи захисту інформації", "Основи режимно-секретної діяльності"), а також використовує знання принципів функціонування систем радіомоніторингу і радіопротидії, засвоєні при вивченні дисципліни "Теорія захисту інформаційних ресурсів та кібервузлів обмеженого доступу" другого (магістерського) рівня освіти. З дисциплін освітньо-професійної програми першого (бакалаврського) рівня вищої освіти, безпосередньо пов'язаними із дисципліною "Інформаційна безпека спеціалізованих електротехнічних систем морського транспорту", є дисципліни "Інформаційні технології в системах захисту інформації", "Бази даних", "Захист програмного продукту", "Мікропроцесорні засоби обробки даних в системах технічного захисту інформації", "Методи та засоби захисту інформації", "Комплексні системи захисту інформації", "Безпека інформаційних та комунікаційних систем", "Схемотехніка пристроїв технічного захисту інформації", що забезпечує знання принципів функціонування і застосування систем технічного захисту інформації та їх апаратних складових.

Предмет "Автоматизація обробки інформації з обмеженим доступом" органічно доповнюється рядом дисциплін, які ви-

кладаються одночасно з ним, зокрема "Дисципліни спеціальної підготовки за темою досліджень", "Технології створення та застосування комплексів захисту інформації з обмеженим доступом", "Менеджмент інформаційної безпеки морських комплексів", формуючи систему знань і вмінь розробки і впровадження інноваційних рішень із захисту інформації, оцінювання їх ефективності в галузі морського транспорту.

"Автоматизація обробки інформації з обмеженим доступом" є основою прийняття роботи схемо-технічних і програмних рішень під час наукового стажування і виконання кваліфікаційної роботи.

Мета вивчення дисципліни – оволодіння теоретичними методами і практичними засобами побудови автоматизованих систем обробки інформації обмеженого доступу.

Предметом навчальної дисципліни "Автоматизація обробки інформації з обмеженим доступом" є автоматизовані системи обробки інформації обмеженого доступу.

Завданням дисципліни є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, зокрема: обґрунтування прийняття рішень у галузі ТЗІ при побудові автоматизованих систем обробки інформації обмеженого доступу й оцінці ефективності їх захисту; здобуття практичних навичок прийняття рішень у галузі ТЗІ на основі діючої нормативно-правової бази (для студентів, що мають форму допуску до складу нормативно-правової бази включені документи з обмеженим доступом) при побудові автоматизованих систем обробки інформації обмеженого доступу й оцінці ефективності їх захисту; здобуття практичних навичок обґрунтованого вибору програмного і апаратного забезпечення автоматизованих систем обробки інформації обмеженого доступу в залежності від задач захисту.

В результаті вивчення дисципліни "Автоматизація обробки інформації з обмеженим доступом" студент повинен

знати:

– архітектуру систем автоматизованого оброблення інформації з обмеженим доступом;

– нормативно-правові засади проєктування, реалізації та впровадження систем автоматизованого оброблення інформації з обмеженим доступом;

– основні напрями реалізації захисту інформації з обмеженим доступом автоматизованої системи;

– порядок розробки та реалізації комплексу засобів захисту інформації з обмеженим доступом автоматизованої системи;

– методи і методики оцінки захищеності автоматизованих систем обробки інформації з обмеженим доступом;

уміти:

– виходячи із загальних принципів реалізації процесів автоматизованого оброблення інформації з обмеженим доступом, створювати архітектуру системи, організаційне та технологічне забезпечення;

– організовувати реалізацію проєкту системи автоматизованого оброблення інформації з обмеженим доступом;

– здійснювати управління розробкою та впровадженням системи автоматизованого оброблення інформації з обмеженим доступом;

– застосовувати системний підхід для побудови системи технічного захисту інформації з обмеженим доступом автоматизованої системи, яка визначає загальну організацію і класифікацію системи даних, систему доступу, напрямки планування, відповідальність користувачів, використання оцінки ризиків тощо в контексті інформаційної безпеки;

– застосовувати сучасні способи, методи та засоби захисту автоматизованої системи: політику безпеки, архітектуру захисту, механізми захисту та засоби захисту;

– здійснювати оцінку відповідності системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів;

мати уявлення про тенденції розвитку автоматизованих систем обробки інформації, методів і засобів захисту інформації в автоматизованих системах обробки інформації обмеженого доступу.

2. РОЗПОДІЛ НАВЧАЛЬНОГО ЧАСУ

Розподіл навчальних годин за формами навчання та видами навчальних занять згідно з навчальним планом здійснено так, як показано в таблиці 2.1.

Таблиця 2.1

Форма навчання	Семестр	Всього годин/ залікових кредитів	Розподіл за видами занять				Форма контролю
			Лекції	Практичні заняття	Лабораторні роботи	СРС	
Денна	10	150/5	15	–	15	120	екзамен
Заочна			8	–	8	134	

3. СТРУКТУРА ДИСЦИПЛІНИ І ТЕРМІНИ КОНТРОЛЮ ЗНАНЬ

Таблиця 3.1

Назви змістових модулів і тем	Денна форма					Контроль, тиждень	Заочна форма				
	Кількість годин						Кількість годин				
	усього	у тому числі					усього	у тому числі			
		лек.	практ.	лаб.	с. р. с			лек.	практ.	лаб.	с. р. с.
Змістовий модуль 1 Системи автоматизованої обробки інформації з обмеженим доступом											
Тема 1. Архітектура системи автоматизованого оброблення інформації з обмеженим доступом	22	2	–	2	18		22	2	–	–	20
Тема 2. Основи проєктування системи автоматизованого оброблення інформації з обмеженим доступом	32	2	–	4	26		32		–	4	28
Тема 3. Реалізація системи автоматизованого оброблення інформації з обмеженим доступом	36	2	–	4	30		36	2	–	2	32
Разом за змістовим модулем 1	90	6	–	10	74		90	4	–	6	80
Модульна контрольна робота № 1						10	Залікова сесія				
Змістовий модуль 2. Технічний захист інформації в системах автоматизованої обробки інформації з обмеженим доступом											
Тема 4. Основні напрями реалізації захисту інформації з обмеженим доступом автоматизованої системи	17	2	–	2	13		14	2	–	–	12
Тема 5. Порядок розробки та реалізації комплексу засобів захисту інформації з обмеженим доступом автоматизованої системи	27	4	–	2	21		14	2	–	2	12

