

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

О. Задерейко, Ю. Лобода

АНАЛІЗ СКЛАДНИХ СИСТЕМ

1847

Навчальний посібник

Для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»



Одеса
Фенікс
2023

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

УДК 004.3:004.31

3-15

*Рекомендовано вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16 червня 2023 р.)*

Укладачі:

Задерейко О. В. (ORCID ID 0000–0003–0497–9861),

Лобода Ю.Г. (ORCID ID 00001–7083–552X)

Рецензенти:

Положаєнко С. А. – доктор технічних наук, професор, завідувач кафедри комп'ютеризованих систем та програмних технологій Національного університету «Одеська політехніка»;

Щербакова Г. Ю. – доктор технічних наук, професор, професор кафедри «Інформаційні системи» Одеського національного політехнічного університету.

Задерейко О., Лобода Ю.

3 15

Аналіз складних систем : навч. посіб. [Електронне видання] / О. Задерейко, Ю. Лобода ; Нац. ун-т «Одес. юрид. академія». – Одеса : Фенікс, 2023. – 124 с. URL: <https://hdl.handle.net/11300/26009>

ISBN 978-966-928-970-4

Навчальний посібник присвячено вивченню проблем аналізу складних систем інформаційного спрямування.

Посібник містить загальні основи поняттєвого апарату складних систем різних типів. Розглянуто методологію аналізу сучасних інформаційно-комп'ютерних систем; наведено базові технології щодо діагностики інформаційно-комп'ютерних систем з точки зору забезпечення їх захищеності від потенційних витоків даних.

Призначений для спеціалістів у галузі системного аналізу, а також викладачів вищих навчальних закладів, студентів і аспірантів, які спеціалізуються у сфері аналізу систем різної складності та призначення.

УДК 004.3:004.31

ISBN 978-966-928-970-4

© Задерейко О.В., Лобода Ю.Г., 2023

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ПЕРЕДМОВА

Дисципліна «Аналіз складних систем» вивчається студентами за напрямом магістерської підготовки (другого освітнього рівня) з галузі знань 12 «Інформаційні технології» на першому курсі навчання.

Метою викладання навчальної дисципліни «Аналіз складних систем» є засвоєння базових знань та практичних навичок з теоретичних основ та закономірностей функціонування складних систем, а також отримання практичних навичок з діагностики, аналізу вірогідних вразливостей складних систем інформаційного спрямування.

Коротким описом предметної сфери є оволодіння студентами поглибленими теоретичними та фундаментальними знаннями в області діагностики складних інформаційно-комп'ютерних систем та вироботки оптимальних заходів що мають запобігати потенційним витокам даних.

Оволодіння курсом «Аналіз складних систем» передбачає читання лекцій, проведення лабораторних занять, виконання самостійної роботи та складання іспиту. Особлива увага приділяється отриманню студентами поглиблених теоретичних та практичних знань, умінь, навичок у виконанні аналізу складних інформаційних систем, що є підґрунтям для засвоєння та удосконалення знань отриманих при вивченні інших модулів професійної та практичної підготовки.

Згідно з вимогами освітньо-професійної програми після вчення дисципліни «Аналіз складних систем» студенти повинні:

- **знати** методологію аналізу складних систем та їх складових об'єктів;
- **знати** фундаментальні стратегії діагностування складних систем різного походження;
- **володіти** навичками з виявлення порушень функціонування складних систем;
- **знати** опис інструментальних засобів що можуть бути використані для аналізу складних систем;
- **вміти** здійснювати пошук, оброблення інформації та аналіз даних отриманих з складних систем.