Продовження таблиці

Назви змістових модулів і тем	Денна форма					Контроль, тиждень	Заочна форма				
	Кількість годин						Кількість годин				
	усього	у тому числі					усього	у тому числі			
		лек.	практ.	лаб.	с. р. с			лек.	практ.	лаб.	с. р. с.
Тема 6. Оцінка захищеності автоматизованої системи обробки інформації з обмеженим доступом	16	3	–	1	12		8		–	–	8
Разом за змістовим модулем 2	60	9	–	5	46		60	4	–	2	54
Модульна контрольна робота №2						15	Залікова сесія				
Усього за модулем 1	150	15	–	15	120		150	8	–	8	134
Екзамен					16–17 За розкладом екзаменаційної сесії		За розкладом залікової сесії				

Примітка 1. Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до таблиці (розд. 3). Студенти заочної форми навчання виконують лабораторні роботи 2, 3, 5, 7.

4. ЗМІСТ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Метою самостійної робота є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних і лабораторних заняттях.

Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті). Самостійна робота студента передбачає проробку лекційного матеріалу, опрацювання окремих питань теоретичного матеріалу, винесених на самостійне вивчення, підготовку до лабораторних робіт, поточного (модульного) контролю знань і екзамену. На самостійну проробку з даного курсу виносяться питання, наведені в таблиці 4.1.

Таблиця 4.1. **Завдання до самостійної роботи**

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	До теми 1. Архітектура систем автоматизованого оброблення інформації з обмеженим доступом транспортних засобів	18	20
2	До теми 2. Зміни в нормативно-правовій базі проектування системи автоматизованого оброблення інформації з обмеженим доступом за останній рік	26	28
3	До теми 3. Сертифіковані на поточний час апаратні засоби захисту інформації	30	32
4	До теми 4. Сертифіковані на поточний час програмні засоби захисту інформації	13	15
5	До теми 5. Сертифіковані на поточний час апаратні і програмні засоби оцінювання ефективності системи захисту інформації в АСОІзОД	21	23
6	До теми 6. Програмні засоби оцінювання ефективності комплексної системи захисту інформації за міжнародними стандартами	12	16
Разом		**120**	**134**

5. ПИТАННЯ ДЛЯ ПОТОЧНОГО І ПІДСУМКОВОГО КОНТРОЛЮ

5.1. Питання до модульної контрольної роботи № 1

Змістовий модуль 1. "Системи автоматизованої обробки інформації з обмеженим доступом"

Тема 1. Архітектура системи автоматизованого оброблення інформації з обмеженим доступом.

1. Розкрийте поняття "інформації", "захист інформації", "публічна інформація", "інформація з обмеженим доступом".

2. Дайте визначення поняттям "телекомунікаційна система", "інформаційна система", "автоматизована система", "автоматична система", "автоматизована інформаційна система", "система документообігу", "автоматизована система документообігу".

3. Розкрийте поняття "державна таємниця", "таємна інформація", "гриф обмеження доступу" до інформації.

4. Розкрийте поняття конфіденційності, доступності, цілісності і спостережності як функціональних критеріїв.

5. Види інформації за змістом та порядком доступу.

6. Завдання й особливості інформаційних систем автоматизованої обробки даних.

7. Компоненти автоматизованої обробки інформації.

8. Режими обробки даних: загальна характеристика.

9. Режими обробки даних: особливості технології обробки текстової інформації на паперових носіях.

10. Режими обробки даних: особливості технології обробки електронних документів.

11. Режими обробки даних: особливості технології обробки графічної інформації.

12. Режими обробки даних: особливості обробки відеоінформації.

13. Режими обробки даних: особливості обробки аудіоінформації.

14. Режими обробки даних: особливості пакетного режиму обробки даних.

15. Режими обробки даних: особливості діалогового режиму обробки даних.

16. Режими обробки даних: особливості мережного режиму обробки даних.

17. Режими обробки даних: особливості режиму обробки даних в реальному часі.

18. Режими обробки даних: особливості обробки даних у багатокористувацьких системах.

19. Режими обробки даних: особливості інтерактивного режиму обробки даних.

20. Структура інформаційних систем.

21. Структура систем документообігу: загальна характеристика.

22. Принципи класифікації інформаційних систем.

23. Класифікація інформаційних систем за структурованістю задач.

24. Класифікація інформаційних систем за функціональною ознакою і рівнями управління.

25. Класифікація інформаційних систем за ступенем автоматизації.

26. Класифікація автоматизованих систем за характером використання інформації.

27. Класифікація автоматизованих інформаційних систем за сферою застосування.

28. Класифікація автоматизованих систем за принципом формальності.

29. Реквізити організаційно-розпорядчих документів, їх розміщення.

30. Кодування інформації в документах.

31. Кодування інформації при автоматизованій обробці інформації.

32. Бланки документів і шаблони в автоматизованих системах.

33. Особливості мережних автоматизованих систем обробки інформації, обумовлені режимами комутації (порівняльний аналіз для мереж з комутацією каналів, комутацією пакетів і комутацією повідомлень).

34. Особливості мережних автоматизованих систем обробки інформації, обумовлені топологією мережі (порівняльний аналіз типових топологій).

35. Нормативно-правове забезпечення системи управління вітчизняного діловодства.

36. Нормативно-правові вимоги до системи управління вітчизняного діловодства.

37. Етапи розробки і впровадження автоматизованих систем, призначених для обробки інформації з обмеженим доступом.

38. Правила обліку, розповсюдження і зберігання документів з грифом "Для службового користування".

39. Заходи захисту секретної інформації в автоматизованій системі.

40. Реєстрація документів. Автоматизована реєстрація документів. Які документи не підлягають реєстрації діловодною службою?

41. Алгорим дій при отриманні документів (електронних документів, пакетів, конвертів) з грифом секретності.

42. Засоби захисту інформації при колективній роботі з текстовими документами.

43. Вимоги до системи безпеки конфіденційного електронного документообігу.

44. Щоденні перевірки при прийманні та обробці вхідних документів.

45. Процедури віднесення інформації до ІзОД.

46. Процедури надання та перегляду прав доступу користувачам інформаційної системи до інформації з обмеженим доступом.

47. Процедури надання та перегляду прав доступу до інформації з обмеженим доступом при мандатній і дискреційній політиках безпеки.

48. Обов'язки осіб, які обробляють інформацію електронного документообігу з обмеженим доступом.

49. Порядок обліку паперових, магнітних та інших носіїв інформації, які призначені для зберігання та обробки інформації з обмеженим доступом.

50. Потенційні канали витоку інформації в автоматизованій системі обробки інформації з обмеженим доступом.

51. Категоріювання об'єктів інформаційної діяльності.

52. Умови дозволу обробки інформації з обмеженим доступом в інформаційній системі.

53. Візи і підписи на документах. Аркуші погодження. Яким чином підписується документ, якщо посадова особа, підпис якої зазначений на проекті документа, відсутня?

Тема 2. Основи проєктування системи автоматизованого оброблення інформації з обмеженим доступом.

54. Принципи забезпечення інформаційної безпеки в АС: загальна характеристика.

55. Принципи забезпечення інформаційної безпеки в АС: принцип системності і комплексності.

56. Принципи забезпечення інформаційної безпеки в АС: принцип неперервності захисту і розумної достатності.

57. Принципи забезпечення інформаційної безпеки в АС: принцип гнучкості управління і застосування.

58. Принципи забезпечення інформаційної безпеки в АС: принцип відкритості алгоритмів та механізмів захисту.

59. Принципи забезпечення інформаційної безпеки в АС: принцип простоти застосування захисних засобів і методів.

60. Функції служби захисту інформації щодо обробки інформації з обмеженим доступом в автоматизованих системах.

61. Зміст плану захисту інформації з обмеженим доступом в автоматизованих системах.

62. Стратегія кібербезпеки України.

63. Звід відомостей, що становлять державну таємницю

64. Постанова КМУ №1772 16.11.02 Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах.

65. Закон України "Про інформацію" .

66. Закон України "Про державну таємницю".

67. Закон України "Про телекомунікації".

68. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" .

69. Закон України "Про Національну систему конфіденційного зв'язку".

70. Закон України "Про електронний цифровий підпис".

71. Закон України "Про електронні документи та електронний документообіг".

72. Закон України "Про основи національної безпеки України".

73. Закон України "Про наукову і науково-технічну діяльність".

74. Закон України "Про захист персональних даних".

75. Закон України "Про доступ до публічної інформації".

76. Положення про технічний захист інформації в Україні УП №1229/99 від 27.09.99. Постанова КМУ №1126 8.10.97.

77. Концепція технічного захисту інформації в Україні.

78. Постанова КМУ № 373 29.03.06 Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

79. Постанова КМУ № 281 13.03.02 Про деякі питання захисту інформації, охорона якої забезпечується державою.

80. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

81. Положення про структуру Національної системи конфіденційного зв'язку та умови її використання для забезпечення безпеки обміну інформацією, затверджене рішенням Кабінету Міністрів України від 14 травня 2015 р. № 303.

82. Положення про автоматизовану систему документообігу суду, затверджене рішенням Ради суддів України від "26" листопада 2010 року № 30 щодо провадження документообігу у судах загальної юрисдикції.

83. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

84. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

85. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

86. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Тема 3. Реалізація системи автоматизованого оброблення інформації з обмеженим доступом.

87. Побудова систем захисту: загальна характеристика.

88. Побудова систем захисту від загрози порушення конфіденційності інформації: організаційно-режимні заходи захисту носіїв інформації в АС.

89. Побудова систем захисту від загрози порушення конфіденційності інформації: класифікація методів захисту від НСД.

90. Побудова систем захисту від загрози порушення конфіденційності інформації: класифікація методів і способів автентифікації.

91. Побудова систем захисту від загрози порушення конфіденційності інформації: структура парольної системи захисту, загрози безпеки парольних систем.

92. Побудова систем захисту від загрози порушення конфіденційності інформації: вимоги до вибору паролів і параметри для кількісної оцінки стійкості парольних систем захисту.

93. Побудова систем захисту від загрози порушення конфіденційності інформації: зберігання паролів і передача паролів по мережі, зв'язок парольної та криптографічної систем захисту.

94. Побудова систем захисту від загрози порушення цілісності інформації: загальна характеристика, цілісність інформації в АС, організаційні заходи захисту цілісності інформації на машинних носіях.

95. Побудова систем захисту від загрози відмови в доступі до ресурсів: загальна характеристика.

96. Побудова систем захисту від загрози розкриття параметрів інформаційної системи: загальна характеристика.

97. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації.

98. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

99. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

100. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

101. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1, затвердженою наказом ДСТСЗІ СБУ 18.06.02 № 37).

102. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

103. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

104. ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок.

105. РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения.

106. РД 50-682-89 Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы (ГОСТ 34.201-89, ГОСТ 34.602-89, РД 50-682-89).

107. РД 50-34-698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих

документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

108. Р–СП Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень НБУ.

109. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

5.2. Питання до модульної контрольної роботи № 2

Змістовий модуль 2.
"Технічний захист інформації в системах автоматизованої обробки інформації з обмеженим доступом"

Тема 4. Основні напрями реалізації захисту інформації з обмеженим доступом автоматизованої системи.

1. Загальна характеристика криптографічних методів захисту інформації в автоматизованих системах.

2. Способи та особливості реалізації криптографічних підсистем.