Α Ω

НАЦІОНАЛЬНИЙ

УНІВЕРСИТЕТ

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ЗМІСТ

ПЕРЕДМОВА	3
ТЕМА 1. ПОНЯТТЄВИЙ АПАРАТ СКЛАДНИХ СИСТЕМ	8
Розділ 1. Загальні положення складних систем	8
1.1. Введення у поняття системи	8
1.2. Мета системи	12
1.3. Зв'язок системи та середовища	14
1.4. Принципи аналізу систем	15
1.5. Принципи аналізу систем	19
1.6. Імовірні ризики аналізу систем	21
1.7. Поняття складної системи	23
1.8. Подання складної системи	24
1.9. Принципи вивчення та аналізу складних систем	24
1.10. Загальна проблематика складних систем	25
1.11. Проблематика процесу вирішення проблеми	27
1.12. Обмеження і умови вирішення проблеми	30
1.13. Особливості постановки проблеми	32
Контрольні запитання	33
Розділ 2. Принципи опису складних систем	35
2.1. Інформаційні аспекти аналізу складних систем	35
2.2. Поняттєвий апарат складних інформаційних систем	36
2.3. Інформаційні моделі складних систем	38
Контрольні запитання	39
ТЕМА 2. ІНФОРМАЦІЙНИЙ ОПИС МЕРЕЖЕВИХ СИСТЕМ	40
Розділ 3. Збір інформації в інформаційно-комп'ютерних системах	40
3.1. Способи збирання інформації про мережеві структури	40
3.2. Попереднє вивчення мети	41
3.2.1. Деякі прийоми	41
3.2.2. Аналіз публічно доступних ресурсів	41
3.2.3. Використання пошукових систем	43
3.2.4. Набуття інформації реєстраційного характеру	44
3.2.5. Використання DNS	45
Контрольні запитання	46

ТЕМА 3. АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ	47
Розділ 4. Вразливості об'єктів інформаційно-комп'ютерних систем.....	47
4.1. Інформаційна мережа як об'єкт захисту	47
4.2. Подія безпеки	49
4.3. Поняття вразливості.....	50
4.4. Класифікація вразливостей	51
4.4.1. Вразливість проєктування	51
4.4.2. Вразливість реалізації.....	52
4.4.3. Вразливість експлуатації.....	53
4.5. Джерела інформації щодо вразливостей	53
4.5.1. База уразливостей (Bugtraq).....	53
4.5.2. База уразливостей X-Force.....	54
4.5.3. База уразливостей US-CERT Vulnerability Notes Database	54
4.5.4. База уразливостей SecurityTracker.....	54
4.5.5. База уразливостей Secunia	54
4.5.6. База уразливостей Open Source Vulnerability Database	54
4.6. Прийняті позначення вразливостей	54
4.6.1. Common Vulnerabilities and Exposures.....	54
4.7. Каталог National Vulnerability Database	56
4.8. Вразливість та безпека промислових систем управління	59
4.8.1. Концепція SCADA	60
4.8.2. Тенденції безпеки АСУ ТП	60
4.9. Виявлення вразливостей комп'ютерних систем	62
4.9.1. Аналіз алгоритму програмно-апаратного забезпечення ...	62
4.9.2. Динамічний аналіз безпеки додатка	62
4.9.3. Статичний аналіз безпеки програми	62
4.9.4. Змішаний аналіз безпеки програми	63
4.9.5. Виявлення «відомих» уразливостей.....	63
4.10. Системи аналізу захищеності	64
4.10.1. Можливості та архітектура	64
4.10.2. Скануючі модулі	65
4.10.3. Приклади засобів аналізу захищеності	67
4.11. Мережеві сканери безпеки	68
4.12. Розміщення мережевих агентів сканування у мережі	69
4.13. Мережеві агенти та збір інформації	71
4.14. Аналіз захищеності бездротових мереж.....	72
4.14.1. Особливості сканування бездротових мереж	72
4.14.2. Завдання сканування бездротових мереж.....	72
4.14.3. Уразливості які характерні для бездротових мереж	72