3. Криптографічний захист транспортного рівня АС.

4. Криптографічний захист прикладного рівня АС: загальна характеристика.

5. Криптографічний захист прикладного рівня АС: абонентський захист.

6. Криптографічний захист прикладного рівня АС: вбудовані СКЗІ.

7. Криптографічний захист прикладного рівня АС: способи реалізації криптографічного захисту в окремому суб'єкті.

8. Криптографічний захист прикладного рівня АС: розподілена реалізація.

9. Особливості стандартизації та сертифікації криптографічних засобів.

10. Перспективні напрямки розвитку криптографічних засобів захисту.

11. Захист від загрози порушення конфіденційності на рівні змісту інформації. Стеганографія.

12. Побудова систем захисту від загрози порушення цілісності інформації: технологічні заходи захисту цілісності інформації на машинних носіях, циклічний код.

13. Побудова систем захисту від загрози порушення цілісності інформації: захист пам'яті, бар'єрні адреси, динамічні області пам'яті і адресні регістри, сторінки і сегменти пам'яті.

14. Цифровий підпис: загальна характеристика.

15. Цифровий підпис: класи формування цифрового підпису.

16. Побудова систем захисту від загрози порушення цілісності інформації: захист від загрози порушення цілісності інформації на рівні змісту інформації.

17. Побудова систем захисту від загрози відмови в доступі до ресурсів: захист від збоїв програмно-апаратного середовища (загальна характеристика).

18. Побудова систем захисту від загрози відмови в доступі до ресурсів: забезпечення відмовостійкості програмного забезпечення АС, запобігання несправностей в програмному забезпеченні АС.

19. Побудова систем захисту від загрози відмови в доступі до ресурсів.

20. Побудова систем захисту від загрози відмови в доступі до ресурсів: захист семантичного аналізу та актуальності інформації.

21. Побудова систем захисту від загрози розкриття параметрів інформаційної системи: захист доступу до інформації.

22. Побудова систем захисту від загрози розкриття параметрів інформаційної системи: приховування логіки роботи і захисних функцій складових АС.

Тема 5. Порядок розробки та реалізації комплексу засобів захисту інформації з обмеженим доступом автоматизованої системи.

23. Поняття доступу і моніторингу безпеки: суб'єкти і об'єкти в АС, породження суб'єктів.

24. Поняття доступу і моніторингу безпеки: потоки, доступ суб'єктів до об'єктів, правила розмежування доступу, моніторинг звертань, моніторинг безпеки об'єктів.

25. Поняття доступу і моніторингу безпеки: тотожність об'єктів АС і тотожність суб'єктів АС, абсолютно взаємно коректні суб'єкти.

26. Політика безпеки: загальна характеристика.

27. Політика безпеки: політика безпеки при обробці електронних документів обмеженим доступом та веденні різних форм обліку.

28. Принципи класифікації порушників в автоматизованих системах обробки інформації з обмеженим доступом.

29. Вимоги до СКЗІ.

30. 22.05.98 № 505 Положення про порядок здійснення криптографічного захисту інформації в Україні УП №505/98 від 22.05.98.

31. Наказ Держспецзв'язку № 141 20.07.07 Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації (в редакції закону від 14.12.2015 № 767).

32. Наказ Держспецзв'язку №114 12.06.07 Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації.

33. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

34. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки.

35. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

36. Особливості систем автоматизованого документообігу ВНЗ.

37. Особливості систем автоматизованого документообігу суду.

38. Особливості банківських систем автоматизованого документообігу.

39. Особливості систем автоматизованого документообігу державних органів.

40. Особливості систем автоматизованого документообігу в аптеках і лікарських установах.

41. Optima-WorkFlow.

42. "M.E.Doc" / "M.E.Doc Електронний документообіг".

43. FossDoc.

44. Work'sOrganizer.

45. Система "ДІЛО-ПІДПРИЄМСТВО"

46. 1С: Документообіг 8.

47. КАІ-Документообіг.

48. Організація захищеного документообігу в системах електронного урядування.

49. Загальнодержавна Інформаційна система "Електронна Україна".

50. Організація міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку.

51. Система "хмарного" електронного документообігу "Megapolis.DocNet".

52. Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 1 "Лоза-1".

53. Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 2 "Лоза-2".

54. Постанова КМУ № 1893 27.11.98 Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави.

55. Постанова КМУ № 1000 19.07.06 Деякі питання обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави.

56. ДСТ СЗІ № 9 23.02.02 Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб.

57. Наказ Держспецзв'язку № 45 26.03.07 Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ.

58. НБУ № 243 04.07.07 Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи.

Тема 6. Оцінка захищеності автоматизованої системи обробки інформації з обмеженим доступом.

59. Причини порушення інформаційної безпеки при обробці інформації в СКЗІ.

60. Побудова систем захисту від загрози порушення цілісності інформації: модель контролю цілісності Кларка-Вілсона.

61. Наказ Держспецзв'язку № 143 24.07.07 Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису.

62. Наказ Держспецзв'язку № 100 23.06.08 Положення про державну експертизу у сфері криптографічного захисту інформації.

63. Наказ Держспецзв'язку № 112 04.07.08 Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних системах.

64. Постанова КМУ № 791 22.08.2012 Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності у галузях криптографічного та технічного захисту інформації, що підлягає ліцензуванню... (На заміну Постанови КМУ від 06.08.2008 № 698).

65. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

66. НД ТЗІ 2.7 -009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

67. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

68. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

69. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

70. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

71. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

6. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ТА СИСТЕМА РЕЙТИНГОВИХ БАЛІВ

6.1. Методи контролю знань

Рівень засвоєння матеріалу дисципліни здійснюється шляхом проведення поточного модульного контролю (МК) у вигляді контрольних робіт, захисту звітів з лабораторних робіт та підсумкового контролю у формі іспиту.

З метою оперативного та якісного засвоєння матеріалу на лекціях і лабораторних заняттях використовуються наочні матеріали: слайди, інтернет-ресурси нормативно-правової бази. За відвідування цих занять студентам нараховуються бали згідно з розд. 6.2.