4.14.4. Сканування точки доступу на мережному рівні	73
4.14.5. Методологія аудиту	74
Контрольні запитання.....	77
Розділ 5. Інструментарій аналізу інформаційно-комп'ютерних систем	79
5.1. Використання протоколу ICMP	79
5.1.1. Загальні відомості про протокол ICMP	79
5.1.2. Використання повідомлень ICMP Echo (Type 8) та Echo Reply (Type 0)	82
5.1.3. Опитування безлічі пристроїв	82
5.1.4. Утиліта fping	82
5.1.5. Утиліта nmap	83
5.1.6. Використання Broadcast ICMP	83
Контрольні запитання.....	83
Розділ 6. Визначення топології інформаційно-комп'ютерних систем	85
6.1. Відстеження маршрутів.....	85
6.2. Відстеження маршрутів та фільтрація	87
6.2.1. Утиліта tracert	88
Контрольні запитання.....	88
Розділ 7. Ідентифікація елементів інформаційно-комп'ютерних систем	89
7.1. Ідентифікація статусу порту	89
7.1.1. Сканування портів.....	89
7.2. Сканування портів TCP	90
7.2.1. Сканування із встановленням з'єднання.....	90
7.2.2. SYN-сканування.....	91
7.2.3. Фільтрування на прикладному рівні	92
7.3. Сканування портів UDP	92
7.4. Ідентифікація сервісів та додатків	94
7.4.1. Ідентифікація TCP-служб	94
7.4.2. Врахування особливостей роботи протоколів.....	95
7.4.2.1. SMTP-сервер	95
7.4.2.2. Web-сервер.....	96
7.4.3. Інструменти сканування	96
7.5. Ідентифікація UDP-служб.....	97
7.5.1. Сканування на прикладному рівні	97
7.5.2. Аналіз параметрів повторної передачі.....	97
7.6. Сканування протоколів	97
7.7. Ідентифікація операційних систем	98
7.7.1. Простейшие методы определения ОС	98

7.7.1.1. Аналіз наборів відкритих портів	98
7.7.2. Використання сервісів прикладного рівня	99
7.7.3. Опитування стека TCP/IP	100
7.7.4. Дослідження значення ISN	101
7.7.5. Дослідження поля Window TCP-пакету	102
7.7.6. Використання поля Reserved (Bogus-flag)	103
7.7.7. Дослідження поля ACK	103
7.8. Інструменти ідентифікації	103
7.8.1. SinFP	104
7.8.2. Використання протоколу ICMP	104
7.8.2.1. Розмір ICMP-повідомлення	104
7.8.3. Зміни у вихідній датаграмі	105
7.8.4. Retransmission Timeout	106
7.8.5. Port 0 OS Fingerprinting	106
7.9. Активна ідентифікація	107
7.10. Пасивна ідентифікація	107
7.10.1. Аналіз мережевого трафіку	107
7.11. Аналіз запитів від сканованого вузла	110
Контрольні запитання	112
ТЕМА 5. АНАЛІЗ ПОТОКІВ ІНФОРМАЦІЙНИХ СИСТЕМ	113
Розділ 8. Моніторинг трафіка інформаційно-комп'ютерних систем	113
8.1. Додатки для відстеження трафіку	113
8.1.1. Як працює мережевий сніффінг	113
8.1.2. Як запобігти атакам мережевих перехоплювачів	114
8.2. Завдання моніторингу мережі та аналізу трафіку	114
8.2.1. Програмний моніторинг	115
8.2.2. Зовнішні атаки	115
8.3. Моніторинг трафіку локальних мереж	115
8.3.1. Причини контролю мережевого трафіку	115
8.3.2. Методи збору даних	116
8.3.3. Міжмережевий екран	116
8.3.4. Маршрутизатор	117
8.3.5. Libpcap	117
8.4. Аналіз мережевого трафіка і його аналізатори	117
8.4.1. Як використовуються аналізатори пакетів	117
8.4.2. Оцінка аналізатора пакетів	118
8.4.3. Принцип дії аналізаторів пакетів	119
Контрольні запитання	120
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ	121

The background of the image is the official coat of arms of the National University of Odessa Law Academy. It features a central shield with a blue and gold design, flanked by golden laurel branches. At the top of the shield is a golden crown. Below the shield is an open book with the Greek letters Alpha (Α) and Omega (Ω) on its pages. A blue ribbon banner at the bottom contains the text "ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ".