Студенти денної і заочної форм навчання виконують і контрольні роботи МК1, МК2, за матеріалами відповідних змістових модулів (розд. 3). За модульні контрольні роботи студент отримує бали згідно з розд. 6.2.

Лабораторні роботи проводяться в спеціалізованих лабораторіях кафедри комп'ютерних технологій та інформаційної безпеки. Під час лабораторних робіт студенти денної форми навчання захищають звіти з попередньо виконаних робіт і отримують бали згідно з розд. 6.2. Студенти заочної форми навчання отримують завдання на лабораторні роботи під час установчої сесії, виконують їх згідно розкладом під час установчої і залікової сесії, захищають звіти з лабораторних робіт під час залікової сесії і отримують бали згідно з розд. 6.2.

Викладач на останньому занятті інформує студентів про узагальнені результати поточного модульного контролю.

Наприкінці семестру студент:

1) пред'являє викладачеві результати самостійної роботи у персональному конспекті та вибірково, за вказівкою викладача-

ча, їх коментує, і на підставі цього отримує певну кількість балів (див. розділ 9); мінімальна кількість балів при цьому становить 60 % від максимуму за цю частину роботи; в іншому разі студент повинен доопрацювати свій конспект до складання екзамену;

2) пред'являє викладачеві захищені протягом семестру звіти з лабораторних робіт і на підставі цього отримує певну кількість балів (див. розділ 9); мінімальна кількість балів при цьому становить 60 % від максимуму за цю частину роботи; в іншому разі студент повинен захистити або перезахистити звіти з окремих лабораторних робіт до складання екзамену;

3) складає екзамен.

Студент ДФН, який захистив лабораторні роботи й отримав за всі контрольні заходи протягом семестру не менше 60 балів, за власним бажанням може бути звільненим від складання екзамену. Студент, який набрав менше 60 балів, складає екзамен (проводиться у письмовій формі згідно з розкладом сесії), якщо має за контрольні, лабораторні та самостійну роботи не менше 16, 18 і 2 балів відповідно.

Кожний студент ЗФН складає екзамен обов'язково, до якого він допускається, якщо має за контрольні, лабораторні та самостійну роботи не менше 18, 14 і 4 балів відповідно.

У зв'язку із всезростаючим потоком інформації, що стосується методів і засобів автоматизації процесів обробки інформації обмеженого доступу, на перших заняттях кожному студенту надаються в електронному вигляді базові джерела лекційного матеріалу, методичні вказівки до лабораторних робіт, питання до модульних контролів та екзамену, допоміжні матеріали у вигляді презентацій, прикладів розрахунків, наукових статей і тез доповідей провідних фахівців галузі на наукових конференціях.

Студент може самостійно розробити конспект, у якому розглянуті всі основні питання навчальної дисципліни, але з обов'язковими індивідуальними записами, зробленими власноруч. Протягом семестру на лекціях і лабораторних заняттях студенту надається можливість отримати додатковий відповідний "роздавальний" матеріал (на електронних носіях) для додавання до персонального конспекту, який повинен містити розгляд питань, що засвідчують самостійну роботу студента над усіма темами навчальної дисципліни.

Усі лабораторні роботи, пов'язані із здобуттям навичок стосовно захисту інформації в автоматизованих системах, являють собою практичну підготовку до майбутньої професійної діяльності.

В окремих випадках (позапланова практика, сімейні обставини, форс-мажорні ситуації тощо) студент в установленому порядку може бути переведений на індивідуальний графік навчання, що оформлюється належним чином. Відвідування студентом лекційних занять скорочується, а роль і обсяг його самостійної роботи зростає. Лабораторні і контрольні роботи виконуються в додатковий (при необхідності) час навчання у повному обсязі.

6.2. Розподіл балів, які отримують студенти (максимально можлива кількість балів)

Модуль 1

Денна форма навчання

Складові модульного контролю	Поточне тестування та самостійна робота (ПМК)						Екзамен	Сума
	Змістові модулі							
	1			2				
	Т1	Т2	Т3	Т4	Т5	Т6		
	8,4	13,4	12,4	8,4	9,8	7,6	40	100
Самостійна робота (конспект)	0,4	0,4	0,4	0,4	0,8	0,6		3
Відвідування, виконання та захист лабораторних робіт	4	8	8	4	4	2	–	30
Контрольні роботи: МК1, МК2	4	5	4	4	5	5		27
	13			14				
Екзамен	–			–			40	100
Разом	34,2			25,8			40	100

Тут і далі: Т1, Т2..., Т6 – теми змістових модулів.

Заочна форма навчання

Складові модульного контролю	Поточне тестування та самостійна робота (ПМК)						Екзамен	Сума
	Змістові модулі							
	1			2				
	Т1	Т2	Т3	Т4	Т5	Т6		
	5,8	11,8	17,8	5,8	12,6	6,2	40	100
Самостійна робота (конспект)	0,8	0,8	0,8	0,8	1,6	1,2	–	6
Відвідування, виконання та захист лабораторних робіт	–	6	12	–	6	–		24
Контрольні роботи: МК1, МК2	5	5	5	5	5	5		30
	15			15				
Екзамен	–			–			40	100
Разом	35,4			24,6			40	100

Система рейтингових балів

1. Лекції:

Ваговий бал – 0,2 бала/год для ДФН; 0,4 – для ЗФН; повнота та якість оформлення конспекту лекцій: 0,2 бала/год для ДНФ; 0,4 бала – для ЗФН.

2. Лабораторні роботи:

Ваговий бал ДНФ – 2 бали:	Ваговий бал ЗФН – 14 балів:
оформлення роботи – 0,5 бала;	оформлення роботи – 4 бали;
захист роботи – 1,5 бали.	захист роботи –10 балів.

3. Штрафні та заохочувальні бали за:

відсутність на занятті без поважної причини…….. – 1 бал

недопуск до лабораторної роботи у зв'язку з незадовільним вхідним контролем…… – 1 бал

несвоєчасний захист лабораторної роботи…….. – 1 бал

підготовка реферату з теми модуля……..... + 5 балів

участь у модернізації лабораторних робіт чи виконання завдань із удосконалення дидактичних матеріалів з дисципліни…….....+ 10 балів

участь у студентських наукових конференціях з фаху.....….+ 10 балів

участь у наукових конференціях професорсько-викладацького складу з фаху…..……+15 балів

участь у студентських олімпіадах з фаху…….+ 15 балів

публікація статті у фахових виданнях……..+10 балів

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
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

7. ІНФОРМАЦІЙНІ РЕСУРСИ

7.1. Рекомендована література з курсу "Автоматизація обробки інформації з обмеженим доступом"

Базова

1. Блінцов В.С., Козирєв С.С. Захист програмних продуктів : навч. посібник. – Миколаїв : НУК, 2010.

2. Гвоздева А.В., Лаврентьев И.Ю. Основы проектирования автоматизированных информационных систем. – М.: ИД "ФОРУМ" – ИНФРА-М, 2007.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: в 2 кн. – М.: Энергоатомиздат, 1994.

4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М.: Издательский центр "Академия", 2009.

5. Гуржій А.М., Коряк С.Ф., Самсонов В.В., Скляров О.Я. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології. – Х.: Компанія СМІТ, 2004.

6. Завгородний В.И. Комплексная защита информации в компьютерных системах. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.

7. Єсін В.І., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій. – Харків: ХНУ імені В. Н. Каразіна, 2013.

8. Кошкін К.В., Кошкіна Л.Л. , Шнейдер О.Б. Інформаційні системи підприємства: у 2 ч. Ч1. – Миколаїв : УДМТУ, 2000.

9. Кошкін К.В., Кошкіна Л.Л. , Шнейдер О.Б. Інформаційні системи підприємства: у 2 ч. Ч2. – Миколаїв : УДМТУ, 2000.

10. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посібник. – К.: НАДУ, 2015.

11. Малюк А.А., Пазизин С.В. Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001.

12. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації : навч. посібник. – Харків: ХНЕУ, 2013.

13. Турти М.В., Нужний С.М., Ємець А.С. Методичні вказівки до лабораторних робіт з дисципліни "Автоматизація обробки інформації з обмеженим доступом" . – Миколаїв: НУК, 2019.

14. Турти М.В., Щелконогов О.О., Єрмакова А.В. Методичні вказівки до самостійної роботи студентів з дисципліни "Автоматизація обробки інформації з обмеженим доступом". – Миколаїв: НУК, 2019.

15. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. – Ростов н/Д: Феникс, 2008.

16. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2010

17. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие. – М.: ИД "Форум" : ИнФРА-М, 2010.

Допоміжна

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ, 2000.

2. Бармен С. Разработка правил информационной безопасности. – М.: Изд. дом "Вильямс", 2002.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС", 2002.

4. Глушко С.В., Шайкан А.В. Управлінські інформаційні системи: Навчальний посібник. – Львів: Магнолія-Плюс, 2006.

5. Кошкін К.В., Возний О.М., Григорян Т.Г. Інформаційні технології в управлінні проектами: навчальний посібник. – Миколаїв: НУК, 2009.

6. Норткат С. Анализ типовых нарушений безопасности в сетях. – М.: Вильямс. 2001.

7. Норткат Т.С., Новак Дж. Обнаружение нарушений безопасности в сетях. – М.: Вильямс, 2003.

8. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Издательский центр "Академия", 2008.

9. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 2001.

10. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие. – М.: Изд. дом гос. ун-та – Высшей школы экономики, 2011.

11. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК-Пресс, 2002.

12. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 1999, 2001, 2006.

13. Ярочкин, В.И. Информационная безопасность: учебник. – М.: "Международные отношения", "Летописец", 2000.

7.2. Навчально-методичні матеріали кафедри КТІБ

1. Тематичні презентації з кібербезпеки.
2. Приклади виконання контрольних робіт.

3. Зразки звітів з лабораторних робіт.

4. "Лоза-2" (CD).

5. Google Chrome (або будь-який інший браузер для доступу в Internet).

6. Інформаційна база з курсу "Автоматизація обробки інформації з обмеженим доступом" кафедри ЕОС та ІБ кафедри ЕОС та ІБ, в тому числі:

1. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. [Електронний ресурс] – Режим доступу: https://www.iso.org/ru/standard/54533.html

2. Information Integration for Concurrent Engineering (IICE). IDEF5 Method Report. [Електронний ресурс] /Knowledge Based Systems, Inc. – Електронні дані – Texas : Knowledge Based Systems, 1994. – Режим доступу: http://www.idef.com/pdf/Idef5.pdf.

3. Information Technology Security Evaluation Criteria [Електронний ресурс] – Режим доступу:https://www.bsi.bund.de/shareddocs/ downloads/de/bsi/zertifizierung/interpretationen/ais_18_itsec_jil_e_pdf.pdf?_blob=publicationfile.

4. Закон України "Про банки і банківську діяльність" [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2121-14.

5. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України". [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3475-15.

6. Закон України "Про державну таємницю" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/3855-12 .

7. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

8. Закон України "Про інформацію" [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

9. Закон України "Про Національний банк України" [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/679-14

10. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/ laws/show/2163-19

11. Закон України "Про основи національної безпеки України" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2469-19

12. Закон України "Про платіжні системи та переказ коштів в Україні" [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show /2346-14/ed20120527

13. Закон України "Про телекомунікації" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/1280-15

14. Доктрина інформаційної безпеки України [Електронний ресурс] – Режим доступу: http://www.president.gov.ua/documents/472017-21374

15. Стратегія кібербезпеки України [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017

16. ДСТУ 2392-94 "Інформація та документація. Базові поняття. Терміни та визначення" [Електронний ресурс] – Режим доступу: http://dstu-biblio.3dn.ru/load/dstu_2392_94/1-1-0-80

17. ДСТУ 2941-94 "Системи оброблення інформації. Розроблення систем. Терміни та визначення" [Електронний ресурс] – Режим доступу: http://ksv.do.am/GOST/DSTY_ALL/DSTU1/dstu_2941-94.pdf

18. ДСТУ 2960-94 "Організація промислового виробництва. Терміни та визначення" [Електронний ресурс] – Режим доступу: http://www.expertsoft.com.ua /sidocs/1100825/

19. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт [Електронний ресурс] – Режим доступу: http://metrology.com.ua/ download/dstu-gost-gost-r/60-dstu/440-dstu-3396-1-96.