УВАГА!

Повна версія навчального посібника розташована на сайті дистанційного навчання факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

за адресою: <http://cyber.onua.edu.ua>

З усіх питань стосовно повної версії навчального посібника звертатися за адресою:

zadereyko@onua.edu.ua

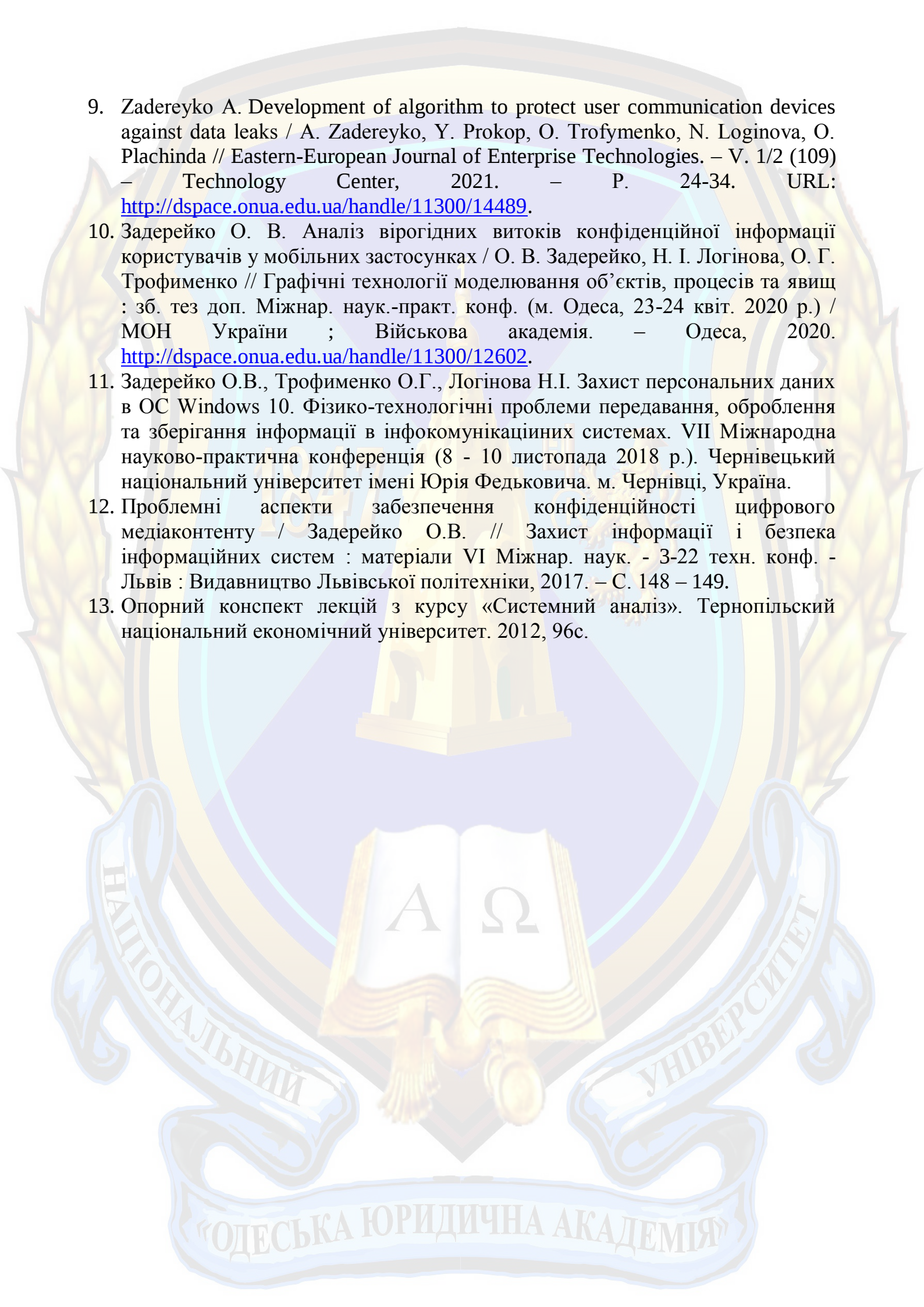
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Список основних джерел