20. ДСТУ ISO/IEC 9797-1 "Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блокові шифри" [Електронний ресурс] – Режим доступу: http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=66914

21. Інструкція користувача автоматизованої системи 3 класу, затверджена Наказом Міністерства економіки та з питань європейської інтеграції України №121 від 23.04.2002. [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/rada/show/v0121569-02/sp:max15

22. Інструкція про міжбанківський переказ коштів в Україні в національній валюті", затверджена Постановою Правління Національного Банку України № 320 від 16.08.2006. [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/go/z1035-06

23. Наказ №45 Адміністрації ДССЗЗІ 26.03.2007 "Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації" [Електронний ресурс] – Режим доступу: http://www.dsszzi. gov.ua/dsszzi/control/uk/publish/article ?art_id=50825&cat_id=38835

24. Наказ № 466 від 20.07.2004 Міністерства фінансів України "Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнання" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/ rada/show/v0466201-04

25. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.afa.biz.ua/documents/31-infobezopasnot/33-what-is-uncategorised-article?format=pdf.

26. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

27. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341

28. НДТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Чинний від 1999-04-22]. – К. : ДСТСЗІСБУкраїни, 1999. – 53 с. Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342

29. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

30. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/ dsszzi/ control/ uk/ publish/article?showHidden=1 & art_id=102287&cat_id=46556&ctime=1344505085689

31. НД ТЗІ 2.5-008-02 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблен-

ня в автоматизованих системах класу 2" [Електронний ресурс] – Режим доступу: http://info-stand.com/nb-ukraine/by-type/nd-tzi/22-ndtzi25-008-02.html.

32. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http:// www.dsszzi.gov.ua%2fdstszi%2fdoccatalog%2fdocument%3fid%3d41647&ei=guz5uk3xg8z3sga4r4cwcq&usg=afqjcnfye5kjfdqsympy-ekqedagtercmw&cad=rja.

33. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102299&ct_id=46556&ctime=1344510938381.

34. НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі" [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document? id=106349

35. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/ dstszi/doccatalog/document?id=106350

36. Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 № 93 Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175 [Електронний ресурс] – Режим доступу: http:// dstszi.kmu.gov.ua/dstszi/ doccatalog/ document?id=105528.

37. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/go/z0245-02

38. Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України [Електронний ресурс] – Режим доступу: http://bank.gov.ua/doccatalog/ document?id=22694128.

39. "Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи", затверджені Постановою Правління Національного банку України №243 від 04.07.2007 [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/go/z0955-07

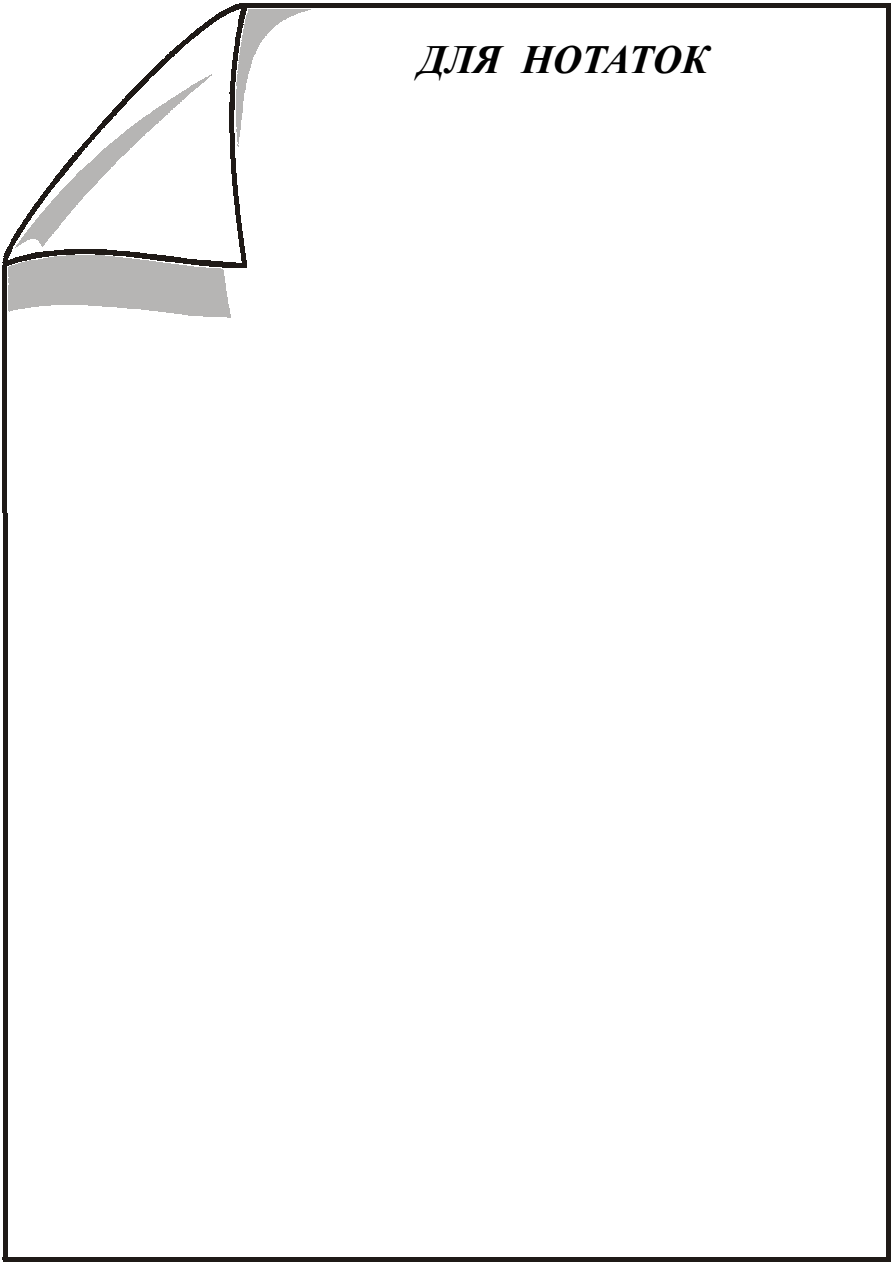
40. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації, затверджені Постановою Правління НБУ №829 від 26.11.2015 [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/ laws/show/z0419-07.