1. Задерейко О.В., Троянський О.В., Чанишев Р.І., Дика А.І. Концептуальні основи захисту інформаційного суверенітету України : монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев, А.І. Дика – Одеса : Фенікс, 2022. – 220 с. ISBN 978-966-928-812-7. URL: <http://dspace.onua.edu.ua/handle/11300/22733>
2. Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Аналіз складних систем» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» / Уклад.:О.В. Задерейко. – Одеса:НУ «ОЮА», 2021. – 103 с.
3. Ситнік Б.Т. Основи інформаційних систем і технологій : Навч. посібник. – Харків:УкрДУЗТ, 2019. – 175 с., рис. 27, табл.7.
4. Ситнік Б.Т. Комп'ютерні системи керування : Навч. посібник. – Ч1. – Моделювання систем. –Харків:УкрДУЗТ, 2019. – 182с.
5. К. П. Макаренко. І. Г. Бачкір. Методичні вказівки щодо виконання контрольної роботи з навчальної дисципліни «основи теорії систем та системного аналізу» для студентів денної та заочної форм навчання зі спеціальності 073 – «менеджмент» освітнього ступеня «бакалавр». Кременчуцький національний ун-т. 2019, 49 с.
6. Конспект лекцій з дисципліни «Системний аналіз» для студентів спеціальності 121 – «Інженерія програмного забезпечення» / Крісілов В.А., Городнича К.А. Одеса:ОНПУ, 2018. - 37 с.
7. Федоров М. В. Системний аналіз:конспект лекцій для студентів 2 курсу денної та 1 курсу прискореної форм навчання освітнього рівня «бакалавр» спеціальності 122–Комп'ютерні науки / М. В. Федоров, О. М. Хренов;Харків. нац. ун-т міськ. госп-ва ім. О.М. Бекетова. – Харків:ХНУМГім. О.М. Бекетова, 2018. – 62 с.
8. Яковлев С.В. Конспект лекцій з дисципліни «Основи загальної теорії систем». Харків:Харківський національний університет внутрішніх справ, 2017, 34 с.
9. Роїк, О. М. Системний аналіз. Навчальний посібник / О.М. Роїк, А.А. Шиян, Л.О. Нікіфорова – Вінниця:ВНТУ, 2015. – 83 с.
10. Варенко В. М. Системний аналіз інформаційних процесів:навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – К.:Університет «Україна», 2013. – 203 с.
11. Системний аналіз складних систем управління:Навч. посіб. / А. П. Ладанюк, Я.В. Смітюх, Л.О. Власенко та ін. — К.:НУХТ, 2013. — 274 с.
12. Варенко В. М., Братусь І. В., Дорошенко В. С., Смольников Ю. Б., Юрченко В. О. Системний аналіз інформаційних процесів : Навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – К.:Університет «Україна», 2013. – 203с.

Список допоміжних джерел

1. Задерейко О. В., Логінова Н.І. Захист приватних даних користувачів при web-серфінгу. Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень: у 2 т. : матеріали Міжнар. наук.- практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. - Одеса : Видавництво «Юридика», 2023. - Т. 1. С. 588 - 593.
2. Задерейко О.В., Ханов Б.В. OSINT – базові знання у розвідці. Інформаційне суспільство: проблеми та перспективи : матеріали VIII Всеукр. наук.- практич. конф. (м. Одеса, 2 черв. 2023 р.) / відп. ред. Н. І. Логінова. - Одеса, 2023, С. 109 - 111. DOI: <https://doi.org/10.32837/11300.25263>.
3. Задерейко О.В. Аналіз процесів як умова виживання суспільства // Кібербезпека в сучасному світі: актуальні виклики : матер. IV всеукр. наук.- практ. конф. (25 листопада 2022 р.). Одеса, НУ «ОЮА», 2022, – С. 186 - 188. – URL: <http://dspace.onua.edu.ua/handle/11300/23214>.
4. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. Radioelectronic and Computer Systems. 2022. No 4. P.64-84. DOI: <https://doi.org/10.32620/reks.2022.4.05>. URL: <http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2022.4.05>.
5. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Дика А.І. Захист даних користувачів в інформаційних системах. Сучасна спеціальна техніка. № 1 (68), 2022, С. 23-33. URL: <http://dspace.onua.edu.ua/handle/11300/23313>.
6. Задерейко О.В. Янковський О.В. Дика А.І. Забезпечення конфіденційності месенджера Telegram / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. С. 708 - 715. URL: <http://dspace.onua.edu.ua/handle/11300/19768>.
7. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021, С. 16-30. URL: <http://dspace.onua.edu.ua/handle/11300/23298>.
8. Задерейко О.В., Кухаренко С.В. Захист персональних даних від витоків в операційних системах сімейства Windows / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса:Видавничий дім «Гельветика», 2022. – Т. 1. С. 685 - 689. URL: <http://dspace.onua.edu.ua/handle/11300/19761>.

- 
9. Zadereyko A. Development of algorithm to protect user communication devices against data leaks / A. Zadereyko, Y. Prokop, O. Trofymenko, N. Loginova, O. Plachinda // Eastern-European Journal of Enterprise Technologies. – V. 1/2 (109) – Technology Center, 2021. – P. 24-34. URL: <http://dspace.onua.edu.ua/handle/11300/14489>.
 10. Задерейко О. В. Аналіз вірогідних витоків конфіденційної інформації користувачів у мобільних застосунках / О. В. Задерейко, Н. І. Логінова, О. Г. Трофименко // Графічні технології моделювання об'єктів, процесів та явищ : зб. тез доп. Міжнар. наук.-практ. конф. (м. Одеса, 23-24 квіт. 2020 р.) / МОН України ; Військова академія. – Одеса, 2020. <http://dspace.onua.edu.ua/handle/11300/12602>.
 11. Задерейко О.В., Трофименко О.Г., Логінова Н.І. Захист персональних даних в ОС Windows 10. Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах. VII Міжнародна науково-практична конференція (8 - 10 листопада 2018 р.). Чернівецький національний університет імені Юрія Федьковича. м. Чернівці, Україна.
 12. Проблемні аспекти забезпечення конфіденційності цифрового медіаконтенту / Задерейко О.В. // Захист інформації і безпека інформаційних систем : матеріали VI Міжнар. наук. - 3-22 техн. конф. - Львів : Видавництво Львівської політехніки, 2017. – С. 148 – 149.
 13. Опорний конспект лекцій з курсу «Системний аналіз». Тернопільський національний економічний університет. 2012, 96с.

НАВЧАЛЬНЕ ВИДАННЯ

*Олександр Владиславович Задерейко
Юлія Геннадіївна Лобода*

АНАЛІЗ СКЛАДНИХ СИСТЕМ

Навчальний посібник

*Для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»*

Електронне видання

В авторській редакції

Ум-друк. арк. 7,44. Зам. № 2308-11.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

НАВЧАЛЬНЕ ВИДАННЯ

*Олександр Владиславович Задерейко
Юлія Геннадіївна Лобода*

АНАЛІЗ СКЛАДНИХ СИСТЕМ

Навчальний посібник

1847 Для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»

Електронне видання

В авторській редакції

Ум-друк. арк. 7,44. Зам. № 2308-11.

Видавець ПП «Фенікс»
(Свідцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net

НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»