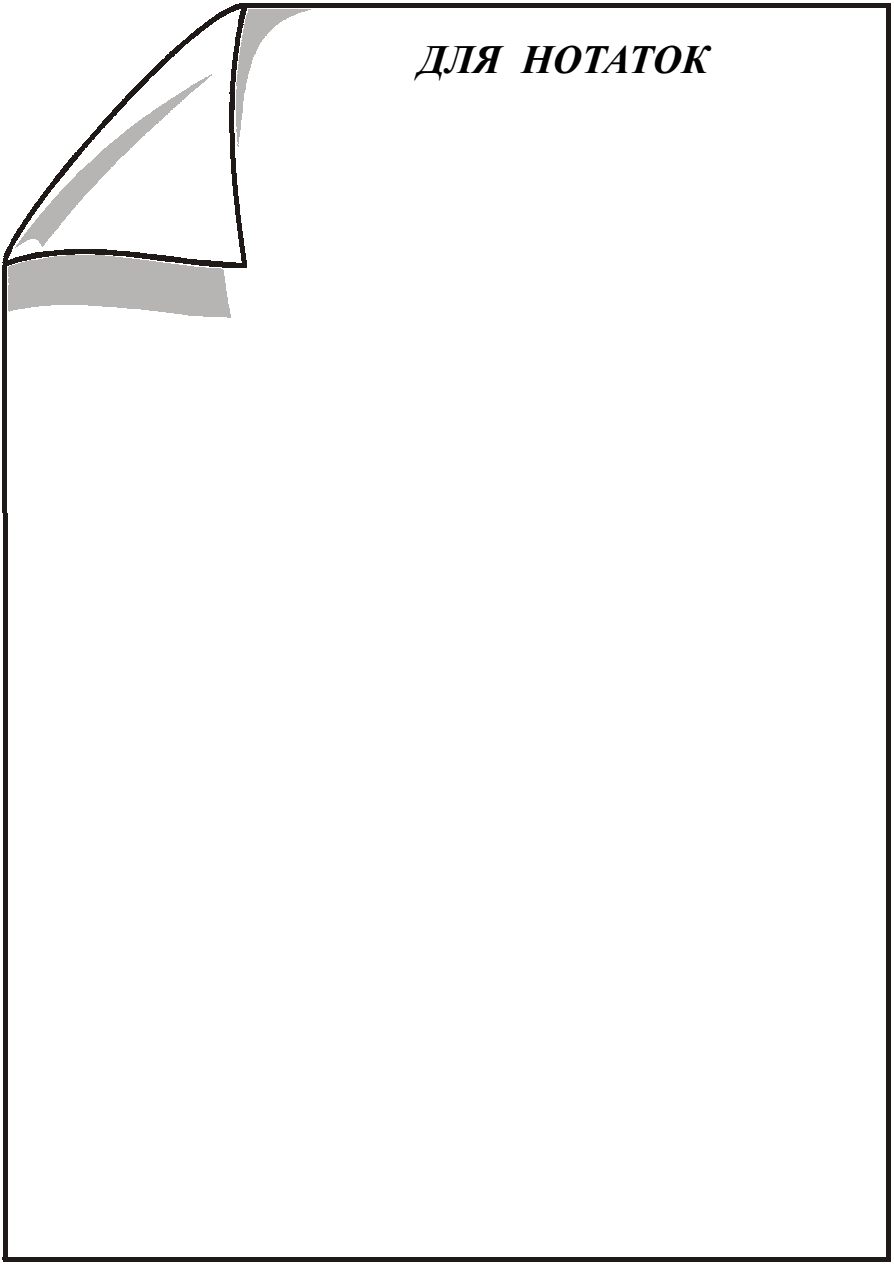
41. Р–СП Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень. – К.: ТОВ "НікС", 2003. – 25 с.

42. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/ control/uk/publish/article?showHidden=89769 &ctime=1421836194327.

43. ТРТЗІ – ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi /control/uk/publish/ article?showHidden=1 &art_id=101798&cat_id=89734 &ctime=1344500065981.

ЗМІСТ


ДЛЯ НОТАТОК


ДЛЯ НОТАТОК

Навчальне видання

ТУРТИ Марина Валентинівна
ЩЕЛКОНОГОВ Олег Олексійович
ЄРМАКОВА Альона Валеріївна

МЕТОДИЧНІ ВКАЗІВКИ
до самостійної роботи студентів
з дисципліни "АВТОМАТИЗАЦІЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ"

Комп'ютерне складання та верстання *В. В. Москаленко*
Коректор *О. Є. Вакула*

Формат 60×84/16. Ум. друк. арк. 2,4. Тираж 100 прим. Вид. № 19. Зам. № 2502-15.

Видавець і виготівник Національний університет кораблебудування
імені адмірала Макарова
просп. Героїв України, 9, м. Миколаїв, 54025
E-mail : publishing@nuos.edu.ua
Свідоцтво суб'єкта видавничої справи ДК № 6402 від 19.09.2018 р.